



Know Your Customer: Quick Reference Guide

January 2016



Know Your Customer: Quick Reference Guide

Understanding global KYC differences

January 2016

As predicted, 2015 saw a continued rise in regulatory pressures concerning Anti-Money Laundering (“AML”), with a number of high profile fines and investigations. Compliance with AML, Know Your Customer (“KYC”) and sanctions requirements continues to be a key focus area for management, and firms must ensure they are following appropriate compliance procedures to meet the increasing regulatory demands. Firms operating on a global scale must also demonstrate a robust compliance framework, ensuring that each territory has sufficient management oversight and that AML requirements are being adhered to at both a local and global level.

Given these challenges, we have further developed our KYC Quick Reference Guide, an easy access tool providing the key information firms need to understand and mitigate their AML risks. Since its launch seven years ago, the Guide has remained a popular resource and continues to be of value to those seeking to understand AML requirements globally. This year, we have continued to increase the level of global coverage, with information on Bangladesh, the Dominican Republic, Ecuador, Ethiopia, Honduras and Latvia as new additions to the 2016 Guide, taking the total countries covered to 92. We are keen to continue expanding our reach, so please let us know if your country is not currently part of our Guide and you would like to be included next year.

Please rollover map to select your region then click to select country of choice



Know Your Customer: Quick Reference Guide

Understanding global KYC differences

Content of the Guide

Fundamental KYC requirements, regulators' views on the use of the risk based approach, dealing with Politically Exposed Persons ("PEPs") and guidance on prohibitions relating to shell banks are all subjects covered within the Guide.

The Guide also contains up to date information on regulatory and other cultural issues which need to be addressed when conducting business across multiple jurisdictions. Useful links to Financial Action Task Force ("FATF") reports and country evaluations are also included, in addition to questions on suspicious activity reporting obligations, penalties for non-compliance, AML audits and data privacy. Our Guide also provides an insight into the relevant AML regulations affecting each country and includes links, where relevant, detailing further information.

From time to time, you may need expert advice from AML specialists. We've included details of the appropriate PwC Financial Crime professionals in the countries featured. They would be happy to discuss any AML issues you might have.

[Click to return to main map](#)



Europe

Austria	Estonia	Hungary	Luxembourg	Russia	UK
Belgium	Finland	Ireland	Malta	Slovakia	Ukraine
Bosnia & Herzegovina	France	Isle of Man	Netherlands	Slovenia	
Croatia	Germany	Italy	Norway	Spain	
Cyprus	Gibraltar	Jersey	Poland	Sweden	
Czech Republic	Greece	Kazakhstan	Portugal	Switzerland	
Denmark	Guernsey	Latvia	Romania	Turkey	

Know Your Customer: Quick Reference Guide

Understanding global KYC differences

Content of the Guide

Fundamental KYC requirements, regulators' views on the use of the risk based approach, dealing with Politically Exposed Persons ("PEPs") and guidance on prohibitions relating to shell banks are all subjects covered within the Guide.

The Guide also contains up to date information on regulatory and other cultural issues which need to be addressed when conducting business across multiple jurisdictions. Useful links to Financial Action Task Force ("FATF") reports and country evaluations are also included, in addition to questions on suspicious activity reporting obligations, penalties for non-compliance, AML audits and data privacy. Our Guide also provides an insight into the relevant AML regulations affecting each country and includes links, where relevant, detailing further information.

From time to time, you may need expert advice from AML specialists. We've included details of the appropriate PwC Financial Crime professionals in the countries featured. They would be happy to discuss any AML issues you might have.

[Click to return to main map](#)



Americas

Argentina	Canada	Colombia	Honduras	Paraguay	USA
Bolivia	Cayman Islands	Dominican Republic	Jamaica	Peru	
Brazil	Chile	Ecuador	Mexico	Uruguay	

Know Your Customer: Quick Reference Guide

Understanding global KYC differences

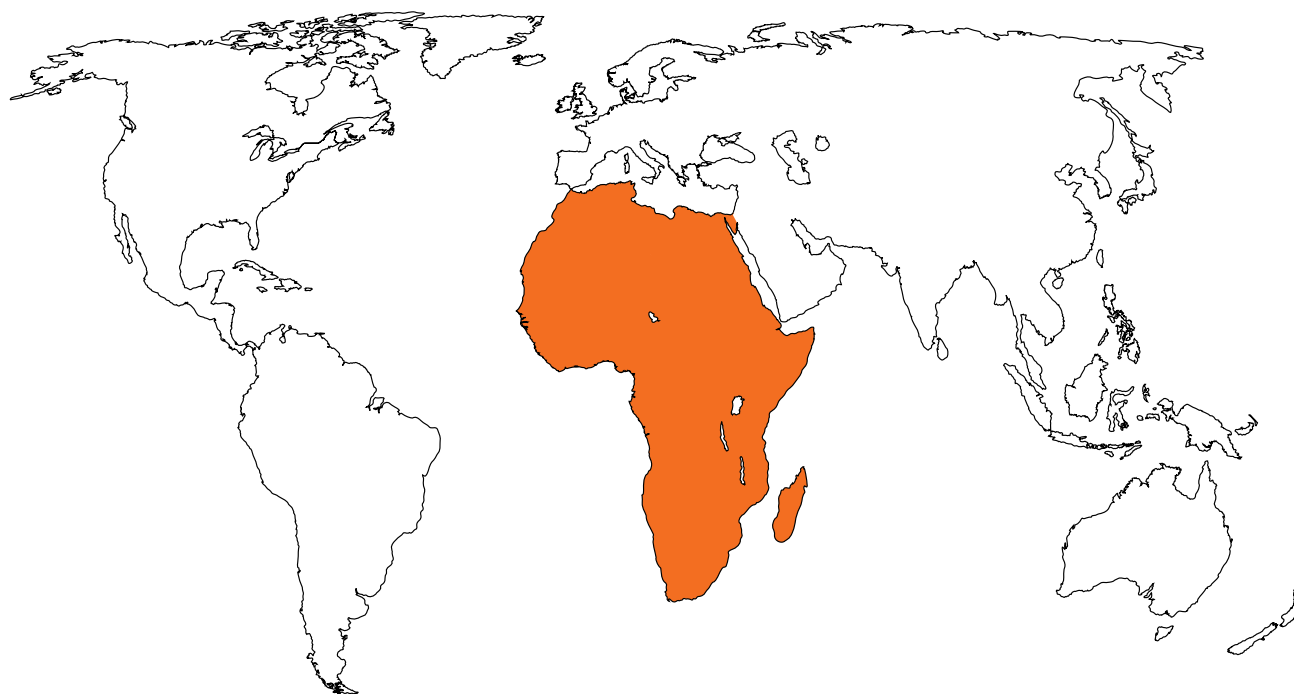
Content of the Guide

Fundamental KYC requirements, regulators' views on the use of the risk based approach, dealing with Politically Exposed Persons ("PEPs") and guidance on prohibitions relating to shell banks are all subjects covered within the Guide.

The Guide also contains up to date information on regulatory and other cultural issues which need to be addressed when conducting business across multiple jurisdictions. Useful links to Financial Action Task Force ("FATF") reports and country evaluations are also included, in addition to questions on suspicious activity reporting obligations, penalties for non-compliance, AML audits and data privacy. Our Guide also provides an insight into the relevant AML regulations affecting each country and includes links, where relevant, detailing further information.

From time to time, you may need expert advice from AML specialists. We've included details of the appropriate PwC Financial Crime professionals in the countries featured. They would be happy to discuss any AML issues you might have.

[Click to return to main map](#)



Africa

Angola
Cameroon

Côte d'Ivoire
Egypt

Ethiopia
Gabon

Ghana
Kenya

Mauritius
Nigeria

South Africa
Zambia

Know Your Customer: Quick Reference Guide

Understanding global KYC differences

Content of the Guide

Fundamental KYC requirements, regulators' views on the use of the risk based approach, dealing with Politically Exposed Persons ("PEPs") and guidance on prohibitions relating to shell banks are all subjects covered within the Guide.

The Guide also contains up to date information on regulatory and other cultural issues which need to be addressed when conducting business across multiple jurisdictions. Useful links to Financial Action Task Force ("FATF") reports and country evaluations are also included, in addition to questions on suspicious activity reporting obligations, penalties for non-compliance, AML audits and data privacy. Our Guide also provides an insight into the relevant AML regulations affecting each country and includes links, where relevant, detailing further information.

From time to time, you may need expert advice from AML specialists. We've included details of the appropriate PwC Financial Crime professionals in the countries featured. They would be happy to discuss any AML issues you might have.

[Click to return to main map](#)



Middle East

Bahrain
Iraq

Israel
Jordan

Kuwait
Lebanon

Oman
Qatar

Saudi Arabia
UAE

West Bank & Gaza

Know Your Customer: Quick Reference Guide

Understanding global KYC differences

Content of the Guide

Fundamental KYC requirements, regulators' views on the use of the risk based approach, dealing with Politically Exposed Persons ("PEPs") and guidance on prohibitions relating to shell banks are all subjects covered within the Guide.

The Guide also contains up to date information on regulatory and other cultural issues which need to be addressed when conducting business across multiple jurisdictions. Useful links to Financial Action Task Force ("FATF") reports and country evaluations are also included, in addition to questions on suspicious activity reporting obligations, penalties for non-compliance, AML audits and data privacy. Our Guide also provides an insight into the relevant AML regulations affecting each country and includes links, where relevant, detailing further information.

From time to time, you may need expert advice from AML specialists. We've included details of the appropriate PwC Financial Crime professionals in the countries featured. They would be happy to discuss any AML issues you might have.

[Click to return to main map](#)



Asia/Pacific

Australia	Hong Kong	Japan	Pakistan	South Korea	Vietnam
Bangladesh	India	Malaysia	Philippines	Taiwan	
China	Indonesia	New Zealand	Singapore	Thailand	

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Angola

Key contact: Ines Correia Neves
Email: ines.correia.neves@pt.pwc.com
Tel: +351 21 359 93 345

Postal address: Presidente Business Center
Largo 4 de Fevereiro n.º3, 1º andar- Sala 137
Luanda; Angola

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Law no. 34/11 was issued on 12 Dec 2011 and Aviso N° 21/2012 and N° 22/2012 for financial institutions.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	The regulators for AML controls are: a) Banco Nacional de Angola (www.bna.ao); and b) Direcção Nacional de Investigação e Inspeção das Actividades Económicas do Comando Geral da Policia Nacional (http://www.policiaeconomica.gv.ao/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	There is a guide issued by the banking regulator at (http://www.bna.ao/uploads/%7B336b248e-8785-4a72-ade1-2dc17a3f962e%7D.pdf).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Law no. 34/11 does not make any reference to requirements to retrospectively verify the identity of customers before the date the new AML regime was introduced. This may be clarified in regulation expected to be issued in the near future.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Law no. 34/11 provides that, in compliance with identification and due diligence requirements, financial institutions can adapt the nature and scope of verification and due diligence procedures, taking into account the risk associated with the type of customer, the business relationship, the product, the type of transaction and the origin or the purpose of the funds.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The last FATF Mutual Evaluation conducted for Angola was published in October 2012 (http://www.esaamlg.org/userfiles/ANGOLA_MUTUAL_EVALUATION_DETAIL_REPORT.pdf). However, in October 2014, FATF published a Global AML/ CFT Compliance publication where Angola's AML regime is briefly analysed: (http://www.fatf-gafi.org/countries/a-c/angola/documents/fatf-compliance-oct-2014.html). The last IMF Country Report was published in May 2012. The report is the sixth country review under the stand-by agreement: (http://www.imf.org/external/pubs/cat/longres.aspx?sk=25888.0). The IMF country page for Angola is (http://www.imf.org/external/country/ago/index.htm).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes. One-off transactions under USD15,000 (or equivalent in local currency). All cash operations equal or above USD15,000 should be reported to national authorities.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: should provide a valid document with: full name, signature, address, profession and work place (when applicable), birth date, nationality, funds provenience and tax identification number (optional). Corporates: should provide a valid document with their deeds of incorporation or valid licence (certification should be made through the card Cartão de Identificação de Pessoa Colectiva or Certidão do Registo Comercial), the headquarters address, tax identification number, shareholder identification if more than 20% of the voting rights, and board of directors identification.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	The copies of documentation must be certified.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Management Board and shareholder identification must occur if more than 20% of the voting rights are held. Identification and verification requirements for beneficial owners are the same as those for individuals or companies listed above.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	a) where the customer is a State or a Public Sector Entity (at country, regional or local level); or b) where the customer is a Governmental Authority or Public Institute subject to transparent accounting practices and supervision.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Entities shall apply enhanced due diligence measures in respect of customers and transactions which by their nature or characteristics can present a higher risk of money laundering or terrorist financing. Those measures are always required when operations are carried out with non face-to-face customers; with Politically Exposed Persons ("PEPs"); a resident outside the national territory; in the case of correspondent banking transactions with credit institutions established in third countries; those designated by the competent supervisory authorities and Private Banking.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	A PEP relationship requires additional due diligence. When establishing a relationship with a non-resident PEP, the entities should have appropriate risk based procedures to determine whether the customer is a PEP; have approval from senior management before establishing business relationships with such customers; take adequate measures to establish the source of wealth and funds involved in the business relationship or occasional transactions; and conduct enhanced ongoing monitoring of the business relationship.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	When establishing a relationship through correspondence with third country banks, this relationship must take into consideration the banks country and its AML risk, the analysis of the bank's internal procedures regarding the international laws of anti-money laundering, the guarantee of information accuracy and the bank's reputation. In addition, the financial institution should guarantee that the due diligence duty was observed.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Non face-to-face relationships (especially those that can favour anonymity) require additional due diligence. In such relationships, the institution should either ask for legal documentation as additional documentation to verify/ certify the documentation provided by the customer. This may be provided by another financial institution or it can be requested that the first payment is made through an account opened in the name of the customer with another financial institution.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The SARs are made to Banco Nacional de Angola (www.bna.ao) and Direcção Nacional de Investigação e Inspeção das Actividades Económicas do Comando Geral da Polícia Nacional (http://www.policiaeconomica.gv.ao/).

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Cash transactions equal or above USD15,000 (or the equivalent amount in local currency) should be reported to national authorities (article 13).
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Article 49 provides that breaches of regulations shall be punishable as follows: a) Where the offence is committed within the scope of activity of a financial entity: a. By a fine from USD25,000 to USD2.5m, (or the equivalent amount in local currency) where the offender is a legal person; or b. By a fine from USD12,500 to USD1.25m, (or the equivalent amount in local currency) where the offender is a natural person. b) Where the offence is committed within the scope of activity of a non-financial entity, with the exception of lawyers and solicitors: c. By a fine from USD5,000 to USD500,000, (or the equivalent amount in local currency) where the offender is a legal person; or d. By a fine from USD2,500 to USD250,000, (or the equivalent amount in local currency) where the offender is a natural person. Article 50 provides for the imposition of additional penalties.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	a) yes; b) n/a; and c) yes.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	N/A
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Cameroon

Key contacts:

Douty Fadiga / Geoffroy Kamga

Email: d.fadiga@cm.pwc.com /geoffroy.kamga@cm.pwc.com

Tel: +237 677 93 40 70 / +237 677 50 01 18

Postal address: P.O.Box 5689,

Douala,

Cameroon

Last updated:

January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	AML law and regulations became effective in 2005 and are only applicable for banks.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) The Banking Commission (www.beac.int); b) none; and c) none.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	No.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, an update of the customer database is required.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	No. There is no risk based approach approved by the local regulator.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, the country has been subjected to a FATF evaluation, but the report is not publicly available.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No, there are no minimum transaction thresholds under which customer due diligence is not required.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The requirements are: a) verification of the identity and address of the customer by reference to official identity papers; b) for legal entities, the verification of legal documents and legal representatives is required; c) public officials require heightened scrutiny; and d) the bank must collect information to cover the following: anticipated account activity, source of wealth and sources of funds.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	None in practice. Copies of identification documentation are only made by the bank after a visual check. An independent verification is not required.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The requirements are: a) obtain information on the beneficial owner; and b) verification of the identification and the address of the professional intermediary.

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Customer due diligence arrangements are reduced for low value transactions.

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Customer due diligence is enhanced for unusual or suspicious activities/transactions.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	For a PEP, the bank's senior management must give authorisation before an account opening. The transactions in their accounts require heightened scrutiny.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Banks must acquire information on the compliance of their correspondent with AML regulation. The relationship must not be established if the correspondent is not compliant with AML regulation.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	For a non face-to-face relationship, a bank must consider the need to perform independent verification.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	National Agency for Financial Investigation ("ANIF"): www.anif.cm

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs (The website of ANIF has not been updated since 2013): 2010 – 124 SARs GDP (in current prices): 2010 – USD23,622m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD190.5m of GDP.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	There is an obligation to report on transactions where the identity of the beneficiary or the originator is suspicious.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	No.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of “personal data” cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of “sensitive data”? How is it defined and what are the additional protections?
A29.	No.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes.

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Côte d'Ivoire (Ivory Coast)

Key contact: Douty Fadiga
Email: d.fadiga@cm.pwc.com
Tel: +237 77 93 40 70

Postal address: P.O.Box 5689,
Douala,
Cameroon

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	AML law and regulations became effective in 2007 and are only applicable for banks.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) Banking Commission (www.bceao.int); b) none; and c) none.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	No.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, an update of the customer database is required.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	No, there is no risk based approach approved by the local regulator.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, the country has been subjected to a FATF evaluation, but the report is not publicly available.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No, there are no minimum transaction thresholds under which customer due diligence is not required.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The requirements are: a) verification of the identity and address of the customer by reference to official identity papers; b) for legal entities, the verification of legal documents and legal representatives is required; c) public officials require heightened scrutiny; and d) the bank must collect information to cover the following: anticipated account activity, source of wealth and sources of funds.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	None in practice. Copies of identification documentation are only made by the bank after a visual check. Independent verification is not required.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The requirements are: a) obtain information on the beneficial owner; and b) verification of the identification and the address of the professional intermediary.

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Customer due diligence arrangements are reduced for low value transactions.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Customer due diligence is enhanced for unusual or suspicious activities/transactions.

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	For a PEP, the bank’s senior management may give authorisation before opening an account. The transactions in their accounts require heightened scrutiny.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Banks must acquire information on the compliance of their correspondent with AML regulation. The relationship must not be established if the correspondent is not compliant with AML regulation.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	For a non face-to-face relationship, a bank must consider the need to perform independent verification.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	National Centre for Processing of Financial Information (‘CENTIF’) (www.centif.ci).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2010 – 56 SARs GDP (in current prices): 2010 – USD24,800m (Source: data.worldbank.org) This results in a ratio of 1 SAR for every USD443m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	There is an obligation to report on transactions where the identity of the beneficiary or the originator is suspicious.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	No.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	No.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Egypt

Key contacts: Nabil Diab
Email: nabil.diab@eg.pwc.com
Tel: +1 (0) 876 932 8335

Postal address: Plot no 211, Second Sector,
City Center, New Cairo, 11835, Egypt
PO Box 170 New Cairo

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2002.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) CBE (Central Bank of Egypt): (www.cbe.org.eg/); b) it depends on the nature of the financial services (e.g. Insurance companies are regulated by the EISA (Egyptian Insurance Supervisory Authority). However, all of the "non-banking" financial services providers are governed and regulated by the EFSA (Egyptian Financial Supervisory Authority): (http://www.efsa.gov.eg/jtags/efsa_en/index_en.jsp); and c) governed by the "Anti Money Laundering Law"- Law # 80 for year 2002.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	There is only the "Anti-Money Laundering Law" - Law # 80 for year 2002.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: name, address and date of birth, ideally from government-issued documents such as government identification, passport and weapon licence that includes the customer's full name and photograph, and either address or date of birth. Corporates: should obtain full name, Commercial Register copy, business address, and additionally for private companies, names of all directors and beneficial owners. This should be clearly noted in the Commercial Register of the company and also show the authorised signatories of the company. If the company is regulated (e.g. insurance or capital markets) it should provide confirmation of the company's listing on the regulated market or a copy of the company's Certificate of Incorporation.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Copies of documents should be authenticated by a banks' senior staff after reviewing and verifying the original documents. Only copies certified and stamped by governmental bodies/authorities can be relied upon by banks. Authenticated copies from attorneys or other third parties are not accepted unless original copies are obtained.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Each natural or legal person having a real interest in any of the activities of financial institutions, even if the transaction is conducted via another natural or legal person acting as a trustee, a proxy or under any other capacity, should provide documentation to verify identity.

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	None stated in local regulations or guidance.

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	None stated in local regulations or guidance.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	The law states that financial institutions and other entities shall take special customer due diligence measures when a customer (or an individual acting on their behalf) or a beneficiary is identified as a PEP.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	None stated in local regulations or guidance.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	No.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	None stated in local regulations or guidance.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	SARs are made directly to regulators as specified in A3 above.

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, as per the AML Egyptian Law there is such an obligation.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, as stated in the Egyptian AML Law (Anti Money Laundering Law - Law # 80 for year 2002).

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes - as stated in the Egyptian AML Law (Anti Money Laundering Law - Law # 80 for year 2002).

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Egypt does not have a law which regulates the protection of personal data. However, there are some piecemeal provisions in connection with data protection in different laws and regulations in Egypt. Constitutional principles concerning individuals' right to privacy under the Egyptian Constitution as well as general principles on compensation for unlawful acts under the Egyptian Civil Code govern the collection, use and processing of personal data.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	This is only applicable to Banks as enforced by the Laws of the Central Bank of Egypt.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	The Egyptian Penal Code no. 58/1937 imposes criminal punishment for unlawful collection of images or recordings for individuals in private places. Some other laws provide for protection and confidentiality on certain data, such as the Egyptian Labour Law no. 12/2003 (confidentiality of the employee's file information including punishment and assessment) and the Egyptian Banking Law no. 88/2003 (confidentiality of client and account information). Egyptian Civil Status Law no. 143/1994 provides for the confidentiality of citizens' civil status data. The Executive Regulations of Mortgage Finance Law no. 148/2001 issued by virtue of Cabinet Decree no. 1/2001 as amended by Prime Minister Decree no. 465/2005 has a similar clause which provides for the confidentiality of the data of the clients of mortgage finance companies. The Mentally Disordered Care Law no. 71/2009 has the same clause on confidentiality of the patient's data. The New Constitution has been promulgated in December 2012 and has replaced all the previous Constitutional Declarations issued by the Armed Forces Supreme Council and the President of the Arab Republic of Egypt. The New Constitution has not defined data protection. However, it referred to the legislative authority to regulate the communication of data in a manner that does not encroach upon the privacy of citizens, their rights and National Security.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	N/A



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Ethiopia

Key contact: Muniu Thoithi
Email: muniu.thoithi@ke.pwc.com
Tel: +254 (20) 2855684

Postal address: PwC Tower,
Waiyaki Way, Westlands,
Nairobi, Kenya

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The first AML laws were gazetted on 16 Dec 2009, implementation of a preventive system began in 2012.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	Prior to the establishment of an AML framework in Ethiopia, the revised penal code of 2005 had criminalized money laundering.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) the Financial Intelligence Centre ("FIC"), established in 2009 under the National Bank of Ethiopia, is the supervisor of financial institutions with regard to AML obligations. The FIC began limited operations in 2011 and is designated as the central authority for handling money laundering, terrorist financing, and other related matters in the country (http://www.nbe.gov.et/); b) the FIC also regulates insurance companies and microfinance institutions; and c) the Ministry of Mines (http://www.mom.gov.et) supervises dealers in precious metals and stones and the Ministry of Urban Development, Housing and construction (http://www.mwud.gov.et/) regulates real estate agents.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes. The National Bank of Ethiopia has established Customer Due Diligence Directives for banks (http://www.nbe.gov.et/pdf/directives/bankingbusiness/sbb-46-10.pdf).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. Proclamation no 680 – 2013 provides for enhanced customer due diligence where there is a higher risk of money laundering or terrorist financing and simplified customer diligence in the cases where there is a lower risk of money laundering and terrorist financing. Under the Customer Due Diligence directives issued by the National Bank of Ethiopia, banks are required to perform enhanced due diligence on high risk categories of customers, business relationships or transactions.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	A mutual evaluation report took place in May 2015 and was adopted as the first of its kind by Eastern and South African Anti-Money laundering group ("ESAAMLG") in Arusha, Tanzania on 5 Jun 2015. The report is accessible here (http://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/WB-ESAAMLG-Mutual-Evaluation-Report-Ethiopia-2015.pdf).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	The proclamation details that the FIC will establish a minimum threshold, which is currently the equivalent of USD10,000. Banks are required to undertake customer due diligence procedures when carrying out occasional cash transaction with a customer, which exceed Birr 200,000 (approx. USD10,000) or equivalent in other foreign currencies; this shall include situations where the transaction is carried out in a single operation or in several operations that appear to be linked or structured.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	a) individuals identification requirements include: a. given or legal name and all other names used; b. permanent address; c. telephone number, fax number and email address if available; d. date and place of birth if possible; e. nationality; f. occupation, public position held and/or name of employer; and g. signed statement certifying accuracy of information given. b) legal entities identification requirements include: a. name; b. legal form; c. some form of official identification (Tax identification Number if available); d. address; e. names of Directors and CEO if applicable; f. provisions regulating the power to bind the legal person or arrangement; g. board resolution authorizing the representative to open an account; and h. identification of those with authority to operate an account.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Institutions are required to verify documents from independent sources, however, no specific requirements around the verification are given.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Banks are required to identify the ultimate beneficiaries of accounts using relevant information or data from a reliable source such that they are satisfied that they know who the beneficial owner is/are. Banks are required to determine, for all customers, whether the customer is acting on behalf of another person, and then take reasonable steps to obtain sufficient identification data to verify the identity of that other person.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	a) where the customer is a regulated bank or other financial institution subject to AML and Counter Terrorist Financing laws and regulations; and b) credit/debit card transactions for standard customers provided they are not used as tools to effect a money transfer.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	a) complex transactions; b) unusually large transactions; c) unusual patterns of transactions; d) politically exposed persons; e) non-residents; f) personal asset holding vehicles e.g. trusts; g) transactions with no apparent economic or lawful purpose; h) relationships/Transactions with persons from jurisdictions that have known deficiencies in AML and terrorist Financing Strategies; and i) companies that have shares in bearer form.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Under the Customer Due Diligence directives issued by the National Bank of Ethiopia, all new business relationships with PEPs must be approved by senior management of the entity. For existing relationships, if a customer becomes a beneficial owner and is subsequently found to be, or subsequently becomes a politically exposed person, continuation of a business relationship with such person shall be approved by a member of senior management of the bank. Banks are required to undertake reasonable steps to establish the source of wealth and funds for customers and beneficial owners identified as PEPs.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	a) for cross border correspondent banking, in addition to normal due diligence, banks are required to: a. gather sufficient information of the correspondent institution to understand their nature of business and establish from publicly available information whether the institution has been subject to AML investigation or regulatory action. b. access their AML and combating terrorism controls c. obtain approval from senior management d. document the respective AML and combating terrorism responsibilities for each party b) for payments through accounts, banks have to be satisfied that: a. the correspondent institution has done all due diligence checks b. the correspondent institution shall provide upon request relevant customer identification data c) banks shall satisfy themselves that respondent financial institutions in foreign countries do not allow business relationship with shell banks.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	None specified.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The Financial Intelligence Center ("FIC") under the National Bank of Ethiopia (http://www.nbe.gov.et/).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes. The requirement under the National Bank of Ethiopia directives is that all cash deposits or withdrawals exceeding Birr 200,000 (approx. USD10,000), or its equivalent in other foreign currency, should be reported to the FIC.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Yes. Obligatory reporting is applicable to withdrawals/deposits in excess of USD10,000.

Q22.	Are there any penalties for noncompliance with reporting requirements e.g. tipping off?
A22.	Yes. Under no circumstances shall a financial institution, or designated non-financial institution and professions, disclose to customers or third parties information concerning suspected AML and Financing of terrorism information: a) a person convicted of noncompliance with reporting requirements is liable to rigorous imprisonment for three to five years and a fine from ETB5,000 to 10,000 (approx. USD300); and b) legal persons are liable to a fine equal to ten times that of a Natural person.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Suspicious transactions are required to be postponed until they are reported to FIC who will then provide a way forward, except when it is impossible or doing so would frustrate investigative efforts.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Not specifically. However, the competent authorities ¹ are required to provide necessary information to competent authorities of other states.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

¹ Financial Intelligence Centre, National Intelligence and Security Service, the police, Public Prosecutor or other investigative body, Ethiopian Revenue and Customs Authority or any concerned regulatory body.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	No.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	The National Bank of Ethiopia administers access to the Credit Information Sharing System. This is available to banks upon request.

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Under the AML proclamation, there's no protection given to customers or clients if the confidential information pertains to "investigation or prosecution of crime involving money laundering or financing of terrorism or for taking regulatory measures." Article 6 of the proclamation, provides for no obligation of confidentiality imposed by other laws shall affect any obligation under this Proclamation to report or furnish information. This holds true for most of the banking and micro-finance institutions in Ethiopia. However, the duty of disclosure also includes the following institutions; a) money transfer agent or a foreign exchange bureau; b) a financial leasing company; c) the Ethiopian Revenues and Customs Authority; d) a notary office or an organ empowered to authenticate documents; e) a licensing authority; f) the Ethiopian Investment Agency; g) non-governmental organisations; h) religious institution or other charitable organization; i) an advocate; j) an auditor or a licensed accountant; k) a person engaged in real estate business; l) a dealer in precious metals and gems; and m) a broker, dealer or investment adviser.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Gabon

Key contact: Douty Fadiga
Email: d.fadiga@cm.pwc.com
Tel: +237 77 93 40 70

Postal address: P.O.Box 5689,
Douala,
Cameroon

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	AML law and regulations became effective in 2005 and are only applicable for banks.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include a link to the regulator(s) website
A3.	a) Banking Commission (https://www.beac.int/); b) none; and c) none.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	No.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, an update of the customer database is required.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	No. There is no risk based approach approved by the local regulator.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes. The country has been subjected to a FATF evaluation, but the report is not publicly available.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No. There are no minimum transaction thresholds under which customer due diligence is not required.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The requirements are: a) verification of the identity and address of the customer by reference to official identity papers; b) for legal entities, the verification of legal documents and legal representatives is required; c) public officials require a heightened scrutiny; and d) the bank must collect information to cover the following: anticipated account activity, source of wealth and sources of funds.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	None in practice. Copies of identification documentation are only made by the bank after a visual check. Independent verification is not required.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The requirements are: a) obtain information on the beneficial owner; and b) verification of the identification and the address of the professional intermediary.

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Customer due diligence arrangements are reduced for low value transactions.

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Customer due diligence is enhanced for unusual or suspicious activities/transactions.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	For a PEP, the bank’s senior management may give authorisation before opening an account. The transactions in their accounts require heightened scrutiny.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Banks must acquire information on the compliance of their correspondent with AML regulations. The relationship must not be established if the correspondent is not compliant with AML regulations.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	For a non face-to-face relationship, a bank must consider the need to perform independent verification.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	National Agency for Financial Investigation (“ANIF”): http://www.anif.ga/

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	There is an obligation to report on transactions where the identity of the beneficiary or the originator is suspicious.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	No.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	No.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes.

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Ghana

Key contact: Eric Nipah
Email: eric.nipah@gh.pwc.com
Tel: +233 21 761500

Postal address: No 12 Airport City, UNA Home,
3rd Floor, PMB CT42,
Cantonments, Accra, Ghana

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2008. The Anti-Money Laundering Act of 2008 (Act 749), and the Anti-Money Laundering Regulations 2008 (LI 1925).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	Banks were to comply with the Bank of Ghana and/or parent bank's KYC policies/procedures. No financial intelligence centre reporting requirements. Bank of Ghana Supervision Department (and also security agencies and Serious Fraud Office) played the quasi-role of a centre investigating "suspicious" transactions.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non-financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	Financial Intelligence Centre (http://www.fic.gov.gh/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes (http://www.fic.gov.gh/).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No, however banks are encouraged to ensure that due diligence on customers is a continuous exercise.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	In Oct 2012, Ghana was removed from the Financial Action Task Force (FATF) blacklist. See (http://www.fic.gov.gh/sites/all/themes/biz/fic%20news/FIC%20ANNUAL%20REPORT%202012%20-%20Final.pdf).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, the equivalent of USD10,000.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Information required for individuals includes: legal name and other names, location of client, telephone, fax numbers, mailing address, date and place of birth, nationality, hometown, occupation, position held and employer's name, identity documents, nature of the business relationship and signature. Legal entities: They require a registered name, location address, head office, mailing address, contact phone and fax numbers, original or certified copy of regulations, certificate of business registration and commencement of business, copy of latest auditor's report and accounts, annual report filed with the Registrar General and names, location and mailing addresses of directors.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Identity shall be verified whenever a business relationship is to be established, on account opening or during one-off transaction or when series of linked transactions take place.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	When one person is acting on behalf of another, the obligation is to obtain sufficient evidence of the identities of the two persons involved. In consortium lending, the lead manager/agent shall supply a confirmation letter as evidence that he has obtained the required identity.

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	None.

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence is required when dealing with PEPs.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Additional due diligence is required for PEPs. Senior management approval must be sought before establishing a relationship with such a person. It is also a requirement to establish the PEP's source of wealth/source of funds and the beneficial owners.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	If the broker or other introducer is a regulated person or institution (including an overseas branch or subsidiary) from a country with equivalent legislation and financial sector procedures, and the broker or introducer is subject to anti-money laundering rules or regulations, then a written assurance can be taken from the broker that he/she has obtained and recorded evidence of identity of any principal and underlying beneficial owner that is introduced.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	No.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	The specific requirements are in process of being formalised by the Bank of Ghana.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Financial Intelligence Centre (http://www.fic.gov.gh/).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, reporting should not be limited to Suspicious Transaction Reports ("STRs") alone.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Yes.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	The Act requires the bank to report such acts to the Financial Intelligence Centre, Bank of Ghana and their External Auditors.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) as soon as a transaction is noted; b) Financial Intelligence Centre primarily; c) this is reported in the "long form" report to the Bank of Ghana.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) the External Auditors are required to review the "Accounts Opening Procedures" used by the bank; b) all reports sent to the Financial Intelligence Centre are reviewed; c) yes.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	No.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes. They can only be obtained by a court order.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Kenya

Key contact: Muniu Thoithi
Email: muniu.thoithi@ke.pwc.com
Tel: +254 (20) 2855684

Postal address: PwC Tower,
Waiyaki Way, Westlands,
Nairobi, Kenya

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2010. The Proceeds of Crime and Anti-Money Laundering Act 2009 ("POCAMLA") was enacted on 11 Dec 2009, and came into effect on 28 Jun 2010.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	There was not a specified AML regime in existence previously. However, the 1994 Narcotic Drugs and Psychotropic Substances Control Act prohibits concealing or transferring the proceeds of drug trafficking.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) the Financial Reporting Centre ("FRC") is designated as the competent authority for supervising financial institutions for compliance with AML obligations. The FRC became operational in Apr 2012 (http://frc.go.ke/); b) the Capital Markets Authority ("CMA") regulates AML controls for listed entities and entities licenced by the CMA; the Central Bank of Kenya regulates banks in Kenya and the Insurance Regulatory Authority regulates the insurance industry; and c) the FRC is designated as the competent authority for designated non-financial businesses and professions: Casinos, real estate agencies, dealers in precious stones and metals and accountants are designated as Designated Non-Financial Businesses or Professions ("DNFBP") under POCAMLA. Lawyers, notaries and trust and company service providers are not subject to the requirements under POCAMLA.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The Central Bank of Kenya issued a Guideline on Proceeds of Crime and Money Laundering Prevention which became effective on 01 Jan 2006. The Central Bank also issued Foreign Exchange Bureau Guidelines which in part addresses AML requirements, which became effective on 01 Jan 2007 (www.centralbank.go.ke). The FRC is empowered to develop regulations on anti-money laundering and to provide guidance to support the implementation of POCAMLA. The FRC website also includes guidance on AML issues (http://frc.go.ke/). The Insurance Regulatory Authority issued guidelines to the insurance industry on implementation of POCAMLA in Jun 2011. The purpose of the guidelines is to provide guidance on detection, deterrence and reporting incidences of possible crimes related to proceeds of crime and money laundering by the insurance industry (http://www.ira.go.ke/attachments/article/63/Anti-Money%20Laundering%20Guidelines1.pdf). The Capital Markets Authority ("CMA") on 01 Oct 2015 issued a guideline on AML and combating financing of terrorism in the capital markets (http://www.cma.or.ke/).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. POCAMLA subsidiary legislation 2013 requires organisations classified as reporting institutions by the Act to conduct on-going due diligence on its customers and develop risk based systems and procedures. Additionally, the CMA guidelines specify that enhanced due diligence to be carried out for customers with higher risk of money laundering and simplified due diligence for customers for lower risk customers.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	A Mutual Evaluation Report on Kenya was undertaken by the Eastern and Southern Africa Anti-Money Laundering Group ("ESAAMLG") and published in Sept 2011. The report can be accessed here: http://www.esaamlg.org/userfiles/Kenya_Mutual_Evaluation_Detail_Report(2).pdf The FATF's Public Statement of 18 Oct 2013 identified Kenya as a jurisdiction with strategic AML/CFT deficiencies that has not made sufficient progress in implementing its action plan within the agreed timelines. The Statement can be accessed here: http://www.fatf-gafi.org/countries/j-m/kenya/documents/fatf-public-statement-oct-2013.html#kenya On 27 Jun 2014, FATF noted Kenya's significant progress in improving its AML/CFT regime and noted that Kenya had established the legal and regulatory framework necessary to meet its commitments in its action plan regarding the strategic deficiencies that the FATF had identified in Feb 2010. Kenya is therefore no longer subject to FATF's monitoring process under its on-going global AML/CFT compliance process. The statement can be accessed here: http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-june-2014.html

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, for telegraphic transfers and travellers cheques. A foreign exchange bureau should not sell foreign currency or travellers cheques in excess or equal to the equivalent of USD10,000 per customer per day without seeing and recording a valid identification document.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: a) an official record such as passport, birth certificate, identity card or driving licence; b) address verified by a referee or utility bill; c) source of income; and d) written confirmation from the customer's previous bank attesting to their identity and account relationship history (bank referee). Corporates / Firms: a) Certificate of Registration, Certificate of Incorporation, Partnership Deed, Memorandum and Articles of Association; b) Board Resolution stating authority to open accounts and designating persons having signatory authority; c) identity the address of the chairman, managing director, or the general partner and at least one limited partner for partnerships, or the principal owner for sole traders; d) audited financial statements for corporations; and e) where applicable, references from the customer's previous bank.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Independent means of verifying these details include requesting sight of a recent utility bill, local authority tax bill or institution statement (care should be taken to check that the documents offered are originals in order to guard against forged or counterfeit documents); checking a local telephone directory (for businesses); making telephone contact with the applicant on an independently verified home or business number; verifying salary details appearing on a recent bank account statement; or with the customer's consent, calling their employer's personnel department to confirm employment etc. Documents must be certified by suitable third parties and confirmation from the previous bank obtained where possible. Suitable third parties include advocates, notaries public, commissioners for oaths, judges, magistrates and certain government officials.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Local guidance requires institutions to have full disclosure of beneficial owners or controlling persons behind nominee accounts.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	None stated in POCAMLA or guidance. According to CMA guidelines, simplified due diligence is applicable to lower risk customers including: a) persons employed by a legitimate employer; b) customers with a positive reputation (well-known reputable public or private company); and c) public entities.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Under the POCAMLA regulations, enhanced due diligence measures are required with respect to persons and business relations and transactions carrying a high risk and with persons established in jurisdictions that do not have adequate systems in place to combat money laundering. Under the CMA guidelines, enhanced due diligence is required where: a) a customer is a politically exposed person; b) there is a complex relationship, including use of corporate structures, with no legitimate commercial rationale; c) undue secrecy/ use of numbered accounts in a transaction; d) involvement in cash intensive business; e) high risk nature, scope and location of business activities; and f) origin of wealth is unverifiable.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Under the POCAMLA subsidiary regulations 2013, additional due diligence procedures required for PEPs are as follows: a) obtain approval from senior management to transact or establish the relationship with that person; b) take adequate measures to establish the source of wealth and the source of funds which are involved in the proposed business relationship or transaction; c) obtain information on the immediate family members or close associates of the person who may have transaction authority over the account; d) determine the purpose of the transaction or account and the expected volume and nature of account activity; e) review public sources of information on the politically exposed person; and f) once the account has been established, conduct enhanced ongoing monitoring of the relationship.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	According to POCAMLA Regulations 2013 Section 24, a financial institution intending to establish a correspondent financial relationship either as the correspondent financial institution or the respondent financial institution shall undertake the following measures before establishing a business relationship: a) gather sufficient information about the correspondent financial institution regarding the nature of its business activities; b) determine, from available information, the reputation of the correspondent financial institution and the quality of its supervision; c) determine the quality of anti-money laundering regulation in the correspondent financial institution's jurisdiction or country of domicile; d) assess the correspondent financial institution's anti-money laundering controls; e) obtain approval from senior management before establishing a new correspondent financial institution relationship; f) in respect to the correspondent financial institution's customers, be assured that it verifies the identity of its customers and conducts on-going monitoring; and g) verify the ownership and management structures of the correspondent financial institution including whether a politically exposed person has ownership or control of the financial institution.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes. According to POCAMLA guidelines, relationships with shell banks are specifically prohibited. Reporting institutions are prohibited from: a) opening a foreign account with a shell bank; b) permitting its accounts to be used by a shell bank; or c) enter into or continue a correspondent financial relationship with— a. a shell bank; or b. a respondent financial institution that permits its account to be used by a shell bank.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	As with face-to-face verification, the procedures to check identity must ensure that a person bearing the name of the applicant exists and lives at the address provided and that the applicant is that person he claims he is. Local guidance requires the following due diligence: requesting sight of a recent utility bill, local authority tax bill, institution statement or checking a local telephone directory (for businesses). In addition, satisfactory evidence of personal identity can be obtained by a number of means, including telephone contact with the applicant on an independently verified home or business number, employer's personnel department confirming employment by verbal confirmation on a listed number (with the customer's consent), and salary details appearing on a recent bank or building society statement.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The Act requires that SARs are made to the Financial Reporting Center (http://www.frc.go.ke/contact-us). SARs can also be made to the Central Bank of Kenya (www.centralbank.go.ke).
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	The Act requires monitoring on an ongoing basis all complex, unusual, suspicious, and large or other transactions, and upon suspicion, it should be reported accordingly. Additionally, the Act requires that reporting institutions file reports with the FRC for all cash transactions equivalent to or exceeding USD10,000 or its equivalent in any other currency carried out by it, whether or not the transaction appears to be suspicious.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Section 5 of POCAMLA makes it an offence to willfully fail to report a suspicion regarding the proceeds of crime. Section 8 of POCAMLA makes tipping off an offence. Section 16 of POCAMLA provides that contravention of either section 5 or 8 is, on conviction, liable in the case of a natural person to imprisonment for a term not exceeding 7 years, or a fine not exceeding KES2.5m (approx. USD24,915), or to both and in the case of body corporate to a fine not exceeding KES10m (approx. USD99,660) or the amount of the value of the property involved in the offence, whichever is the higher. In addition to the above, the President of Kenya in his speech of 24 Nov 2015, issued the following directives in relation to non-compliance with AML regulations: a) banks that break anti money laundering laws and regulations will, at a minimum, lose their banking licenses; b) directors and senior officials of such banks were put on notice that they will be pursued relentlessly, individually and collectively, in accordance with the law should they commit offences under AML laws and regulations; and c) the Central Bank and the Financial Reporting Centre were directed to strengthen their supervision capabilities over banks.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No. However, the reporting institution is required to keep all records relating to that transaction and ensure that its reporting obligations under the Act are discharged.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	According to the Act, anti-money laundering measures consistent with the POCAMLA and the subsidiary regulations of POCAMLA apply to foreign subsidiaries and branches. Where the minimum requirements of the host country are less strict than those applicable in Kenya, a reporting institution is required to ensure that its branches and subsidiaries apply the requirements of the Act and these Regulations to the extent that the laws of the host country permit.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	No. The Data Protection Bill 2012 is yet to be enacted into law. The bill seeks to give effect to Article 31(c) and (d) of the Kenya Constitution; to regulate the collection, retrieval, processing, storing, use and disclosure of personal data and for connected purposes.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	POCAMLA prohibits the disclosure of confidential information without the written permission of the Attorney-General unless to a court of law or for the purpose of performing functions stipulated in the Act.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No. A bank is under an obligation of secrecy under the Banking Contract regarding its customers' affairs. This obligation is a legal obligation arising out of the contract.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Mauritius

Key contact: Avinash Ramessur / Razi Daureeawo
Email: avinash.ramessur@mu.pwc.com /
razi.daureeawo@mu.pwc.com
Tel: +230 404 5000

Postal address: PricewaterhouseCoopers Ltd,
18, Cybercity,
Ebene, Mauritius

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Financial Intelligence and Anti Money Laundering Act 2002 ("FIAMLA") and the Prevention of Corruption Act 2002 ("POCA") were enacted in 2002. The FIAMLA Regulations were introduced in 2003.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	The Financial Intelligence Unit ("FIU") is the central agency in Mauritius responsible for oversight of AML controls and works in conjunction with the investigatory and supervisory authorities of each sector: a) The Bank of Mauritius ("BOM") (https://www.bom.mu/pdf/Legislation_Guidelines_Compliance/Guidelines/GUIDANCE_AML-CFT20140715.pdf); b) The Financial Services Commission ("FSC") (http://www.fscmauritius.org/being-supervised/aml-cft.aspx); and c) The FIU (http://www.fiumauritius.org/index.php?option=com_content&view=article&id=29%3Acasinos-gaming-house-a-interactive-gambling-totalisator-or-bookmaker&catid=2&lang=en).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes. See (http://www.fiumauritius.org/index.php?option=com_content&view=article&id=108&Itemid=11&lang=en) and (http://www.bom.mu/?ID=90721).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, for example the guidelines issued by the FSC for Effective Customer Risk Assessment. See (http://www.fscmauritius.org/media/116497/aml_cft_v4.pdf) and (https://www.bom.mu/pdf/Legislation_Guidelines_Compliance/Guidelines/GUIDANCE_AML-CFT20140715.pdf) (refer to paragraph 6.21, 6.103 & 6.104 for risk-based approach guidelines).

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No, the last assessment exercise was done in 2008 for both FATF and IMF. See (http://www.fatf-gafi.org/documents/documents/mutualevaluationofmauritius.html).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, every financial institution, bank or cash dealer is required to carry out customer due diligence for transactions exceeding MUR350,000 or an equivalent amount in foreign currency USD10,000).

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Where the customer is an individual, the original or a certified copy of an official, valid document containing details of his current permanent address, a recent photograph of him and such other documents as may be required. Legal Entities: Every relevant person shall establish and verify: a) the identity and the current permanent address of an applicant for business; and b) the nature of the applicant's business, his financial status and the capacity in which he is entering into the business relationship with the relevant person.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Certified copies should be provided.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Financial institutions are required to identify and verify (to the same level as a personal customer) all UBOs who directly or indirectly hold 20% or more of the capital or voting rights of a company. Specific requirements apply to banks and licensees of the FSC. Broadly, financial standing, qualifications and reputation, financial integrity and character would be considered.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Guidance issued by the regulatory authorities suggests that for financial institutions and public companies listed on a recognised, designated and approved stock / investment exchanges, simplified CDD measures can be applied in cases where a low Money Laundering and Terrorism Financing ("ML/TF") risk has been demonstrated.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Guidance issued by the regulatory authorities provides for specific circumstances where enhanced CDD should be applied. For example, enhanced due diligence must be applied where the ML/TF risk is high or where an applicant to a bank has been rejected by another bank.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Enhanced due diligence should be applied by financial institutions in connection with PEPs, including: a) obtaining further customer due diligence information (identification and relationship information) from either the customer or independent sources (such as the internet, public or commercially available databases); b) verifying additional aspects of the customer due diligence information obtained; c) obtaining additional information required to understand the purpose and intended nature of such a business relationship; d) taking appropriate and reasonable measures to establish the source of the funds and source of wealth of the customer, any beneficial owner and underlying principal; and e) carrying out more frequent and more extensive ongoing monitoring on such business relationships including setting lower monitoring thresholds for transactions connected with such business relationships.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The Licensee should: a) gather sufficient information about their correspondents to understand fully the nature of the correspondent's business. Factors to consider include information about the correspondent's management, major business activities, where they are located; their money-laundering prevention and detection efforts; and the identity of any third party entities that use the correspondent services; b) determine from publicly available information the reputation of the institution and quality of the institution's regulation and supervision, including whether it has been subject to money laundering or terrorist financing investigation or regulatory action; c) assess the institution's AML/CFT controls and ascertain that they are adequate and effective and establish correspondent relationships with foreign financial institutions only if they are satisfied that the foreign financial institutions are effectively supervised by the relevant authorities and have effective customer acceptance and KYC policies; d) obtain approval from senior management before establishing new correspondent relationships; and e) document the respective AML/CFT responsibilities of each institution.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, financial institutions should refuse to enter into or continue a correspondent relationship with a financial institution incorporated in a jurisdiction in which the correspondent has no physical presence and which is unaffiliated with a regulated financial group (i.e. it may involve a shell financial institution).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In accepting business from non-face to face customers, financial institutions must apply effective customer identification procedures as well as specific and adequate measures to mitigate the high risk posed by non-face-to-face verification of customers. The Code on the Prevention of Money Laundering and Terrorist Financing enacted by the FSC stipulates that for non-face to face business relationships, additional steps (Enhanced Due Diligence) in relation to identification and verification is required.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	There is an obligation on every bank, financial institution, cash dealer or member of a relevant profession or occupation to make a report to the FIU of any transaction which they have reason to believe may be a suspicious transaction (http://www.fiumauritius.org/index.php).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 – 354 SARs GDP (in current prices): 2013 – USD11,931.8m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD33.7m of GDP.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	The FIAMLA imposes only a duty to report STRs. However, the POCA imposes an obligation upon a public officer to report any act of corruption that he suspects to have happened within or in relation to that public body to the Independent Commission Against Corruption ("ICAC").

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

*GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes. Offences for failing to report an STR and tipping off are punishable by a fine not exceeding MUR1m (approx. USD28,620) and imprisonment for a term not exceeding five years. Supervisory authorities may take regulatory action in the event of non-compliance.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	As far as we are aware, there is no requirement to use automated suspicious transaction monitoring technology.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	There is no specific provision under domestic law.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Mauritius is a member of the Egmont Group and has signed a number of Memorandum of Understandings on exchange of information with its foreign FIUs.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Guidelines from the regulatory authority require that the institution review their practices as part of their general external and internal audit processes.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	There is no requirement for an independent external audit report, however financial institutions have to make a report on themselves to the BoM: a) reports are issued on a yearly basis; b) reports are submitted to the Bank of Mauritius; and c) no, the report is not part of the Financial Statement.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	As above, there is no requirement for an independent external audit report, however financial institutions have to make a report on themselves to the BoM. There are no specific requirements for the content of an external report on a bank's AML systems and controls: a) yes, sample testing of KYC files is required; b) no, sample testing of SAR reports is not required; and c) this would be part of the review of KYC review.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes: a) we are governed by the Data Protection Act 2004. Per the Act, personal data refers to (i) data which relate to an individual who can be identified from those data or; (ii) data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion; b) the Data Protection Act 2004 applies only to personal data; and c) Yes, "sensitive personal data" means personal information concerning a data subject and consisting of information as to: a. racial or ethnic origin; b. political opinion or adherence; c. religious belief or other belief of a similar nature; d. membership to a trade union; e. physical or mental health; f. sexual preferences or practices; g. the commission or alleged commission of an offence; and h. any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Per the Data Protection Act 2004, no data controller shall, except with the written authorisation of the Commissioner, transfer personal data to another country. No personal data shall be processed, unless the data controller has obtained the express consent of the data subject. Notwithstanding the above, personal data may be processed without obtaining the express consent of the data subject where the processing is necessary: a) for the performance of a contract to which the data subject is a party; b) in order to take steps required by the data subject prior to entering into a contract; c) in order to protect the vital interests of the data subject; d) for compliance with any legal obligation to which the data controller is subject; e) for the administration of justice; or f) in the public interest.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No. There is a general confidentiality obligation upon banks (s64 Banking Act 2004) to keep the information on their customers confidential. Such an obligation may only be lifted by way of a court order.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Nigeria

Key contact: Eyita Otudor
Email: eyita.otudor@ng.pwc.com
Tel: +234 1 2711700, +234 (0)803 326 958

Postal address: Plot 252E
Muri Okunola Street
Victoria Island, Lagos, Nigeria

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Money Laundering and Prohibition Act was enacted in 2004 but has since been repealed by the Money Laundering (Prohibition) Act 2011 (amended in 2012).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) Central Bank of Nigeria ("CBN") (http://www.cenbank.org/); b) Nigerian Financial Intelligence Unit ("NFIU") (www.nfiu.gov.ng); National Insurance Commission ("NAICOM") (www.naicom.gov.ng); and c) SCUML (Special Control Unit for Money Laundering) (http://www.scuml.org/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	a) CBN (http://www.cenbank.org/out/2014/fprd/aml%20act%202013.pdf); b) NFIU (http://nfiu.gov.ng/index.php/resources/cir/guidadv); c) SCUML: None; d) Securities and Exchange Commission ("SEC") (http://www.sec.gov.ng/files/AML-CFT_SEC%20REGULATIONS%20GAZETTED.pdf); e) Nigerian Stock Exchange ("NSE") (http://www.nse.com.ng/regulation-site/Circular%20to%20Dealing%20Member%20Firms/Regular%20Internal%20Review%20of%20Records%20-%20January%2017,%202013.pdf#search=laundering); and (http://www.femiamao.com/nse.html.pdf); and f) NAICOM (http://naicom.gov.ng/content?id=26).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Nigeria is a member of the Inter-Governmental Action Group Against Money-Laundering in West Africa ("GIABA"). GIABA is a FATF-Style Regional Body ("FSRB") that works in conjunction with FATF to monitor its member countries' progress in implementing FATF standards. Nigeria's first Mutual Evaluation report was issued in May 2008. In subsequent years, GIABA conducted follow-up evaluations and issued follow-up reports. The follow-up evaluation reports in the last three years. May 2015, May 2014 and May 2013 are listed below: a) (http://www.giaba.org/media/f/932_7th%20FUR%20Nigeria%20-%20English.pdf); b) (http://www.giaba.org/media/f/838_6th%20FUR%20Nigeria%20-%20English.pdf); and c) (http://www.giaba.org/media/f/832_5th%20FUR%20Nigeria%20-%20English.pdf).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: a) government issued means of identification; b) passport photograph; c) public utility bill; and d) visitation. Corporates: a) company registration documents (memorandum of association, articles of association, shares allotment certificate, particulars of directors, certificate of incorporation, person appointed as company secretary, registered office address etc.); b) details of directors, passport photographs and means of identification; c) details of promoters; d) public utility bills showing either registered address or business address; e) Special Control Unit Against Money Laundering ("SCUML") registration certificate; and f) corporate search. See (http://www.cenbank.org/out/2014/fprd/aml%20act%202013.pdf).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	a) ascertaining that the documents provided are certified true copies; and b) corporate searches with the Nigerian Corporate Affairs Commission ("CAC") (for identification documents relating to company registration).
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Beneficial owners who control more than 5% of shares in a company or have significant influence over a company should be identified directly through an identification check through official databases (e.g. a Customer Identification Program) or through other documents received that can verify the identity of the beneficial owner.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence arrangements are available where the prospect is a(n): a) financial institution; b) public company; c) government ministry / parastatal; d) life insurance policy account; e) insurance policy for pension scheme; f) beneficial owner of pooled accounts held by designated non-financial business and professions; or g) unbanked person intending to be financially included through the CBN financial inclusion initiative. Financial inclusion is an initiative of the CBN to ensure that all unbanked persons (e.g. peasants, hawkers, market traders etc.) can open and operate bank accounts but under reduced/simplified due diligence arrangements. See (http://www.cenbank.org/out/2013/ccd/3%20tiered%20kyc%20requirements.pdf) and (http://www.cenbank.org/out/2014/fprd/aml%20act%202013.pdf).
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Where the prospective relationship is a: a) Politically Exposed Person ("PEP"); b) non-resident customer; c) private banking customer; d) legal person or legal arrangement such as a trust; or e) a company that has nominee shareholders. See (http://www.cenbank.org/out/2014/fprd/aml%20act%202013.pdf).
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	There are no circumstances stated in the law or relevant regulations.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Examples of such enhanced CDD measures include (but are not limited to): a) obtaining additional information on the customer; b) obtaining additional information on the intended nature of the business relationship, and on the reasons for intended or performed transactions; c) obtaining information on the source of funds or source of wealth of the customer; and d) conducting enhanced monitoring of the business relationship, e.g. by increasing the number and timing of controls applied and identifying patterns of transactions that warrant additional scrutiny.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Additional due diligence is required for non-face-to-face transactions where the following are involved: a) cross border transfers; b) mobile banking; c) telephone banking systems; d) debit and credit card transactions; and e) where there is a suspicion of money laundering in relation to that customer, or where there is a material change in the way that the customer's account is operated which is not consistent with the customer's business profile. See (http://www.cenbank.org/out/2014/fprd/aml%20act%202013.pdf).

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	NFIU (www.nfiu.gov.ng).
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes. Financial institutions are required to report to the NFIU in writing within seven days any single transaction lodgement or transfer of funds in excess of: a) NGN5m (approx. USD25,400) or its equivalent, in the case of an individual; or b) NGN10m (approx. USD50,790) or its equivalent in the case of a body corporate. A person other than a financial institution may voluntarily give information on any transaction lodgement or transfer of funds in excess of: a) NGN1m (approx. USD5,080) or its equivalent, in the case of an individual; or b) NGN5m (approx. USD25,400) or its equivalent in the case of a body corporate. Any financial institution that contravenes the provision of this section shall be liable to a fine of not less than NGN250,000 (approx. USD1,270) and not more than NGN1m (approx. USD5,080) for each day the contravention continues. See (http://www.cenbank.org/out/2013/fprd/amendment%20of%20anti-money%20laundering.pdf).
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Yes. Below the thresholds as stipulated in A20, transactions do not need to be reported according to the AML law. However, the threshold should be applied by taking into consideration all other qualitative characteristics of transactions and customers as stipulated by the AML law.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	No.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	No.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.



'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



South Africa

Key contact: Roy Melnick
Email: roy.melnick@za.pwc.com
Tel: +27 11 797 4064

Postal address: 2 Eglin Road
Sunninghill, 2157,
South Africa

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	AML Laws: The Prevention of Organised Crime Act No. 121 of 1998. The Financial Intelligence Centre Act, 38 of 2001 ("FICA") was enacted in 2001. The Financial Intelligence Centre Amendment Act, 2008 (Act No. 11 of 2008) was released in Aug 2008 and became effective on 01 Dec2010. Section 28 and Section 51 of FICA – the cash threshold reporting provisions - came into operation in Oct 2010. Regulations: The Money Laundering and Terrorist Financing Control regulations were published in Dec 2002 and have been amended on various occasions, the most recent being in Nov 2010. Guidance Notes: Guidance Notes issued by the FIC have since Mar 2013 been declared as authoritative in nature, guidance must be applied or demonstrate an equivalent level of compliance. Failure to follow guidance issued by the Centre may result in enforcement action. There are at present 5 Guidance Notes that have been issued by the Centre these include: a) Guidance Note 1 - General Guidance Note Concerning Identification of Clients (not dated); b) Guidance Note 2 - Guidance to Financial Services Industries regulated by the Financial Services Board concerning the meaning of the word "transaction" (18 Jun 2004); c) Guidance Note 3 - Guidance for banks on customer identification and verification and related matters (18 Jul 2005); d) Guidance Note 3A (replaced Guidance Note 3) - Guidance for accountable institutions on client identification and verification and related matters (28 Mar 2013); e) Guidance Note 4 – Guidance on Suspicious Transaction Reporting (14 March 2008); and f) Guidance Note 5 – Guidance on Cash Transaction Reporting (not dated).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The main amendments to FICA do not detract from the original AML requirements but rather clarify areas in the law. The purpose of the amendments are <i>inter alia</i> to clarify the roles and responsibilities of supervisory bodies; authorise the Financial Intelligence Centre and supervisory bodies to conduct inspections; to provide for administrative sanctions and to make further provision for offences. Guidance Note 3A, issued in Mar 2013; rendered Guidance notes authoritative in nature, thus ensuring that accountable institutions adopt a risk based approach and take heed of High Risk clients and enhanced due diligence requirements for these.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	The Financial Intelligence Centre ("FIC") (www.fic.gov.za) fulfils an overarching regulatory role for combating money laundering and terrorist financing. Industry regulators and supervisory bodies provide oversight within the various industries: a) South African Reserve Bank (www.resbank.co.za/); b) Financial Services Board (https://www.fsb.co.za/Pages/Home.aspx); and c) multiple, including: a. Casinos - National Gambling Board (www.ngb.org.za/); b. Real Estate - Estate Agency Affairs Board (www.eaab.org.za/); and c. Attorneys - Law Society (www.lssa.org.za/).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The FICA has issued various guidance notes with regards to AML requirements (https://www.fic.gov.za/SiteContent/ContentPage.aspx?id=15).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes. Banks and other accountable institutions were required to retrospectively identify and verify the identity and other information of all clients that held accounts with them at the time that the law became operational. An accountable institution that had an established business relationship with a client before the FICA took effect may not conclude a transaction in the course of that business relationship, unless it has taken the prescribed steps to establish and verify the identity of the client.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, although the FICA, 38 of 2001 and the regulations do not expressly make reference to a risk-based approach, it is covered in Guidance Note 1 issued by the FIC in Ap 2004 and reinforced by Guidance Note 3A issued in Mar 2013. Guidance Notes were declared to be authoritative in nature at this date and therefore accountable institutions are expected to apply a risk-based approach <i>inter alia</i> in respect of customer relationships. The Act is currently being reviewed to incorporate a risk-based approach; we expect the amended Act to be promulgated during in 2016.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The last FATF Mutual Evaluation conducted on South Africa was finalised in 2008. The applicable report was published on 02 Mar 2008: http://www.fatf-gafi.org/topics/mutualevaluations/documents/mutualevaluationofsouthafrica.html

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No. Due diligence is always required for all client relationships and single transactions, irrespective of the value involved. However the law does make a provision for certain exemptions where a reduced level of due diligence is permitted. These exemptions form part of the FICA regulations and affect various industries.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals (SA residents): An accountable institution must verify the full name, date of birth and identity number of a natural person to an identification document of that person. The residential address must be compared to information that can be used for verification purposes (e.g. a utility bill stating the residential address of the individual). Legal entities: The registered name, registration number, registered address, trading name and the address of the entity as well as the identity of the board of directors of the company and each authorised person. The FICA regulations contain the detail of other requirements pertaining to these as well as other persons/entities (foreign nationals, agents, foreign companies, trusts, partnerships and close corporations).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Although the FICA stipulates that a record must be kept of the identity document, it does not specify the requirements pertaining to authentication. In terms of the guidance notes and best practices, it would be sufficient to review the original identity document and to obtain a copy of a document which is either certified by a Commissioner of Oaths; or where the original has been sighted by an employee of the accountable institution, and an indication of such is made on the copy. Guidance is also provided on non face-to-face verification by the FIC. Where non face-to-face verification is accepted as a means, the verification methods used must be as effective as those that are applied to customers who are available for an interview.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The FICA stipulates, <i>inter alia</i> , that the identity of the client, or if the client is acting on behalf of another person, the person acting on behalf of the client, must be established and verified. The regulations have put in place measures to determine beneficial owners in respect of entities. For example, the particulars of every member and every representative of a close corporation must be obtained. In respect of a company the particulars of its manager and representatives must be provided as well as the particulars of its major shareholders who are able to exercise more than 25% of the votes at a general meeting of the company. In respect of trusts, the identity of the founder, beneficiaries and trustees must be established. The Act is currently being amended to include due diligence requirements for ultimate beneficial ownership; we expect these amendments to be promulgated during 2016.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Depending on the risk profile, the level of due diligence is simplified for low risk clients or in respect of existing clients who are applying for different products. The exemptions, which form part of the FICA regulations, contain details of the circumstances under which reduced or simplified due diligence may be applied. Simplified due diligence applies <i>inter alia</i> to companies listed on approved stock exchanges (exemption 6) and banking products issued to customers subject to particular conditions and thresholds (exemption 17).
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	The FICA Guidance note 3A states that accountable institutions should follow a risk-based approach to customer due-diligence. Clients are given a risk-rating based on various risk factors. High-risk client types, high risk transactions and services warrant enhanced due diligence procedures. Enhanced due diligence is also recommended when the client is identified as a PEP; when non-face-to-face verification is undertaken, if the client is a correspondent bank, money service business, intermediary or an employee account.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Guidance from the FIC defining PEPs stipulates that the bank should conduct enhanced due diligence specifically on PEPs, persons acting on their behalf as well as their families and close associates. The Wolfsberg principles as well as the FATF recommendations are referred to for additional guidance on how to recognise and deal with a PEP. In addition to performing customer due diligence measures, banks should put in place appropriate risk management systems to determine whether a customer, a potential customer or the beneficial owner is a PEP. The Act is currently being amended to include an enhanced definition of PEPs; we expect these amendments to be promulgated during 2016.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The FIC guidance notes provide that banks should pay particular attention when continuing relationships with correspondent banks located in jurisdictions that have poor KYC standards or have been identified by FATF as being "non co-operative". The Wolfsberg principles are referred to which set out the following risk indicators that a Bank shall consider, to ascertain the level of due diligence it will undertake, namely the correspondent banking client's domicile, ownership and management structures and business and customer base.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	The FIC guidance notes provide that banks should refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell banks).

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	The FICA Regulations and guidance notes provide for instances in which client information is obtained in a non face-to-face situation. In such cases, banks "must take reasonable steps" to confirm the existence of the client and to verify the identity of the natural person involved, for example, receipt of faxes. In accepting business from non face-to-face customers banks should apply customer identification procedures to non face-to-face customers that are as effective as those that were applied to customers who were available for interview; there must be specific and adequate measures to mitigate the higher risk. Decisions concerning the additional steps to be taken in cases of a non face-to-face situation should be based on a bank's risk framework.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Suspicious Activity Reports are referred to as Suspicious Transaction Reports ("STRs") and submitted to the Financial Intelligence Centre ("FIC"): https://www.fic.gov.za/

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013-14 – 355,369 STRs (Source: FIC Annual report 2013) Comparative GDP data is not available for this specific period.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, the FICA has additional reporting requirements as contained within its Regulations. These are: a) Regulation 22A: Information to be reported concerning property associated with terrorist and related activities; and b) Regulation 22B: Cash threshold reporting.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Cash transactions below ZAR24,999 (approx. USD1,560) do not need to be reported as per the terms of Regulation 22B. However, suspicious transactions do not have de-minimis thresholds. The FICA makes provision for conveyance of cash to or from the Republic (section 30) and for electronic transfers of money to and from the Republic, these amounts have however not as of yet come into effect.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Not reporting within the required time period may lead to a maximum imprisonment of six months and/or a ZAR100,000 (approx. USD6,260) fine. Penalties for not reporting a suspicion or tipping off may lead to a maximum 15 years imprisonment and/or a ZAR10m (approx. USD625,960) fine. These can be imposed on an individual within an accountable institution.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Once a suspicious transaction has been reported, section 33 of the FICA allows an accountable institution to continue with the relationship/transaction unless directed otherwise by the FIC. This is confirmed by Guidance Note 4 on Suspicious Transaction Reporting, issued by the FIC on 14 Mar2008.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No. South African law only applies within the borders of the country.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No such requirement is in place.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	The Protection of Personal Information Bill ("POPI") is in draft before parliament and is expected to be established soon: a) yes. POPI is intended to protect the integrity and sensitivity of private information. In response, entities operating in sectors that request personal particulars – such as financial services or telecommunications – will be required to carefully manage the data capture and storage process; b) entities operating in sectors that request personal particulars – such as financial services or telecommunications – will be required to carefully manage the data capture and storage process; and c) no.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	There are prohibitions on the transfer of certain information outside the Republic with a few exceptions e.g. the data subject consents to the transfer; the recipient of the information is subject to a law, binding code of conduct or contract, etc. Section 25 prohibits the processing of information related to a: a) child who is subject to parental control in terms of the law; or b) data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life or criminal behaviour.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	There are prohibitions on the transfer of certain information outside the Republic, but none we are aware of in respect of transfer of information into the Republic.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No. However, in terms of case law, the confidentiality of customer information is considered a qualified legal right that can be overridden by greater public interest.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Zambia

Key contact: Nasir Ali
Email: nasir.y.x.ali@zm.pwc.com
Tel: +260 211 334000

Postal address: Stand No. 2374
Thabo Mbeki Road
P.O Box 30942, Lusaka, Zambia

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2001 (Prohibition & Prevention of Money Laundering Act), 2010 (Prohibition & Prevention of Money Laundering (Amendment) Act # 44). 2004 (Bank of Zambia Anti-Money Laundering Directives), and the Financial Intelligence Centre Act 2010.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	Bank of Zambia: http://www.boz.zm/ Pensions and Insurance Authority: www.pia.org.zm
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	No.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No, the most recent review was in 2008 (http://www.esaamlg.org/userfiles/Zambia_Mutual_Evaluation_Report.pdf). The FIC is currently carrying out a local AML survey, the results of which should be available in early 2016.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	There are no minimum transaction thresholds, under which customer due diligence is not required.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: A Zambian national has to present a national registration card or a valid passport or driving licence. In the case of a foreign national, a national registration card and a valid passport (and where applicable, an issued visa). Legal entities: Verify the identity of the directors, beneficial owners and management i.e. obtain Certificate of Incorporation or equivalent and details of the registered office/place of business; details of the nature of their business; the reason for the account being opened; indication of the expected turnover; the source of funds and a copy of the last available accounts where applicable. The Financial Intelligence Centre Act stipulates that a reporting entity shall, with respect to each customer obtain and verify the following: a) for a natural person, the full name and address and date of birth and place of birth; b) for a legal entity, the corporate name, the head office address, identities of directors, proof of incorporation or similar evidence of legal status and legal form, provisions of governing the authority to bind the legal person, and such information as is necessary to understand the ownership and the control of the legal person; c) for legal arrangements, the name address of the trustees, the settlor and the beneficiary of express trusts, and any other parties with the authority to manage, vary or otherwise control the arrangement; d) in addition to the identity of a customer, the identity of any person acting on behalf of the customer, including evidence that such person is properly authorised to act in that capacity; e) information on the intended purpose and nature of each business relationship; and f) sufficient information about the nature and business of the customer to permit the reporting entity to fulfil its obligations under the Act.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Certification of relevant identification copies by a Commissioner of Oaths.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Regulated institutions should identify the beneficial owner of an account (regardless of whether it is a corporate body or trust opening the account) and if it fails to ascertain the identity of the said owner or person, it should make a report to the AML Investigations Unit. The Financial Intelligence Centre Act stipulates that a reporting entity shall identify the beneficial owner and shall take reasonable measures to verify the identity of the beneficial owner unless the Minister prescribes the circumstances, such as the ownership of publicly held corporations, in which such identification and verification is not necessary.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	For regulated institutions, the circumstances are to be determined by the regulated institution and approved by the Bank of Zambia.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	In the case of trusts and internet banking. Also in circumstances of suspicion as stated below: a) suspicious customer behaviour; b) suspicious customer identification circumstances; c) suspicious cash transactions; d) suspicious wire transfer transactions; e) suspicious safe deposit area activity; f) suspicious activity in credit transactions; g) suspicious commercial account activity; h) suspicious trade financing transactions; i) suspicious investment activity; or j) suspicious deposits.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	The circumstances are to be determined by the regulated institution and approved by the Bank of Zambia.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	A financial institution shall require its foreign branches and majority owned subsidiaries to implement the requirements to the extent that the domestic applicable laws of the host country so permit. Where the laws of the country in which its branch or majority owned subsidiary is situated prevent compliance with the obligations stipulated, institutions must advise its supervisory authority, which may take such steps as it believes to be appropriate to accomplish purposes of the Act.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, the Financial Intelligence Centre Act stipulates that a shell bank shall not be established or permitted to operate in or through the territory of Zambia.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	The standard due diligence procedure of identification and verification applies for non face-to-face transactions and/or relationships. The Financial Intelligence Centre Act states that where any business relationship or execution of transactions is made with a customer that is not physically present, the following is required for purposes of identification: a) take adequate measures to address the specific risk of money laundering, financing of terrorism and any other serious offence; b) ensure that the due diligence conducted is no less effective than where the customer appears in person; and c) require additional documentary evidence or supplementary measures to verify or certify the documents supplied by the customer, or confirmatory certification from financial institutions or other documentary evidence or measure may be prescribed.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Suspicious Activity Reports are made to the Anti-Money Laundering Investigations Unit and for Financial Institutions the Financial Intelligence Centre.
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No, there is no obligation to report anything more than suspicious transactions – please see response to A13. Financial institutions are obliged to report where there is suspicion or reasonable grounds to suspect that any property is the proceeds of crime, or is related to or linked to, or is to be used for terrorism, terrorist acts or by terrorist organisations or persons who finance terrorism.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Any person who knows or suspects that an investigation into money laundering has been, is being or is about to be conducted, without lawful authority, divulges that fact or information to another person, shall be guilty of an offence and shall be liable, upon conviction, to a fine not exceeding one hundred and thirty-nine thousand penalty units (approx. ZMW25,020,000 or approx. USD4,800) or to imprisonment for a term not exceeding five years or to both. The Financial Intelligence Centre act states that the penalties for tipping off upon convictions shall be liable to a fine not exceeding five hundred thousand penalty units (approx. ZMW90,000,000 or approx. USD17,000) or to imprisonment for a period not exceeding five years, or to both. A person who intentionally fails to submit a report to the Centre commits an offence and is liable, upon conviction to a fine not exceeding seven hundred thousand penalty units (approx. ZMW126,000,000 or approx. USD24,000) or to imprisonment for a period not exceeding seven years, or to both.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	The regulated institution shall report to the AML Investigations Unit where the identity of the persons involved, the circumstances of any business transaction or where any cash transaction, gives any officer or employee of the regulated institution reasonable grounds to believe that a money laundering offence is being, has been or is about to be committed. As per the Financial Intelligence Centre acts, a financial institution shall refrain from carrying out a transaction which it suspects to be related to the money laundering, financing of terrorism or any other serious offence.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Although the local legislation does not specify this, one of the mandates of the Anti-Money Laundering Investigations Unit is to cooperate with law enforcement agencies and institutions in other jurisdictions responsible for investigation and prosecution of money laundering offences.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	N/A

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	The country does not have data protection laws.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	N/A

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	N/A

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	N/A



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Australia

Key contact: Malcolm Shackell / Peter Forwood
Email: malcolm.shackell@au.pwc.com / peter.forwood@au.pwc.com
Tel: +61 2 8266 2993 / +61 2 8266 3157

Postal address: 201 Sussex Street;
New South Wales, 2000,
Australia

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2006 (with staggered implementation from 13 Dec 2006 to 12 Dec 2008, thus phasing in the new legislation and replacing the old). A second tranche to include accountants, lawyers, real estate and others has been delayed.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	There is no new legislation; however new AML/CTF Rules commenced in June 2014 primarily focused on customer due diligence. The old legislation (Financial Transaction Reports Act 1988) is still in force but applies to a limited number of entities.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.)? Please include link to the regulator(s) website
A3.	The Australian Transaction Reports and Analysis Centre ("AUSTRAC") regulates AML across all industry sectors: http://www.austrac.gov.au/
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Guidance on AML requirements has been provided by AUSTRAC: http://www.austrac.gov.au/
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No, although there are certain 'trigger events' that require a reporting entity to verify the identity of existing customers. An example of such a trigger event is the customer accessing a new product or service.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. This is the central theme of the AML regime.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes. Australia underwent a Mutual Evaluation in 2014 and 2015 which was released in April 2015: http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-australia-2015.html

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No, however a certain number of exemptions have been provided for transaction thresholds in industries including bullion, low value superannuation, gaming service providers and currency exchange at accommodation facilities.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: The reporting entity must obtain the customer's name, residential address and date of birth. The customer's full name and either their date of birth or their residential address must be verified based on reliable and independent documentation and/or electronic data. Corporates: The reporting entity must collect from the customer the following information: a) the company's full registered name; b) registered address; c) principal place of business address; and d) Australian Company Number ("ACN") or Australian Registered Business Number ("ARBN"). This information can be verified using a range of documentation or electronic data. Reporting entities must include a procedure for the reporting entity to verify, at a minimum, the following information about a company; in the case of a domestic company: a) the full name of the company as registered by the Australian Securities and Investments Commission ("ASIC"); b) whether the company is registered by ASIC as a proprietary or public company; and c) the ACN issued to the company. There is further guidance in chapter 4 of the AML/CTF Rules Instrument 2007 (No.1) where the customer is: a) a domestic company; b) a foreign company that has registered its presence in Australia; or c) a foreign company that has not registered its presence in Australia. There are also customer identification requirements for other types of entities such as trusts, associations and clubs, and due diligence requirements for correspondent banking relationships.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Identification documents must be certified as a true copy by one of a number of categories of qualified individuals including legal practitioners, Justices of the Peace and Police Officers. A list of authorised persons can be found in chapter 1 of the AML/CTF Rules.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Under the new AML/CTF Rules commenced in June 2014: A reporting entity must collect and verify the full name and either the date of birth or address of all beneficial owners on all entity types. The reporting entity is not required to identify beneficial owners if the customer is a company which is verified under the simplified company verification procedure under paragraph 4.3.8 of the AML/CTF Rules 2007, or a trust which is verified under the simplified trustee verification procedure under paragraph 4.4.8 of the AML/CTF Rules 2007. The beneficial owner is defined as an individual who ultimately owns (25% or more) or controls (directly or indirectly) the customer.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence procedures are available to reporting entities in accordance with the risk based approach and procedures that they adopt. Certain pre-commencement customers are subject to modified identification procedures, in that those procedures do not have to be completed prior to the commencement (or continuation, in this case) of the designated service. For information on medium or low risk customers refer to chapter 4 of the AUSTRAC Regulatory Guide. Guide available at (http://www.austrac.gov.au/).
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence procedures are required to be implemented by reporting entities in accordance with the risk based approach and procedures that they adopt. Risk triggers specified in the rules as requiring enhanced customer due diligence are where the provision of a designated service is high risk or when a suspicion has arisen. Also to be considered are prescribed foreign countries in relation to prohibition or regulation of transactions with them. Under the new AML/CTF Rules commenced in June 2014, a foreign PEP or the customer that has a foreign PEP as the beneficial owner must be subject to enhanced customer due diligence.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Reporting entities are required to consider the risk posed by PEPs in accordance with the risk based approach and procedures that have been adopted by the reporting entity. As A13, under the new AML/CTF Rules commenced in June 2014, a foreign PEP or the customer that has a foreign PEP as the beneficial owner must be subject to enhanced customer due diligence.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Due diligence assessments must be carried out on the financial institution with which they wish to enter a correspondent banking relationship, prior to the commencement of the relationship and at regular intervals thereafter.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Reporting entities are required to consider the additional risk posed by non face-to-face business, in accordance with the risk based approach and procedures they have adopted. There are currently no specific rules or guidance relating to non face-to-face business.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Suspicious Matter Reports ("SMRs") are made to AUSTRAC, who act as Regulator and FIU: http://www.austrac.gov.au/

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014/15 – 93,137 SARs (Referred to as SMR or SUSTRs in Australia via a vis the AML/CTF Regulator (AUSTRAC), Source: AUSTRAC Annual Report 2014/15) Comparative GDP data is not available for this specific period.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	All Threshold Transactions ("TTRs") over AUD10,000 (approx. USD7,030) in cash and all International Funds Transfer Instructions ("IFTIs") are required to be reported to AUSTRAC. In addition, Cross Border Currency movements ("CBMs") must be reported to AUSTRAC, the Australian Customs Service, or the Police if over AUD10,000 (approx. USD7,030).

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No minimum threshold for SMRs, or IFTIs, but AUD10,000 (approx. USD7,030) for Cash Transactions.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, prohibited under criminal law and the AML/CTF Act 2006.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No requirement to have automated monitoring, but the AML/CTF Rules require each reporting entity to have a suspicious activity monitoring program.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes, provided the requirements of the Privacy legislation and protocols are complied with. Rules silent on how to monitor and where – AUSTRAC focuses on appropriateness of arrangements.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	There is no requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls. However, there is a requirement for the reporting entity to have an independent review performed on Part A of their Program on a regular basis. This independent review can be performed by either an internal or external party (Standard AML/CTF programs are divided into Parts A and B).

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) part of the financial statement audit?
A27.	As above, an independent review of the Program is required on a ‘regular’ basis. In practice this is conducted based on the bank’s risk-based approach, with many banks choosing to conduct the independent review on an annual basis. The report must be provided to the governing board and senior management. The regulator also requests a copy during their reviews. This does not constitute part of the financial statement audit.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	Chapter 8.6.2 of the AML/CTF Rules states the following: The purpose of the review should be to: a) assess the effectiveness of the Part A program having regard to the ML/TF risk of the reporting entity; b) assess whether the Part A program complies with these Rules; c) assess whether the Part A program has been effectively implemented; and d) assess whether the reporting entity has complied with its Part A program. We note that KYC falls under Part B of the Program and is therefore not required by legislation to be reviewed. In practice, the regulator has commented that it would expect to see Part B reviewed and many reporting entities choose to include Part B in the scope of their independent review.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, Australia's current privacy legislation is the Privacy Act 1988. Pre 12 March 2014: e) yes; f) the Privacy Act applies to Australian, ACT and Norfolk Island government agencies and certain private sector organisations, businesses that have an annual turnover of more than AUD3m (approx. USD2m), all credit reporting agencies and all health service providers; and g) yes. Sensitive data is information or an opinion about an individual's racial or ethnic origin, political opinions, membership or a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record or health information. It is subject to a higher level of privacy protection as it may only be collected with consent, cannot be used or disclosed for a secondary purpose and cannot be shared in the same way that personal information can be shared. Post 12 March 2014: a) yes; b) as above; and c) as above and post 12 March 2014 sensitive data will not be allowed to be collected unless reasonably necessary to perform an activity of an organisation or a function of an agency.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No, Australia is not subject to the above.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Bangladesh

Key contact: Dhruv Chawla
Email: dhruv.chawla@in.pwc.com
Tel: +91 (0) 8130166550

Postal address: PricewaterhouseCoopers Pvt. Ltd.
The Millenia, Tower D, 7th Floor, 1&2 Murphy Road,
Ulsoor, Bangalore - 560008 India

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Money Laundering Prevention Act ("MLPA") 2002, is the primary AML law in Bangladesh. Since then, several amendments have been made and in 2012 a new Money Laundering Prevention Act was passed. There is also the Anti-Terrorism Act ("ATA") which came into effect in 2009 and was amended in 2012 and 2013.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	No.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) Bangladesh Financial Intelligence Unit for banks: (https://www.bb.org.bd/bfiu/index.ph); b) Insurance Development & Regulatory Authority of Bangladesh for insurance: (http://www.idra.org.bd/idra-org/index.htm); Securities and Exchange Commission for asset management companies: (http://www.sec.gov.bd/); and Microcredit Regulatory Authority for non-government micro-finance institutions: (http://www.mra.gov.bd/); and c) N/A
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, the Money Laundering & Terrorist Financing Risk, Management Guidelines have been established to outline the legal and regulatory framework for anti-money laundering and combating the financing of terrorism ("AML"/"CFT") requirements and systems across the financial services sector (https://www.bb.org.bd/aboutus/regulationguideline/aml/aml_cft2015.pdf).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Not specifically mentioned but Bangladesh Bank directed all banks to complete KYC by 31 Mar 2010. See (http://www.unpan.org/PublicAdministrationNews/tabid/115/mctl/ArticleView/ModuleID/1467/articleId/21381/default.aspx).
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Banks should take the necessary measures to review and update the KYC of the customer after a certain interval. This procedure shall be conducted every two years in the case of low risk customers and every year in the case of high risk customers. See (https://www.bb.org.bd/aboutus/regulationguideline/aml/aml_cft2015.pdf) (page 41).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (of FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, see (http://www.apgml.org/mutual-evaluations/documents/default.aspx?s=date&c=8b7763bf-7f8b-45c2-b5c7-d783638f3354&pcPage=2).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No. According to the provision of section 25 (1d) of the MLPA 2012, FIs have to immediately report any suspicious, unusual or doubtful transactions, likely related to money laundering, to the Bangladesh Bank ("BB"). The BB has the power to call STRs from FIs related to the financing of terrorism according to section 15(a) of the Anti-terrorism (Amendment) Act, 2012.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	For customers that are legal persons, legal entities or legal arrangements, the Reporting Organization-Financial Institution ("RO-FI") should verify identity through the following information: a) verify the legal documents that has created the relationship; b) if necessary take legal opinion; c) name, legal form and proof of existence; d) the powers that regulate and bind the legal person or arrangement, as well as the names of the relevant persons having a senior management position in the legal person or arrangement; e) the address of the registered office and, if different, a principal place of business; and f) consider the risk profile of the relationship. See (https://www.bb.org.bd/bfiu/openpdf.php) (page 17).
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	The RO-FI is required to conduct a series of independent checks and inquiries in addition to the identification documents provided by the customer or beneficial owner. RO-FI is also required to verify the person acting on behalf of the customer to make sure they are authorized and their identity is duly verified. See (https://www.bb.org.bd/bfiu/openpdf.php) (page 16).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	For customers that are Legal persons, the RO-FI shall identify and take reasonable measures to verify the identity of beneficial owners through the following information: a) the identity of the natural person(s) (if any) who ultimately has a controlling ownership or interest in a legal person; b) to the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership or interest is the beneficial owner(s) or (b) where no natural person exerts control through ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means; and c) where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official. For customers that are Legal arrangements, the RO-FI shall identify and take reasonable measures to verify the identity of beneficial owners through the following information: a) for trusts, the identity of the settlor, the trustee(s) the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust including through a chain of control/ownership; and b) for other types of legal arrangements, the identity of persons in equivalent or similar positions. See (https://www.bb.org.bd/bfiu/openpdf.php) (page 17).
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	RO-FIs may apply simplified CDD measures where lower risks have been identified by the BFIU or as per the BFIU vetted risk assessment report conducted by the RO-FI itself or by the other independent body. The simplified measures should be commensurate with the lower risk factors, but are not acceptable whenever there is suspicion of money laundering and/or terrorist financing, or specific higher risk scenarios apply. See (https://www.bb.org.bd/bfiu/openpdf.php) (page 19).
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Banks should conduct Enhanced Due Diligence ("EDD") under the following circumstances: a) individuals or legal entities scored with high risk; b) individuals who are identified as PEPs, influential persons and chief executives or top level officials of any international organization; c) transactions identified with unusual in regards to its pattern, volume and complexity which have no apparent economic or lawful purposes; and d) while establishing and maintaining business relationship and conducting transaction with a person (including legal representative, financial institution or any other institution) of the countries and territories that do not meet international standard in combating money laundering and terrorism financing (such as the countries and territories enlisted as High-Risk and Non-Cooperative Jurisdictions in the Financial Action Task Force's Public Statement). See (https://www.bb.org.bd/aboutus/regulationguideline/aml/aml_cft2015.pdf) (page 41).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Enhanced CDD measures include: a) obtaining additional information on the customer (occupation, volume of assets, information available through public databases, internet, etc.) and regularly updating the identification data of the customer and beneficial owner; b) obtaining additional information on the intended nature of the business relationship; c) obtaining information on the source of funds or source of wealth of the customer; d) obtaining information on the reasons for intended or performed transactions; e) obtaining the approval of senior management to commence or continue the business relationship when applicable; f) conducting regular monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination; and g) making the concerned bank officials aware about the risk level of the customer. See (https://www.bb.org.bd/aboutus/regulationguideline/aml/aml_cft2015.pdf) (page 42). In addition to the above, banks should also perform the following: a) banks have to adopt the Risk Based Approach to determine whether a customer or the real beneficial owner of an account is a PEP; b) obtain senior managements' approval before establishing such business relationship; c) take reasonable measures to establish the source of funds of a PEP's account; d) monitor their transactions on a regular basis; and e) all provisions of Foreign Exchange Regulation Act, 1947 and issued rules and regulations by Bangladesh Bank under this act have to be complied with accordingly . See (https://www.bb.org.bd/aboutus/regulationguideline/aml/aml_cft2015.pdf) (page 47).
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Enhanced CDD measures include : a) obtaining additional information on the customer (occupation, volume of assets, information available through public databases, internet, etc.) and regularly updating the identification data of the customer and beneficial owner; b) obtaining additional information on the intended nature of the business relationship; c) obtaining information on the source of funds or source of wealth of the customer; d) obtaining information on the reasons for intended or performed transactions; e) obtaining the approval of senior management to commence or continue the business relationship when applicable; f) conducting regular monitoring of the business relationship, by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination; and g) making the concerned bank officials aware about the risk level of the customer. See (https://www.bb.org.bd/aboutus/regulationguideline/aml/aml_cft2015.pdf) (page 42).
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, see (https://www.bb.org.bd/aboutus/regulationguideline/aml/aml_cft2015.pdf) (page 32).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	Financial institutions should consider the money laundering risks posed by the products and services they offer, particularly where there is no face-to-face contact with the customer, and devise their procedures to that risk with due regard. Where there is no face-to-face contact, and photographic identification would clearly be inappropriate, procedures to identify and authenticate the customer should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity. At least one additional check should be undertaken to guard against impersonation. In the event that internal procedures require sight of a current passport or ID Card where there is no face-to face contact, then a certified true copy should be obtained. See (https://www.imolin.org/doc/amlid/Bangladesh/Bangladesh_Guidance_Notes_on_Prevention_of_Money_Laundering.pdf).

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Institutions enlisted as per the MLPA 2012 and ATA 2009 (as amended in 2012) are obligated to submit STRs/SARs to the Bangladesh Bank. Such reports must come to the Bangladesh Bank from the CCU of the respective institutions by using the specified format/instructions given by the Bangladesh Bank. See (https://www.bb.org.bd/bfiu/index.php).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 -14: 619 (http://lankabd.com/news/getDetailsStory.html?storyId=27944&goToHomePageParam=true&siteLanguage=en). Comparative GDP data is not available for this specific period.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Bank officials need to consider the confidentiality of the reporting of STRs/SARs. They should not behave/perform in a manner that might tip-off the customer as he/she (the customer) could become cautious. See (https://www.bb.org.bd/aboutus/regulationguideline/aml/aml_cft2015.pdf) (page 58).

Q21.	Are there any de-minims thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Bank officials need to consider the confidentiality of the reporting of STRs/SARs. They should not behave/perform in a manner that might tip-off the customer as he/she (the customer) could become cautious. See (https://www.bb.org.bd/aboutus/regulationguideline/aml/aml_cft2015.pdf) (page 58).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Depending on the size, need and complexity of financial institutions, monitoring of unusual transactions may be automated, manual or both. Some financial institutions use specialized software to detect unusual transactions or activities, however, the use of such software can only be complemented <i>with</i> managerial oversight and cannot replace the need for constant monitoring of activity of the accounts of customers. See (https://www.bb.org.bd/aboutus/regulationguideline/aml/aml_cft2015.pdf) (page 58).

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Not Available.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Not Available.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	An external auditor may also play an important role in reviewing the adequacy of AML and CFT controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. An external auditor would be risk-focused while developing their audit programs and conduct intensive reviews of higher risk areas where controls may be deficient. External auditors may report incidences of suspected criminal activity uncovered during audits in its audit report. See (https://www.bb.org.bd/aboutus/regulationguideline/aml/aml_cft2015.pdf) (Page 38).

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) auditors can communicate their findings and recommendations to management via the annual management letter, which accompanies the audit report; b) management; and c) yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) address the adequacy of AML/CFT risk assessment; b) examine/attest the overall integrity and effectiveness of the management systems and the control environment; c) examine the adequacy of Customer Due Diligence (CDD) policies, procedures and processes, and whether they comply with internal requirements; d) determine personnel adherence to the financial institutions AML/CFT policies, procedures and processes; e) perform appropriate transaction testing with particular emphasis on high risk operations (products, service, customers and geographic locations); f) assess the adequacy of the FIs processes for identifying and reporting suspicious activity; g) communicate the findings to the board and/or senior management in a timely manner; h) recommend corrective action for deficiencies; i) track previously identified deficiencies and ensure that management corrects them; and j) assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How it defined and what are the additional protections?
A29.	No, see (http://www.nortonrosefulbright.com/knowledge/publications/121081/business-ethics-and-anti-corruption-laws-bangladesh).
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	N/A
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	N/A

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	N/A



'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



China

Key contact: Antoinette Lau / Chris Wilson
Email: antoinette.yy.lau@cn.pwc.com /
chris.p.wilson@hk.pwc.com
Tel: +86 21 2323 5533 / +852 2289 1993

Postal address: 11/F PwC Center,
202 Hu Bin Road, Shanghai 200021,
P.R. China

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The primary legislation governing AML in China is as follows: a) Anti-Money Laundering Law (2006); b) Provisions on Anti-Money Laundering through Financial Institutions (2006); c) Administrative Measures for Financial Institutions on Report of Large-sum Transactions and Doubtful Transactions (2006); d) Administrative Measures for Financial Institutions on Report of Transactions Suspected of Financing for Terrorist Purposes (2007); e) Administrative Measures for Financial Institutions on Identification of Client Identity and Preservation of Client Identity Materials and Transactions Records (2007); f) Measures on the Administration of Freezing Assets Related to Terrorist Financing (2014); and g) Measures for the Supervision and Administration of Anti-Money Laundering by Financial Institutions (for Trial Implementation) (2014).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	Prior to the Anti-Money Laundering Law, China issued three main regulations on monitoring and reporting large-sum and suspicious transactions within financial institutions in 2003, requiring financial institutions to take the responsibilities for identifying, monitoring and reporting of doubtful and suspicious capital flow. Previously the regulations applied to crimes of drugs, crimes committed by organized criminal gangs, crimes of terrorism, and crimes of smuggling. This has been specifically broadened to bribery and corruption crimes, crimes of disrupting the control of financial order and crimes of financial frauds. In late 2012, the central bank issued "Guidelines for the Assessment of Money Laundering and Terrorism Financing Risks and Categorized Management of Customers of Financial Institutions" that requires Financial Institutions to add a money laundering risk scoring to each of their customers. Please refer to A1 above.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non-financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The AML law in China covers both financial institutions which include banks, insurance companies, securities firms and other deposit taking institutions, as well as the non-financial sector. a) The People's Bank of China ("PBOC") is the main enforcement body who carry out on-site inspections and apply fines if violations are found. (http://www.pbc.gov.cn/english/130437/index.html); b) the industry regulatory body for Banking is China Banking Regulatory Commission ("CBRC") (http://www.cbrc.gov.cn/english/index.html); c) the industry regulatory body for Securities Firms is China Securities Regulatory Commission ("CSRC") (http://www.csrc.gov.cn/pub/csrc_en/); d) the industry regulatory body for Insurance Firms is China Insurance Regulatory Commission ("CIRC") (http://www.circ.gov.cn/web/site0/); and e) for non-financial sectors, the general responsibility rests with the State Administration for Industry and Commerce ("SAIC") (http://www.saic.gov.cn/english/index.html).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	<i>Please note, the below links are only available in Mandarin.</i> PBOC: Guideline for the Assessment of Money Laundering and Terrorism Financing Risks and Categorized Management of Customers of Financial Institutions issued by PBOC: http://www.pbc.gov.cn/chubanwu/114566/114579/114616/2808308/index.html CSRC: Guideline on Anti-Money Laundering and Counter-Terrorist Financing (For Securities Industries) issued by CSRC: http://www.csrc.gov.cn/pub/newsite/flb/flfg/bmgf/zh/gfxwjfq/201310/t20131016_236276.html CIRC: a) Guideline on Anti-Money Laundering for Insurance Industry issued by CIRC: (http://www.circ.gov.cn/web/site0/tab5225/info42692.htm) b) Guideline for the Assessment of Money Laundering and Terrorism Financing Risks and Categorized Management of Customers of Insurance Institutions issued by CIRC: http://www.circ.gov.cn/web/site0/tab5216/info3946815.htm
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	There is no clear requirement to retrospectively verify the identity of customers before a new AML regime was introduced. However, on "Notice of the People's Bank of China on Further Strengthening the Anti-money Laundering Work of Financial Institutions" (2008), it states that: "Pursuant to the time of establishing business relationships, all legal person financial institutions shall, in accordance with the following requirements, formulate specific implementation plans, and urge all branches to complete the client risk classification on schedule: a) financial institutions shall complete, before the end of 2009, the classification of the clients with whom they established business relationships from 01 Aug 2007 to 01 Jan 2009. b) financial institutions shall complete, before the end of 2011, the classification of the clients with whom they established business relationships before 01 Aug 2007 but established no new business relationships after 01 Aug 2007. c) financial institutions shall, within ten working days after the establishment of business relationships, complete the classification of the clients with whom they establish business relationships after 01 Jan 2009. All legal person financial institutions shall file their respective working plans on client risk classification with the People's Bank of China.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. According to Anti-Money Laundering Law of the People's Republic of China issued in 2006, in Article 17, it states that "Where a financial institution identifies the identity of its clients through a third party, it shall be guaranteed that the third party has adopted the measures for clients' identity clarification as required by the present Law. Where any third party fails to adopt the measures for the clients' identity clarification as prescribed by the present Law, the financial institution shall bear the liabilities for its failure to perform the obligation of clarifying the client's identity." With the issuance of the latest KYC regulations in 2007, regulators require financial institutions to establish a risk-based KYC approach and report to PBOC. At the end of 2012, PBOC issued a new guideline called "Guidelines for the Assessment of Money Laundering and Terrorism Financing Risks and Categorized Management of Customers of Financial Institutions". In the new guideline, PBOC required Financial Institutions to take into consideration customer background, products, and geographical location as risk factors. All Financial Institutions need to report to the PBOC the new model by Mar 2013 and complete the implementation by end of 2015.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	FATF has completed an assessment of the implementation of anti-money laundering and counter-terrorist financing standards in the People's Republic of China (China). The first Mutual Evaluation Report of China was adopted by the FATF Plenary in Jun 2007 with the most recent follow up report being 17 Feb 2012 (http://www.fatf-gafi.org/media/fatf/documents/reports/mer/Follow%20Up%20MER%20China.pdf).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, for one-off services such as cash remittance, cash exchange and negotiable instrument cashing, the threshold is a one-off transaction of RMB10,000 or foreign currency with a value of USD1,000 or equivalent. For property insurance contracts paid in cash, the threshold is a single amount insurance premium of RMB10,000, or foreign currency of value USD1,000 or equivalent. For life insurance contracts paid in cash, the threshold is a single amount insurance premium of RMB20,000 or foreign currency of value USD2,000 or equivalent. For any insurance contracts paid by account transfer, the threshold is an insurance premium of RMB200,000 or foreign currency of value USD20,000 or equivalent.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	If any financial institution establishes a business relationship with a client or provides a one-off financial service such as cash remittance, cash conversion and bill payment beyond the prescribed amount, it shall verify and record the customer name and identification number, supported by original documentation. If the customer is represented by an agent, the financial institutions shall verify and record both the agent and the principal's identity details. Individuals: financial institutions are required to verify the customer identification information via a site visit in a face-to-face meeting; they should enquire with the public security bureau and check the online citizens' identity information system owned by the PBOC. Corporates: financial institutions are required to verify the customer identification information via a site visit in a face-to-face meeting. In addition, they should enquire with the state administration of industry and commerce.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Where copies of identification documentation are provided, financial institutions are required to confirm the certified copies with the authentication body, to ensure the accuracy of the information provided. If the financial institution certifies the identity through a third party, it should be assured that the third party has adopted measures for client identity clarification as prescribed by the present Law.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	According to "Notice of the People's Bank of China on Further Strengthening the Anti-Money Laundering Work of Financial Institutions" issued in 2008, financial institutions shall strengthen the maintenance and management of client identity data to ensure the accuracy and validity of client identity data. For the natural person who actually controls the client and actual beneficiary of transactions stated in "Identification Measures", it includes but is not limited to two types of people: the first is the actual controller, and the second is person who actually controls the transactions or enjoys relevant financial benefit but is not disclosed by the client (except for the agent). Financial institutions shall carry out such work as checking clients' valid identity certificates (identity documents) or re-identifying clients through inquiry of client, obtaining corroboration evidence from clients or using investigation agents, depending on the situations.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	When one financial institution (the trustor) entrusts another financial institution (the trustee) to sell financial products to clients, the trustor can rely on the customer due diligence conducted by the trustee based on the following conditions: a) the customer due diligence undertaken by the trustee meets the requirements of anti-money laundering laws and regulations; and b) the trustor is able to effectively obtain and preserve the KYC information.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	According to "Notice of the People's Bank of China on Strengthening the Anti-money Laundering Work of Financial Institutions in their Cross-border Business Cooperations" issued in 2012, for the following overseas non-financial institutions, financial institutions should fully collect the overseas institutional business, reputation, internal control, acceptance of regulation and other information to assess the money laundering risk, and decide whether to provide financial services or start business cooperation with the consent of senior management: a) institutions providing currency exchange, cross-border remittance and other assets transfer services; and b) institutions with operations of network payment, mobile payment, prepaid card, credit card receipts and other non-financial payment services. If financial institutions decide to provide services or build up business relationships with the above institutions, they should classify these institutions as high risk clients in principal and take specific enhanced risk control measures. Financial institutions shall ensure the anti-money laundering responsibilities of this overseas institution in writing and relevant requirements for cooperation with financial institution on anti-money laundering work. It should also be confirmed that due to the anti-money laundering work of financial institutions, the necessary risk control measures include closing accounts, freezing terrorist funds, and limiting transactions.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	According to "Notice of the People's Bank of China on Further Strengthening the Anti-money Laundering Work of Financial Institutions" issued in 2008, if the client or the natural person who has the actual control over the client and the actual beneficiary of transactions are current or previous foreign persons who perform important public functions, such as President, Head of Government, Senior Politicians, important government, judicial or military officials, senior management of SOE, party officials and etc., or the family members and other close associations of these people, financial institutions shall perform due diligence based on the requirements of "Foreign PEP" in <identity measures>.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	There is no specific regulation or guidance on this area in the 2007 AML law update. However, the Administration Regulation on Electronic Banking Business, published by the China Banking Regulatory Commission (CBRC), covers electronic banking including wire transfer, internet banking and telephone banking. This requires that the financial institutions intending to provide cross-border electronic banking services must make an application to the CBRC and provide the following documents: a) the country and its law / regulation relating to electronic banking; b) the main customers and services it intends to provide; c) the analysis and prediction of the business volume and the size of the customer base in the next three years; and d) the legal compliance analysis on cross-border electronic banking. There is no other KYC or other requirement issued by the authorities that specifically covers correspondent banking.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	According to "Notice of the People's Bank of China on Strengthening the Anti-money Laundering Work of Financial Institutions in their Cross-border Business Cooperations" issued in 2012, for the foreign financial institution which has no operating business in its registered place and is not well regulated, financial institutions shall not open a correspondent account for it or develop other business relationships with it which might damage the reputation.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	According to "Guidelines against Money Laundering and Terrorist Financing through Payment and Clearing Organizations" issued in 2012, it states in Article 8 that when a payment organization starts a business relationship with overseas institutions, it shall fully collect the overseas institution information including its business, reputation, internal control policies, and acceptance of regulation to assess the integrity and efficiency of anti-money laundering and anti-terrorist financing measurements. Financial institutions shall ensure the responsibilities and obligations of anti-money laundering and anti-terrorist financing with overseas institutions.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	China Anti-Money Laundering Monitoring and Analysis Centre ("CAMLMAC") (http://www.camlmac.gov.cn/).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 17,725,300 SARs (Source: 2014 Annual Report PBOC) GDP (in current prices) 2014 – USD10,360,000m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD584,475 of GDP.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Different thresholds are used to define Large Value Transactions which are mandatory for reporting. a) for individuals, the threshold is defined as daily cash transactions over RMB200,000 (approx. USD10,000); or wire transactions over RMB500,000 (approx. USD100,000); and b) for entities other than individuals, the threshold is defined as RMB2m (approx. USD200,000). Besides, according to "Measures for the Supervision and Administration of Anti-Money Laundering by Financial Institution (for Trial Implementation)", Article 13, financial institutions shall report to PBOC or its branch when the following situations happen: a) amendments on key internal control policies of anti-money laundering; b) change of anti-money laundering working organ, working staff and contracts; c) significant risk issues relating to anti-money laundering work; d) self-review on money laundering risks or other risk analytical materials; and e) other anti-money laundering issues as requested by PBOC to immediate report.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, the People's Republic of China's AML law states that the Chairman, senior manager or any other person responsible are punishable. Penalties include disciplinary sanction or revoking of qualification to hold a post, fine of RMB 10,000 (approx. USD1,533) up to RMB 500,000 (approx. USD76,686) to an individual and/or RMB20,000 (approx. USD3,067) up to RMB 5m (approx. USD766,589) to the organisation. For very serious cases, the regulator can order to suspend business for rectification or to revoke its business license.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Yes. PBOC decree 2 2006 requires financial institutions to monitor and report both large value and suspicious transactions based on a set of pre-defined patterns/threshold.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	None stated in local regulations or guidance.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	China does not have Data Privacy Laws. Protection of "Personal Data" is governed by different laws and regulations for different purposes. Generally speaking, as long as the data is used within China, no law prohibits personal data to be held for KYC purpose. For the purpose of AML/KYC, there is no definition of "sensitive data". However the financial institutions should observe "Consumer Protection Law Art. 29": a) business operators shall collect and use the personal information of consumers in a lawful and proper manner by following the principle that information collection or use is genuinely necessary. They shall expressly state the purposes, methods and scope of information collection or use, and obtain the consent of the consumers whose information is to be collected. To collect or use the personal information of consumers, business operators shall disclose their information collection or use rules, and shall not collect or use information in violation of laws or regulations, or in breach of the agreements between the parties concerned; b) business operators and their staff members shall strictly keep confidential the personal information of consumers collected, and shall not divulge, sell or illegally provide others with the same. Business operators shall take technical measures and other necessary measures to ensure information security and prevent the personal information of consumers from being leaked or lost. They shall immediately take remedial measures where information has been or may be leaked or lost; and c) business operators shall not send commercial information to consumers without their consent or request, or after the consumers have expressly refused to receive such information.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Credit reports, criminal records and medical data are all prohibited from transfer for a non-related purpose (including KYC) without proper authority/consent.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No law or regulation in China impacts the transfer of information to the country.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	China does not have Bank Secrecy Laws. Personal data and transaction records are governed by different regulations from free transfer, i.e. outside of the bank, or other than the purpose for which the information is obtained. Bank customer records are prohibited from transfer to outside of the country even within the same group of entities.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Hong Kong

Key contact: Adams Chan / Chris Wilson / Hokee Fu
Email: adams.wf.chan@hk.pwc.com /
chris.p.wilson@hk.pwc.com / ho.kee.fu@hk.pwc.com
Tel: : +852 2289 2784

Postal address: ss: 21/F Edinburgh Tower,
15 Queen's Road
Central, Hong Kong

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The primary legislation governing AML in Hong Kong is as follows: a) Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance – 2012 (amended 2015) ("AMLO"); b) Drug Trafficking (Recovery of Proceeds) Ordinance - 1989 (amended 2005) ("DTROP"); c) Organised and Serious Crimes Ordinance - 1994 (amended 2012) ("OSCO"); d) United Nations (Anti-Terrorism Measures) Ordinance - 2002 (amended 2012) ("UNATMO"); and e) United Nations Sanctions Ordinance – 1997 ("UNSO").
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The AMLO became effective on 1 Apr 2012 and was amended in 2015. Previous AML regime was governed by DTROP, OSCO, UNATMO and UNSO.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.)? Please include link to the regulator(s) website
A3.	a) The Financial Services and Treasury Bureau has taken over the overall co-ordinating role for anti-money laundering/counter-terrorist financing policies and monitor Hong Kong's overall compliance with all the FATF recommendations (http://www.fstb.gov.hk/fsb/aboutus/welcome/index.htm); b) The Hong Kong Monetary Authority ("HKMA") is the regulator for AML controls for banking sector (http://www.hkma.gov.hk/eng/index.shtml); c) The Securities and Futures Commission ("SFC") is the regulator for AML controls for securities sector (http://www.sfc.hk/sfc/html/EN/index.html); d) The Officer of the Commissioner of Insurance ("OCI") is the regulator for AML controls for insurance sector (http://www.oci.gov.hk/about/index.html); e) The Customs and Excise Department is the regulator for AML controls for money service operators ("MSOs") (i.e. Remittance Agents and Money Changers) (http://www.customs.gov.hk/en/home/index.html); and f) The Narcotics Division of Security Bureau ("ND") will assist in overseeing the implementation of the FATF recommendations that are related to the non-financial sectors and the non-profit organisations with a view to ensuring that the anti-money laundering/counter-terrorist financing measures taken by the relevant sectors and organisations are in line with established international standards. (http://www.nd.gov.hk/en/index.htm).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, the links of the guidance note issued by the relevant authorities are set out as below: a) Guideline on Anti-Money Laundering and Counter-Terrorist Financing (For Authorised Institutions) issued by the HKMA (revised March 2015) (http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/q33.pdf); b) Guideline on Anti-Money Laundering and Counter-Terrorist Financing issued by the SFC (revised April 2015) (http://en-rules.sfc.hk/net_file_store/new_rulebooks/hk/HKSFC3527_3705_VER30.pdf); c) Guideline on Anti-Money Laundering and Counter-Terrorist Financing (For authorised insurers, reinsurers, appointed insurance agents and authorised insurance brokers carrying on or advising on long term business) issued by the OCI (revised March 2015) (http://www.gld.gov.hk/egazette/pdf/20151913/egn201519132445.pdf); d) Guideline on Anti-Money Laundering and Counter-Terrorist Financing (For Money Service Operators) issued by the Customs and Excise Department (revised March 2015) (https://eservices.customs.gov.hk/MSOS/download/guideline/AMLO_Guideline_en.pdf); e) Anti-Money Laundering & Counter-Terrorist Financing – A Practical Guide for: Accountants, Estate Agents, Precious Metals and Precious Stones Dealers and Trust and Company Service Providers issued by the ND (June 2009) (http://www.nd.gov.hk/pdf/moneylaundering/AML_eng_full_version.pdf); f) The Guideline for Precious Metals and Precious Stone Dealers issued by the ND (2008) (http://www.nd.gov.hk/pdf/pmpsd_guideline-e.pdf); and g) An Advisory Guideline on Preventing the Misuse of Charities for Terrorist Financing issued by the ND (July 2007) (http://www.nd.gov.hk/pdf/guideline-e.pdf).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No, although under the revised guidelines, enhanced AML assessment requirements are expected to be applied to all customers, including existing customers. As part of their ongoing AML due diligence process, intermediaries should consider and determine whether additional identification information, in line with the current standards, should be obtained from all existing customers, particularly those customers in higher risk categories. In particular, authorised institutions regulated by the HKMA are required to conduct a review, at least once annually, on all high risk customers to ensure that the customer's records maintained are up-to-date and relevant. Under the AMLO, the identity of pre-existing customers is not subject to retrospective verification. The AMLO only requires the financial institution to review the documents, data and information relating to the customer that is held at the time it conducts the review.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	It is expected that financial institutions should adopt a risk based approach to customer due diligence and ongoing monitoring (e.g. suspicious transaction monitoring).
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Generally speaking, the current legislation does not specifically set out minimum transaction thresholds where customer due diligence is, or is not, required. However, less stringent due diligence requirements would be permitted in certain circumstances, such as: a) a remittance/exchange transaction carried out by remittance agents/money changers, where the transaction amount is less than HKD8,000 (approx. USD1,030) or equivalent; or b) a transaction carried out by authorised institutions on behalf of a non-account holder, where the transaction amount is less than HKD120,000 (approx. USD15,460) or equivalent.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: The identity of an individual including his/her name, residential address (and permanent address - if different), date of birth and nationality, etc. should be obtained. Identification should be from documents issued by official or reputable sources, i.e. passports or identity cards. The address should be checked by appropriate means, e.g. by reviewing utility or rates bills or checking the electoral roll. Corporates: The following documents or information should be obtained, including the Certificate of Incorporation and Business Registration Certificate, copy of the company's memorandum and articles of association, a company search enquiry of the registry and a company report, details of ownership and structure control of the company, the board resolution evidencing the opening of the account and conferring authority on those who will operate it, identification documents of the directors, principal shareholders and account signatories, as required. Additional requirements will arise for higher risk customers
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Copies of identification documentation should generally be checked against original documents. However, reliance may be placed on a 'suitable' certifier to certify that the copy document is a complete and an accurate copy of the original. Such certifiers include, inter alia, officer of an embassy, member of the judiciary, Justice of the Peace, etc.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	There is a requirement to identify the beneficial ownership and control, i.e. to determine which individual(s) ultimately own(s) or control(s) the direct customer, and/or the person on whose behalf a transaction is being conducted. For corporates, the identity of the principal shareholders (e.g. those holding 10% or more voting interests) should be identified. The identity of all shareholders holding 25% (for normal risk circumstance) /10% (for high risk circumstances) or more of the voting rights or share capital are required to be verified.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	The HKMA, SFC and OCI all take a risk based approach and in the circumstances where there is no suspicion of money laundering, the inherent risk of money laundering or terrorist financing is assessed to be low, and there is adequate public disclosure in relation to the customers, a simplified due diligence arrangement may be adopted. Examples of customers who are of a lower risk are: a) financial institutions authorised/supervised by the HKMA, SFC, OCI or by an equivalent authority in a jurisdiction that is a FATF member or in an equivalent jurisdiction; b) public companies that are subject to regulatory requirements, e.g. listing; c) government or any public body (e.g. government department, legislative, municipal, etc.) in Hong Kong, or the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body; d) companies which acquire an insurance policy for pension schemes which does not contain a surrender clause and the policy cannot be used as collateral; and e) companies which acquire a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence is required for higher risk categories of customers, business relationships or transactions. These may include companies with unduly complex ownership structure, PEPs, business relationships and transactions with persons from or in jurisdictions that do not meet international AML standards, customers who are not physically present for identification purposes, or remittance transactions for which the remittance messages do not contain complete originator information.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	Local regulatory guidance includes a requirement to gather sufficient information from a new customer and check publicly available information to establish whether or not the customer is a PEP. The decision to open an account for a PEP should be taken at a senior management level. A number of risk factors that institutions should consider in handling a business relationship with a PEP are also outlined.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	A bank providing correspondent banking services is required to gather sufficient information about its respondent banks to understand their business. Approval from senior management should be sought before establishing new correspondent banking relationships and the respective responsibilities of each institution should be documented. A corresponding banking relationship should not be established unless it is satisfied that the AML/CFT controls of the proposed respondent bank are adequate and effective. Particular care is required if a correspondent banking relationship is maintained with banks incorporated in jurisdictions that do not meet international AML standards, or where the respondent banks allow the direct use of the correspondent account by their customers to transact business on their own behalf (i.e. payable-through accounts).
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Firms are required to apply effective customer identification procedures to satisfy the true identity of the customer. Such procedures may include: a) requisition of additional documents to complement those required for face-to-face customers; b) taking supplementary measures to verify all the information provided by the customer; and c) requiring the first payment from the account to be made through an account in the customer’s name with a bank having satisfactory customer due diligence standards.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	SARs should be made to Joint Financial Intelligence Unit ("JFIU") and the relevant regulator of the reporting entity. JFIU: (http://www.jfiu.gov.hk/en/) HKMA: (http://www.hkma.gov.hk/eng/index.html) SFC: (http://www.sfc.hk/web/EN/index.html) OCl: (http://www.oci.gov.hk/about/index.html)
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 37,188 SARs (Source: Joint Financial Intelligence Unit of the Government of the Hong Kong Special Administrative Region, (http://www.jfiu.gov.hk/info/report/2015/)) GDP (in current prices): 2014 – USD290,895.8m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD7.8m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Financial institutions shall report to JFIU if there is knowledge or suspicion of ML/TF. Examples include, inter alia: a) customers are reluctant to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is complex or expensive for the institution to verify; and/or b) customers who decline to provide information that in normal circumstances would make the customer eligible for credit or for other banking services that would be regarded as valuable.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Institutions are required to refrain from carrying out transactions which they know or suspect to be related to money laundering until they have informed the JFIU which consents to the institution carrying out the transactions. Where it is impossible to refrain or if this is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering operation, institutions may carry out the transactions and notify JFIU on their own initiative and as soon as it is reasonable for them to do so.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	There are no explicit restrictions on "offshore" transactions monitoring provided that the other regulatory requirements, in particular the outsourcing and record keeping requirements, are fulfilled.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	According to s.59 (2) of the Banking Ordinance, HKMA may, as it thinks necessary (e.g. when actual/potential control or supervisory issues within the Bank were identified), direct a bank to submit a report prepared by an external auditor on prescribed subject matters. These include, inter alia, AML systems and controls.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) part of the financial statement audit?
A27.	As above, an independent review of the Program is required on a 'regular' basis. In practice this is conducted based on the bank's risk-based approach, with many banks choosing to conduct the independent review on an annual basis. The report must be provided to the governing board and senior management. The regulator also requests a copy during their reviews. This does not constitute part of the financial statement audit.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	The scope of work varies depending upon the circumstances which trigger the review as mandated by the HKMA. However, in a comprehensive AML review carried out by external auditors, sample testing of KYC files/SAR reports and examination of risk assessments would normally form part of the scope of work.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	The primary data protection law in Hong Kong is the Personal Data (Privacy) Ordinance ("PDPO"). Under the PDPO, personal data means any data relating directly or indirectly to a living individual; from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and in a form in which access to or processing of the data is practicable. The PDPO does not define corporate data or sensitive data.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	The PDPO stipulates that personal data shall not, without the prescribed consent of the data subject, be used for a new purpose (i.e. any purpose other than the purpose for which the data was to be used at the time of the collection of the data or a purpose directly related to it. There is prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	We are not aware of any such laws or regulations that may significantly impact upon the transfer of information to Hong Kong.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	There is no specific bank secrecy law in Hong Kong. It should, however, be noted that banks are subject to confidentiality obligations which are applicable under common law (i.e. the legal framework adopted by Hong Kong) and the regulators also expect that banks duly protect the use of its customer data in the normal course of business.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



India

Key contact: Dhruv Chawla
Email: dhruv.chawla@in.pwc.com
Tel: +91 (0) 8130166550

Postal address: PricewaterhouseCoopers Pvt. Ltd.
The Millenia, Tower D, 7th Floor, 1&2 Murphy Road,
Ulsoor, Bangalore - 560008 India

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Prevention of Money Laundering Act 2002 ("PMLA") came into force in Jul 2005. Current Amendment to the PMLA in 2012 became operational with effect from 15 Feb 2013.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	Amendment to the PMLA was enacted on 17 Dec 2012 and came into effect on 15 Feb 2013. The highlights of the amendments are as follows: a) the scope of money laundering activities has been broadened to include proceeds of crime including its concealment, possession, acquisition, or use and projecting and claiming, making mere possession of proceeds of crime an offence; b) possession of money received from criminal proceeds is also classified as crime; c) the threshold limit (earlier INR3m (approx. USD45,000)) for initiating money laundering cases has been removed; d) penalty schemes for money laundering activities have been revisited; e) the imprisonment term has been lengthened from at least three years to a maximum of seven years; and f) the upper limit for fines of INR500,000 (approx. USD7,500) has been removed (i.e. there is no upper limit fixed).
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) Reserve Bank of India Financial Intelligence Unit ("RBI FIU") for Banks (http://fiuindia.gov.in/); b) Insurance Regulatory and Development Authority ("IRDA") for Insurance: (https://www.irda.gov.in/); and c) Securities and Exchange Board for India ("SEBI") for asset management companies. (http://www.sebi.gov.in/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	RBI Master Circular dated 01 Jul 2014 on AML and KYC prescribes the following additional measures: a) full verification of identity at least every two years for high risk customers, every eight years for medium risk customers and every ten years for low risk customers; b) positive confirmation (obtaining KYC related updates through e-mail, letter, telephonic conversation, forms, interviews, visits, etc.) to be completed at least every two years for medium risk and at least every three years for low risk individuals and entities; and c) risk categorisation of accounts needs to be reviewed every six months.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, the local regulators (RBI, IRDA and SEBI) allow banking companies, financial institutions and intermediaries to use a risk based approach. On the basis of a risk based approach, verification of identity is done for high risk customers every two years, medium risk customers every eight years and low risk customers every ten years. A review of risk categorisation of accounts should be carried out at a periodicity of not less than once in six months.
Q7.	Has the country been the subject of a FATF (of FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The first Mutual Evaluation report on India was adopted on 24 Jun 2010 and recommended that India be placed in a regular follow-up process for mutual evaluation processes. The 8th Follow Up Report on the Mutual Evaluation of India was published in Jun 2013 and can be found at (http://www.fatf-gafi.org/media/fatf/documents/reports/mer/India_FUR8_2013.pdf). The report concluded that India had made sufficient progress for all core and key recommendations and recommended that India be removed from the follow-up procedure. In Jan 2013, the IMF published its update entitled 'India: Financial System Stability Assessment Update' which can be found here: http://www.imf.org/external/pubs/ft/scr/2013/cr1308.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	In the case of transactions carried out by a non-account based customer (walk-in customer) where the amount of the transaction is lower than INR50,000 (approx. USD750), the customer's identity and address do not require verification. However, if a bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of INR50,000 (approx. USD750), the bank should verify the identity and address of the customer and also consider filling in a suspicious transaction report. Verification of identity must be conducted in respect of all cross border payments.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The banking company, financial institution or intermediary must verify and maintain the records in respect of the identity and the current address of the client. The documents required are: Individuals: Official valid documents such as passport, driving licence, Permanent Account Number ("PAN") Card, Voter's Identity Card issued by the Election Commission of India, or any other document. Corporates: - Certificate of Incorporation; - Memorandum and Articles of Association; - a resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and - an official valid document in respect of managers, officers or employees holding an attorney to transact on its behalf. Association of Persons or Body of Individuals: - resolution of the managing body of such association or body of individuals; - power of attorney granted to him to transact on its behalf; - an official valid document in respect of the person holding an attorney to transact on its behalf; and - such information as may be required by the banking company or the financial institution or the intermediary to collectively establish the legal existence of such an association or body of individuals.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Certified copies of an official valid document may be used. The copies need to be verified by seeing the originals and stamped as 'originals seen and verified'.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The banking company, financial institution or intermediary should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the ultimate beneficial owner(s) is/are.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Customers can be categorised based on their risk profile. For example, individuals and entities whose identities and sources of wealth can be easily identified may be categorised as low risk. Reduced due diligence arrangements may be followed by the banking company, financial institution or intermediary in the case of low risk customers. The review of low risk clients' KYC documents can be performed once every ten years as per RBI circular dated 23 Jul 2013. In addition, under RBI Circular on KYC dated 10 Dec 2012, norms were further simplified to have only one document for both identity and address if the address on the document submitted for identity proof is the same as that declared in the account opening form. Introduction from an existing customer of the bank is not mandatory when documents of identity and address are provided.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Customers that are likely to pose a higher than average risk to the bank may be categorised as medium or high risk depending on the customer's background, nature and location of activity, country of origin, source of funds and client profile etc. Banks may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive due diligence for higher risk customers, especially those for whom the sources of funds is not clear. Examples of customers requiring higher due diligence may include: a) non-resident customers; b) high net worth individuals; c) trusts, charities, NGOs and organisations receiving donations; d) companies having a close family shareholding or beneficial ownership; e) firms with 'sleeping partners'; f) PEPs of foreign origin; g) non-face to face customers; h) those with a high risk reputation as per public information available; and i) correspondent banking relationships.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Banks should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Banks should verify the identity of the person and seek information about their source of funds before accepting the PEP as a customer. The decision to open an account for a PEP should be taken at a senior level which should be clearly identified in the Customer Acceptance policy. Banks should also subject such accounts to enhanced monitoring on an ongoing basis. The above may also be applied to the accounts of the family members or close relatives of PEPs. In the case of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, banks should obtain senior management approval to continue the business relationship and subject the account to the customer due diligence measures as applicable to the customers of a PEP category including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner. Further, banks should have appropriate ongoing risk management procedures for identifying and applying enhanced customer due diligence to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Banks should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Banks should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. It should also be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing due diligence on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request. Additionally, in view of monitoring and reviewing 'at par' cheque facility extended to walk-in-customers of cooperative banks through correspondent banking arrangements and to assess the risks including credit risk and reputation risk arising therefrom, banks should retain the right to verify the records maintained by the client cooperative banks/societies for compliance with the extant instructions on KYC and AML under such arrangements.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes. Guidance issued by the local regulator prohibits entering into a correspondent relationship with shell banks. Shell banks are not permitted to operate in India. Banks should also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by shell banks.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, banks must adopt specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented should be insisted upon and, additional documents may be called for in such cases. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the bank may have to rely on third party certification/ introduction. In such cases, it must be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place. Additionally, the first transaction should be through a cheque issued from an existing bank account.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Financial Intelligence Unit (FIU-IND): (http://fiuindia.gov.in/). In India SARs are known as "STRs" (Suspicious Transaction Reports).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013-14 - 54,000 (Source: FIU India Annual Report 2013-14). Comparative GDP data is not available for this specific period.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, as per the RBI and FIU guidelines, all banking institutions are required to report all such activities in terms of STR (on occurrence), Cash Transaction Reports and Counterfeit Currency Reports (periodically as per timelines laid down by the regulators) including all transactions involving receipts by non-profit organisations of value more than INR1m (approx. USD15,000) or its equivalent in foreign currency.

Q21.	Are there any de-minims thresholds below which transactions do not need to be reported?
A21.	Cash transactions below INR50,000 (approx. USD750) need not be reported. However, if there is a suspicion of deliberate effort to structure the transactions in such a way to keep the transaction just below the threshold, then such activities need to be reported as an STR.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	There are punitive clauses in the existing PMLA (2002) which were revised in 2013. Penalty schemes for money laundering activities were amended: a) imprisonment term lengthened from at least three years to a maximum of seven years; b) upper limit for fines of INR500,000 (approx. USD7,500) removed (i.e. no upper limit fixed); c) scope of money laundering activities broadened (possession of money received from criminal proceeds is also classified as crime); and d) threshold limit (earlier INR3m (USD45,000)) for initiating money laundering cases removed.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Yes, as per RBI and FIU guidelines.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Internal clearance is required.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes. Section 2.17 of the RBI's Master Circular (01 Jul 2013) on KYC norms/AML standards/Combating of Financing of Terrorism /Obligation of banks under PMLA, 2002 stipulates: "The guidelines contained in this master circular shall apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two."

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes. Section 7 of the RBI's Master Circular (12 Jul 2013) on KYC norms/AML standards/Combating of Financing of Terrorism /Obligation of banks under PMLA, 2002 stipulates: "Concurrent/Internal auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard should be put up before the Audit Committee of the Board on quarterly intervals."
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	Yes, once a year the external and internal auditors are mandated by the regulator to specifically report on KYC and AML controls. In addition, the RBI, SEBI and IRDA conduct annual inspections.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	Yes, they need to include the steps described in Q28 and to report on the findings.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How it defined and what are the additional protections?
A29.	Yes, they are governed by the Personal Data Protection Bill 2006 and Information Technology Act 2000.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Since banks collect Sensitive Personal Data or Information ("SPDI"), they need to comply with the Rules, which lay down certain procedures to be followed at the time of collection of data, transfer of data, and disposal of data, and to maintain relevant security practices and procedures. In the event a bank is negligent in implementing and maintaining "reasonable security practices and procedures" in relation to SPDI, which causes "wrongful loss or wrongful gain" to any person, then the bank is liable to pay compensation to the affected person whose SPDI was compromised. The aggrieved person claiming compensation may approach an adjudicating officer appointed under the Act in the case of damages of up to INR50m (approx. USD750,800) or before the civil court in case the damages claimed are above INR50m (approx. USD750,100). The Personal Data Protection Bill 2006 protects the privacy of individuals, but the bill was not passed into law. In the meantime, the Act was amended in 2008 to include Section 43A and Section 72A to protect personal data ("PI") and SPDI.

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	The Personal Data Protection Bill 2006 and Information Technology Act, 2000. The Information Technology Act provides for recognition of electronic signatures, e-documents and e-transactions, and seeks to control offences conducted over the internet. Also, post-2001, the RBI introduced guidelines governing internet banking, confidentiality, anti-money laundering and KYC norms, which may have prompted customers to move towards the e-platform, albeit with some concerns with respect to the privacy and security of their banking transactions.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	As per the Personal Data Protection Bill 2006, while collecting SPDI, the bank must seek express written consent from the provider of information via a letter, fax or e-mail, or consent given by any mode of electronic communication, in relation to the purpose for which SPDI may be used. The provider of information must also be given an option to withdraw such consent and must have knowledge and/or be provided information as to: a) the fact that information is being collected; b) the purpose for which it is being collected; c) intended recipients of the information; and d) the name and address of the agency that is collecting and/or retaining the information.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Indonesia

Key contact: Elizabeth Goodbody
Email: elizabeth.x.goodbody@id.pwc.com
Tel: +62 21 5212901

Postal address: JI HR Rasuna Said Kav X-7
No. 6 Jakarta 12940;
Indonesia

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2002 (amended through Law of Republic of Indonesia No 8 year 2010).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) Bank of Indonesia (http://www.bi.go.id/web/en); b) Otoritas Jasa Keuangan ("OJK" or Indonesian Financial Services Authority) (http://www.ojk.go.id/); and c) Pusat Pelaporan dan Analisa Transaksi Keuangan ("PPATK" or Indonesian Financial Transaction Reports and Analysis Center/INTRAC) (http://www.ppatk.go.id/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	a) Frequently Asked Questions (FAQ) Appendix of Bank Indonesia Regulation No 14/27/PBI/2012 (http://www.bi.go.id/en/peraturan/perbankan/Documents/bcde3006bbe64dd991ba14f41af57d31FAQ1427_REVMB.pdf); b) Bank Indonesia Circular Letter No. 3/29/DPNP concerning Standard Guidelines for Application of KYC Principles for All Commercial Banks (http://www.bi.go.id/en/perbankan/prinsip-mengenal-nasabah/Documents/StandardGuidelinesforApplicationofKnowYourCustomer.pdf); and c) Decree of Director General of Financial Institutions (Bapepam-LK) No. Kep-2833/LK/2003 on Direction of Drafting on KYC Implementation for Non-Bank Financial Services Sector.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.
Q7.	Has the country been the subject of a FATF (of FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The most recent mutual evaluation was conducted in 2008: The APG second Mutual Evaluation Report on Indonesia, July 2008 (http://www.fatf-gafi.org/topics/mutualevaluations/documents/mutualevaluationreportofindonesia.html). The most recent FATF Public Statement issued on 18 Oct 2013 identified Indonesia as a jurisdiction with strategic AML/CFT deficiencies that has not made sufficient progress in addressing the deficiencies and implementing its action plan within the agreed timeline. The Statement can be found here: http://www.fatf-gafi.org/countries/d-i/indonesia/documents/fatf-public-statement-oct-2013.html#indonesia The IMF 'Indonesia Staff Report for the 2013 Article IV Consultation' published in Dec 2013 can be found here: https://www.imf.org/external/pubs/ft/scr/2013/cr13362.pdf Indonesia is due for its FATF Mutual Evaluation in 2016.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, simplified CDD is allowed for walk-in customers ("WIC") with transactions less than or amounting to IDR100m (approx. USD7,179).
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Financial institutions are required to conduct a face-to-face meetings with prospective customers, at least once, at the time of account opening. Alternatively, face-to-face meeting requirements can be satisfied through electronic media such as video calling and/or other electronic documentations. For Individuals: obtain and cross reference: name, address, place and date of birth and verification documentation from a regulatory body authorised to issue documents which includes customer's full name and photograph, and either address or date of birth, for example an identity card, passport or photocard driving licence. For Companies: obtain and cross reference: name, registration number, registration office in country of incorporation, tax registry number, business address, and identity of personnel who have the legal authority to represent the company.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	All three regulators require the firm to scrutinise the information provided by cross-referencing the available documentation which may include other sources of information beyond what is provided by the prospective customers that are deemed to be reliable and independent.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	All beneficial owners must be identified. Local regulation does not specify a minimum threshold of ownership as means of identifying beneficial ownership.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Non-Bank Financial Institutions ("NBFI") may implement simplified CDD for prospective customers when: a) the prospective Customer is a publicly-listed company; and b) the prospective Customer is a walk-in Customer ("WIC") engaging in a transaction less than or amounting to IDR100m (approx. USD7,179). Banks may implement simplified CDD procedures for prospective Customers or transactions having a low level of risk for the occurrence of money laundering or financing of terrorism and that meets the following criteria: a) the purpose for the opening of the account is for the payment of salaries; b) customers in the form of a public company subjected to regulations concerning performance disclosure obligations; c) prospective customers of a company of which the majority of shares are owned by Government; d) customers in the form of State/Government Agencies; e) transactions for the cashing of cheques by a walk-in customer that is a legal person; f) the purpose of opening the account is associated with a Government program in order to increase social welfare and poverty alleviation; or g) the maximum amount of initial deposit is IDR50,000 (approx. USD3.58), the maximum amount of balance at the end of month is IDR1m (approx. USD71.79), and the maximum amount of transaction within one month is IDR5m (approx. USD359).
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence ("EDD") should be performed when: a) engaging with a high-risk Customer (as classified by considering the customer's citizenship, occupation/industry, risk profile and relationship with Politically Exposed Person ("PEP")); b) engaging with a customer who performs transactions with high-risk countries; c) engaging with a customer who performs transactions inconsistent with its risk profiles; and d) engaging with a customer who performs transactions using high-risk products and services.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	PEPs are considered high-risk customers and both banks and non-bank financial institutions should always perform EDD when engaging with a PEP.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	There are two conditions for correspondent banking relationships: a) if the correspondent bank is regulated by a territory which has the equivalent standard of KYC implementation to Indonesia, then a formal letter should be written stating that the bank has implemented KYC in relation to the customer properly; and b) if the correspondent bank is regulated by a territory which has lower KYC standards than Indonesia, then the bank/NBFI entering into a customer relationship with the correspondent bank shall also perform KYC procedures on the customer of that bank as well and the correspondent bank.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Face-to-face meetings should be performed at least once in the account opening process. The only exception to this requirement is for NBFIs where OJK allows the meetings the meetings to be conducted via video link.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Reports of suspicious transactions ("STR") are made to the FIU for Indonesia, the Pusat Pelaporan dan Transaksi Analisis Transaksi Keuangan ("PPATK") by both banks and non-banks. Government Regulation No 43 Year 2015 issued by the President of Indonesia on 23 Jun 2015 requires the following additional parties to undertake KYC and report to PPATK: a) venture capital companies; b) infrastructure financing companies; c) microfinance institutions; d) export financing institutions; e) advocates; f) notaries; g) land deed officials; h) accountants; i) public accountants; and j) financial planners. The source can be found here: http://jdih.ppatk.go.id/peraturan-pemerintah-nomor-43-tahun-2015-tentang-pihak-pelapor-dalam-pencegahan-dan-pemberantasan-tindak-pidana-pencucian-uang/

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, there is an obligation to make cash transaction reports ("CTR") and international funds transfer reports ("IFTs"). The former is a requirement after a certain threshold value for transactions has been revealed, while the latter, IFTs, are required for both incoming and outgoing transfers without any threshold for the transaction amount.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	a) STR - No; b) CTR - IDR100m (approx. USD7,179); and c) IFT - No.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes. Tipping off is a criminal offence and other penalties apply for non-compliance with AML obligations (including reporting requirements).

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Authority to proceed with suspicious transaction may be obtained, on a case by case basis, from Regulator. Authority to proceed internally could form part of the escalation and governance matters within financial institutions.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No, reviews are conducted by AML specialists and are not a part of annual statutory audits. There is no statutory requirement for independent review but financial institutions can undertake such reviews either internally using their Internal Audit function, 3 rd line of Defence or an external party, if they wish.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of “personal data” cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of “sensitive data”? How is it defined and what are the additional protections?
A29.	a) banking privacy is in place. This is different to broader data protection, which is still emerging. Customer financial data is “protected” under Banking Privacy legislation; b) refer to a), Banking Privacy specifically; and c) no. The relevant regulation is under Indonesia Basic Banking Law Number 23/1999. There have been some amendments to this law, but no basic change to the requirements.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Different legislation and regulations govern different data restrictions. Advice should be sought on a case-by-case basis.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Refer to A29 and A30 above.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. Refer to A29 above.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Japan

Key contact: Yoshihiko Nishikawa
Email: yoshihiko.nishikawa@jp.pwc.com
Tel: +81 3 3546-8450

Postal address: Sumitomo Fudosan Shiodome Hamarikyu Bldg,
8-21-1, Ginza, Chuo-ku,
Tokyo, 104-0061 Japan

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Based on the revisions of the Financial Action Task Force ("FATF") 40 Recommendations in 2003, Japan enacted the Act on the Prevention of Transfer of Criminal Proceeds 2007. The Act was amended on 28 Apr 2011 and came into force on 01 Apr 2013. Several other laws implemented for Anti-Money Laundering measures include the Anti-Drug Special Prevention Law 1992 and Act on the Punishment of Organised Crime 2000. The Act on The Prevention of Transfer of Criminal Proceeds is being updated and will be enacted in Oct 2016.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The amendments in 2011 expanded the types of information requested as part of the KYC process. Where previously, under the Act on Prevention of Transfer of Criminal Proceeds, the customer identification information for verification was as follows. Natural person: Name, address, date of birth. Legal person: Name, location of the head or main office.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.)? Please include link to the regulator(s) website
A3.	Japan Financial Services Agency ("FSA"): http://www.fsa.go.jp/en/index.html There are respective regulatory agencies for each business operator: http://www.npa.go.jp/sosikihanzai/jafic/index_e.htm
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The FSA has issued comprehensive supervisory guidelines for the financial sector. Although they are general guidelines for financial institutions, it contains some guidance regarding Anti-Money Laundering compliance. See (http://www.fsa.go.jp/en/refer/legislation/index.html).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Financial institutions are required to verify the identity of customers upon undertaking the specified transactions from pre-existing customers, where customer identification was not undertaken before the implementation of the Act on Prevention of Transfer of Criminal Proceeds.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Despite the fact that the AML regime in Japan is not risk based, some aspects of this approach are incorporated into the guidelines issued by the FSA. Banks are expected to establish and maintain an internal control environment to detect, monitor, and analyse suspicious customers, considering various factors such as customer attributes, transaction types and customer business profiles. In addition, the Japanese Bankers Association issued the "Guidance Note on the Risk based Approach" in Nov 2007 for combating money laundering and terrorist financing. The Guidance Note is available for member banks and advises on the implementation of the risk based approach.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The most recent FATF Mutual Evaluation on Japan was published in Oct 2008: http://www.fatf-gafi.org/documents/documents/mutualevaluationofjapan.html

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, customer identification is not required for one-off cash transactions below JPY2m (approx. USD16,950) and one-off wire transfer transactions below JPY100,000 (approx. USD850).
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The verification method of customer identification information varies depending if the customer is a natural person or a legal entity. Natural person: The following information has to be verified from valid customer identification documents such as a driving licence, passport, alien registration card or any other acceptable documents: name, address and date of birth. In addition, the following additional information has been required since 01 Apr 2013, based on the amended Act: a) occupation; b) purpose of the business relationship; c) verification that natural persons acting on behalf of account holder are so authorised; and d) for higher risk customers described in the ordinance, verify asset and/or income of the customer. Legal Entity: The following information has to be verified from valid identification documents such as certificate of registration, seal registration certificate or any other acceptable documents: name and location of the head or main office. In addition, the following information/procedures have been required since 01 Apr 2013, based on the amended act: a) business contents; b) purpose of the business relationship; c) identity of beneficial owner; d) verify that natural persons acting on behalf of the legal entity are so authorised; and e) for higher risk customers described in the ordinance, verify asset and/or income of the customer.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Upon receiving copies of identification documents, financial institutions are required to use registered mail (which cannot be forwarded) to complete the customer identification process. The customer identification process is considered complete unless the registered mail is returned to the financial institution as being undelivered.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	For legal entities, the beneficial owners owning more than 25% of its shares or voting rights are required to be identified and verified.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced due diligence arrangements are not explicitly stipulated in law/regulations. Rather, the ordinance exempts certain types of transactions from customer identification requirements (e.g. transactions with the government or governmental entities), due to no or limited money laundering/terrorist financing risk.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence is required where: a) the Specified Operator suspects that the counterparty of the transaction may impersonate a customer or its representative; b) the Specified Operator suspects that the counterparty of the transaction may be disguising identification items at the execution of the transaction; or c) transactions with a Customer originating in Iran or North Korea. Where such circumstances apply the Specified Operator must conduct customer due diligence again. Additionally, when the transaction amount is above JPY2m (approx. USD16,950), the Specified Operator must verify the assets and/or income of the customer.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	There is no legal obligation to undertake enhanced due diligence in respect of business relationships or transactions involving PEPs.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	There is a requirement in the ordinance that financial institutions undertake enhanced due diligence with respect to correspondent banking relationships. Additionally, guidelines issued by the FSA expect financial institutions to appropriately assess the prospective foreign financial institutions before entering into the correspondent banking relationships.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	No, relationships with shell banks are not explicitly prohibited. However, guidelines issued by the FSA require that financial institutions ascertain that prospective foreign financial institutions are not shell banks.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	Upon initiating non face-to-face transactions such as internet or telephone banking, financial institutions are required to verify a customer's address by sending registered mail or conducting a site visit.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	SARs are submitted to the respective regulatory agency (e.g. the FSA in respect of the financial sector) and consolidated by Japan Financial Intelligence Center ("JAFIC") (http://www.fsa.go.jp/str/) and (https://www.npa.go.jp/sosikihanzai/jafic/index_e.htm).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 377,513 SARs (Source: https://www.npa.go.jp/sosikihanzai/jafic/en/nenzihokoku_e/data/jafic_2014e.pdf) GDP (in current prices): 2014 – USD4,601,461m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD12.1m of GDP.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Yes, an administrative penalty may be received from the respective authorities.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes: a) under the Personal Information Protection Law (2003), personal information is defined as information of a living individual, such as the name, the date of birth, and/or any other descriptions by which a specific individual can be identified (including information that can be easily collated with other information so that a specific individual can be identified); b) the law does not cover corporate data; and c) yes. The FSA Guideline defines 'sensitive information', and requires financial institutions not to obtain such information. See "Guidelines for Personal Information Protection in the Financial Field" (http://www.fsa.go.jp/frtc/kenkyu/event/20070424_02.pdf).
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	The definition of sensitive information includes both criminal records and medical data. As noted at A29, financial institutions are restricted in obtaining such information from customers.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Malaysia

Key contact: Alex Tan
Email: alex.tan@my.pwc.com
Tel: +60 3 2173 1338

Postal address: Level 10, 1 Sentral, Jalan Rakyat
Kuala Lumpur Sentral, PO Box 10192,
50706 Kuala Lumpur, Malaysia

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	15 Jan 2002.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	Bank Negara Malaysia (the Central Bank) (http://amlcft.bnm.gov.my/index.html).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	For banks and other financial institutions, a new guideline was issued on 01 Sept 2013: http://www.bnm.gov.my/guidelines/01_banking/03_anti_money/04_gl_amlcft_deposit.pdf For accountants and other non-financial sector entities, a new guideline effective 01 Nov 2013 has been introduced: http://www.bnm.gov.my/guidelines/50_others/AMLCFT(DNFBPS%20&%20Others).pdf For Money Services Business, a new guideline effective 01 Dec 2011 has been introduced: http://www.bnm.gov.my/index.php?ch=en_legislation&lang=en For insurance and Takaful entities, a new guideline effective 15 Sept 2013 has been introduced: http://www.bnm.gov.my/guidelines/02_insurance_takaful/02_anti_money/03_policy_instkf_amlcft.pdf
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, a risk based approach is approved. However a specific approach is not detailed and it remains the responsibility of the reporting institution to devise an approach.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, see: http://www.apgml.org/members-and-observers/members/member-documents.aspx?m=b1b0ea02-b04a-4b44-bb78-4d98fec54862

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	In broad terms there is no minimum threshold for the following: a) establishing businesses relationships; b) wire transfers; c) if there is suspicion of ML/TF; and d) if there is doubt about veracity or adequacy of previously obtained information. Otherwise: For banks and deposit taking institutions: Money changing and wholesale currency business - RM3,000 (approx. USD690) and above; occasional transactions - RM50,000 (approx. USD11,510) and above in a single transaction or several transactions in a day that appear to be linked; cash transactions - RM50,000 (approx. USD11,510) and above in a day. For insurance and takaful: May perform simplified CDD on customer, beneficial owner and beneficiary if: a) all insurance policies are sold with premium amount below RM5,000 (approx. USD1,150); or b) any single premium insurance policy is below RM10,000 (approx. USD2,300). For money service businesses: Money changing and wholesale currency business - RM3,000 (approx. USD690) and above: a) RM3,000 (approx. USD690) to RM10,000 (approx. USD2,300), sighting and keying in customer/beneficial owner identification information; and b) above RM10,000 (approx. USD2,300), sighting and keying in customer/beneficial owner identification information and making a copy of identification document. For licensed casino: Any transaction involving RM10,000 (approx. USD2,300) and above (exchange cash for cash chips, exchange cash/vouchers for chip warrants, request for cheques or wire transfers for payments of winnings/capital, use of membership cards/temporary cards in respect of e-cash out facility). CDD is also required on the third party when customer requests RM10,000 (approx. USD2,300) and above to be paid to a third party. For licensed gaming outlets: Appropriate thresholds are decided internally based on their own risk assessment. Thresholds are not publicly disclosed. For dealers in precious metals and stones: Any cash transaction equivalent to RM50,000 (approx. USD11,510) and above, either as a single transaction or multiple transactions on a given day.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: reporting institutions should obtain at least: full name; date of birth; nationality; permanent and mailing address and NRIC/passport number. Institutions should verify the identity, representative capacity, domicile, legal capacity, occupation or business purpose of any person, as well as other identifying information on that person, whether an occasional or usual client, through the use of documents such as an identity card, passport, birth certificate, driving licence, or any other official or private photograph bearing document. Where a particular individual is commonly known by two or more different names, the individuals shall not use one of those names to open an account with the reporting institutions, unless he/she has disclosed the other names to the reporting institutions. The reporting institution should make a record of the different names by which the individual is commonly known as and upon request provide the information to the competent authority. Corporates: reporting institutions should require the company/business to provide original documentation and copies should be made of each of the following documents: a) Memorandum and Articles of Association/Certificate of Incorporation/partnership; b) identification documents of directors/shareholders/partners; c) authorisation for any person to represent the company/business; d) identification document of the person authorised to represent the company/business in its dealing with the reporting institution; and e) registered office address and principle place of business
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Original documents must be provided and the reporting institution should make copies, as required. Certified true copies/duly notarised copies may be accepted.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The reporting institution must identify and verify the beneficial owner. They should conduct customer due diligence on the natural person that ultimately owns or controls the customer's transaction when they suspect the transaction is conducted on behalf of a beneficial owner and not the customer who is conducting such a transaction. The customer due diligence conducted should be as stringent as that imposed on an individual customer.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	A simplified customer due diligence process is adopted for lower risk categories of customers, business relationships or transactions. The relevant simplified process may vary from case to case depending on the customer's background, transaction type and specific circumstances.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Local AML guidance requires an enhanced customer due diligence process for higher risk categories of customers, business relationships or transactions. Enhanced due diligence should include at least obtaining more detailed information from the customer and through publicly available information, in particular, on the purpose of the transaction and source of funds; and obtaining approval from the Senior Management of the reporting institution before establishing the business relationship with the customer. Examples of higher risk customers are individuals with high net worth, non-resident customers, individuals from locations known for their high rates of crime (e.g. drug producing, trafficking, smuggling), countries or jurisdictions with inadequate AML/CFT laws and regulations as highlighted by the FATF, PEPs, legal arrangements that are complex (e.g. trusts, nominee companies), cash based businesses and businesses/activities identified by the FATF as of higher money laundering and/or terrorist financing risk.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	Once a PEP (local and foreign) is identified, the reporting institution should take reasonable and appropriate measures to establish the source of wealth and funds of such a person.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Section 20 of the sectorial guidelines for banks and financial institutions, deals with correspondent banking: S. 20.1 Reporting institutions providing correspondent banking services to respondent banks are required to take the necessary measures to ensure that it is not exposed to the threat of ML/TF through the accounts of the respondent banks such as being used by shell banks. S. 20.2 In relation to cross-border correspondent banking and other similar relationships, reporting institutions are required to: a) gather sufficient information about a respondent bank to understand fully the nature of the respondent bank’s business, and to determine from publicly available information the reputation of the respondent bank and the quality of supervision exercised on the respondent bank, including whether it has been subject to a ML/TF investigation or regulatory action; b) assess the respondent bank’s AML/CFT controls against the AML/CFT measures of the country or jurisdiction in which the respondent bank operates; c) obtain approval from Senior Management before establishing new correspondent banking relationships; and d) clearly understand the respective AML/CFT responsibilities of each institution. S. 20.3 In relation to “payable-through accounts”, reporting institutions are required to satisfy themselves that the respondent bank: a) has performed CDD obligations on its customers that have direct access to the accounts of the reporting institution; and b) is able to provide relevant CDD information to the reporting institution upon request. S. 20.4 Reporting institutions shall not enter into, or continue, correspondent banking relationships with shell banks. Reporting institutions are required to satisfy themselves that respondent banks do not permit their accounts to be used by shell banks. For the non-financial institution sector, there is no specific guideline for correspondent banking.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	For banks and other financial institutions, the guidelines state that they should not establish or have any business relationship with shell banks. There is no such prohibition for the non-financial sector.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Reporting institutions may establish non face-to-face business relationships with its customers. Non face-to-face relationships can only be established if the reporting institutions have in place policies and procedures to address any specific risks associated with non face-to-face business relationships. Reporting institutions are required to be vigilant in establishing and conducting non face-to-face business relationships (e.g. through the Internet) and are required to establish appropriate measures for identification and verification of customer identity that shall be as effective as that for face-to-face customers and to implement monitoring and reporting mechanisms to identify potential ML/TF activities. Reporting institutions may use the following measures to verify the identity of non face-to-face customer such as: - requesting additional documents to complement those which are required for face-to-face customer; - developing independent contact with the customer; or - verifying customer information against any database maintained by the authorities.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Financial Intelligence and Enforcement Department, Bank Negara Malaysia (http://amlcft.bnm.gov.my/AMLCFT05a.html).
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	There are no specific obligations in the non-financial sector. For banking and financial institutions, the obligations are contained at Appendix 1 of the following document: http://www.bnm.gov.my/guidelines/01_banking/03_anti_money/04_gl_aml_aamlcft_deposit.pdf
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes: a) failing to report suspicion (RM1m (approx. USD230,344) fine); b) tipping of (RM3m (approx. USD691,032) or jail (max 5 years) or both); and c) engaging or assisting in money laundering (jail (max 15 years) and the higher of five times the value of the proceeds or RM5m (approx. USD1.2m)).

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) Does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How it defined and what is are the additional protections?
A29.	Yes: a) the law only came into effect on 15 Nov 2013; b) the same law applies to corporate data in a number of scenarios however these have not yet been fully explained; and c) yes. Sensitive personal data is any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data. Due to the nature of sensitive personal data, a higher restriction is imposed for data users in processing it. A data user must not process sensitive personal data without the explicit consent of the data subject.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	The Personal Data Protection Act 2010 came into force on 15 Nov 2013. At this early stage, there is some uncertainty over how the transfer of these types of reports (e.g. for KYC etc.) will be impacted, if at all.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	N/A

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	The Financial Services Act 2013 contains secrecy provisions under section 133 (http://www.bnm.gov.my/documents/act/en_fsa.pdf).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

New Zealand

Key contact: Stephen Drain
Email: stephen.c.drain@nz.pwc.com
Tel: +64 9 355 8332

Postal address: Private Bag 92162,
Auckland 1142,
New Zealand

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The AMLCFTA came into effect on 30 Jun 2013. Regulations to the Act were gazetted on 30 Jun 2011.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The previous regime was captured under the Financial Transactions Reporting Act 1996 ("FTRA"). Lawyers remain subject to the obligations in the FTRA.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) The Reserve Bank of New Zealand for banks, life insurers, and non-bank deposit takers (http://www.rbnz.govt.nz/); b) The Financial Markets Authority for issuers of securities, trustee companies, futures dealers, collective investment schemes, brokers, and financial advisers (http://www.fma.govt.nz/); and c) The Department of Internal Affairs for casinos, non-deposit-taking lenders, money changers, and other reporting entities that are not covered by a) or b) (http://www.dia.govt.nz/).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The AML Supervisors provide guidance – all of which can be found at: http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-Codes-of-Practice-and-Guidelines?OpenDocument The guidance includes the following matters which are more commonly accessed by AML Practitioners: AML Programme guideline: http://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT-Programme-Guideline_FINAL_12-December-2011.pdf/\$file/AMLCFT-Programme-Guideline_FINAL_12-December-2011.pdf AML Risk Assessment guideline: http://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT_RiskAssessmentGuidelineFINAL_14June2011.pdf/\$file/AMLCFT_RiskAssessmentGuidelineFINAL_14June2011.pdf Interpreting “ordinary course of business”: http://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT_OrdinaryCourseofBusinessGuideline_FINAL.pdf/\$file/AMLCFT_OrdinaryCourseofBusinessGuideline_FINAL.pdf Amended Identity Verification Code of Practice: http://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_Amendment-to-IDVCOP-2013-FINAL-October-2013.pdf/\$file/AMLCFT_Amendment-to-IDVCOP-2013-FINAL-October-2013.pdf Auditing guideline: http://www.fma.govt.nz/assets/media/1339626/guideline-for-audits-of-risk-assessments-and-aml-cft-programmes.pdf Countries Assessment Guideline: http://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_CAG_July2012.pdf/\$file/AMLCFT_CAG_July2012.pdf Beneficial Ownership Guideline: http://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_BeneficialOwnershipGuideline_December2012.pdf/\$file/AMLCFT_BeneficialOwnershipGuideline_December2012.pdf User Guide: AML/CFT Report: http://www.dia.govt.nz/diawebsite.nsf/Files/AMLCFT-User-Guide-Oct-2014/\$file/AMLCFT_User-Guide_31-October-2014.pdf Wire Transfers: http://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_FactSheet_WireTransfer_Aug2013.pdf/\$file/AMLCFT_FactSheet_WireTransfer_Aug2013.pdf Territorial Scope of the AML/CFT Act 2009: http://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_TerritorialScope_December2012.pdf/\$file/AMLCFT_TerritorialScope_December2012.pdf Designated Business Groups Guideline: http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-Codes-of-Practice-and-Guidelines#DBG
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Under the AMLCFTA, reporting entities are required to conduct on-going Customer Due Diligence (“CDD”) (or “KYC”). Reporting entities are required to have “triggers” or similar built into their AML systems, to enable on-going CDD to be carried out. Specifically, reporting entities are required to re-verify existing customers where there is both a material change in the nature or purpose of the business relationship and the reporting entity considers that it has insufficient information on that customer. For anonymous accounts, a reporting entity is required to undertake standard customer due diligence when it becomes aware of existing anonymous accounts regardless of whether a material change in the nature or purpose of the business relationship has occurred.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	The AMLCFTA requires a risk based approach.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	A FATF Mutual evaluation Report was produced in October 2009: http://www.fatf-gafi.org/documents/documents/mutualevaluationofnewzealand.html There was also a second Follow up Report produced in October 2013 containing a detailed description of the actions taken by New Zealand in respect of all recommendations rated partially compliant or non-compliant in the 2009 Mutual Evaluation Report: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/FUR-New-Zealand-2013.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes. Under AMLCFTA, occasional transaction thresholds have been established. These are thresholds at which customer due diligence will need to be carried out in respect of occasional transactions including but not limited to: a) those over NZD9,999.99 (approx. USD6,540); b) cash transactions in a casino that are for NZD6,000 (approx. USD3,924) or more; c) travellers' cheques NZD5,000 (approx. USD3,270) ; d) money & postal orders NZD1,000 (approx. USD654); e) wire transfers NZD1,000 (approx. USD654); and f) foreign exchange transactions over NZD1,000 (approx. USD654).
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Section 15 of AMLCFTA stipulates the identification information to be obtained: Individuals: The person's full name, date of birth, (if the person is not the customer, the person's relationship to the customer) and the person's address and any information prescribed by regulations. The Amended Identity Verification Code of Practice 2013 requires an individual's name and date of birth to be verified. Legal persons: Full name, (if the person is not the customer, the person's relationship to the customer), address, company identifier or registration number and any information prescribed by regulations.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Individuals: Name and date of birth can be verified by using one form of photographic identification including <i>inter alia</i> a passport, national identity card, New Zealand Firearms Licence, New Zealand Refugee Travel document or New Zealand Certificate of Identity. Alternatively, one form of non-photographic identification can be used in combination with a secondary or supporting form of photographic identification or a New Zealand Driving Licence can be used in conjunction with other forms of documentation which are itemised in the Code of Practice. Further information can be found here: http://www.dia.govt.nz/pubforms.nsf/URL/AMLCFT_Amendment-to-IDVCOP-2013-FINAL-October-2013.pdf/\$file/AMLCFT_Amendment-to-IDVCOP-2013-FINAL-October-2013.pdf Identification documents must be certified as a true copy by a trusted referee who is at least sixteen years of age and one of the following: a) commonwealth representative (as defined in the Oaths and Declarations Act 1957); b) member of the police; c) justice of the peace; d) registered medical doctor; e) Kaumātua (Kaumātua means Māori Elder and is as verified through a reputable source); f) registered teacher; g) Minister of religion; h) lawyer (as defined in the Lawyers and Conveyancers Act 2006); i) notary public; j) New Zealand Honorary consul; k) Member of Parliament; l) chartered accountant (within the meaning of section 19 of the New Zealand Institute of Chartered Accountants Act 1996); or m) a person who has the legal authority to take statutory declarations or the equivalent in New Zealand.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	A beneficial owner is an individual who satisfies any one element or any combination of the elements listed below: a) who owns more than 25% of the customer; b) who has effective control of the customer; and c) the person(s) on whose behalf a transaction is conducted. Beneficial ownership threshold level is set at 25% meaning that any individuals owning 25% (or more) of a customer would be subject to CDD requirements. Identifying beneficial ownership of a customer is an obligation that must be satisfied, regardless of the level of risk associated with the customer. However, when deciding what reasonable steps to take to satisfy yourself that the customer's identity and information is correct, you may vary your approach depending on the risk assessment of the customer. The process for assessing customer risk and deciding how to identify and verify beneficial ownership should be set out in a Reporting Entity's AML/CFT programme. Section 16 of the AMLCFTA states: A reporting entity must: a) take reasonable steps to satisfy itself that the information provided under section 15 of the AML/CFT Act is correct; b) according to the level of risk involved, take reasonable steps to verify any beneficial owner's identity so that the reporting entity is satisfied that it knows who the beneficial owner is; c) if a person is acting on behalf of the customer, according to the level of risk involved, take reasonable steps to verify the person's identity and authority to act on behalf of the customer so that the reporting entity is satisfied it knows who the person is and that the person has authority to act on behalf of the customer; and d) verify any other information prescribed by regulations.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence can be conducted on a company that is a listed issuer (within the meaning of the Financial markets Conduct Act 2013) that is the issuer of quoted voting products (within the meaning of that Act) , a government department named in Schedule 1 of the State Sector Act 1988, a local authority as defined in section 5 of the Local Government Act 2002, the New Zealand Police, the New Zealand Security Intelligence Service or any other entity or class of entities specified in regulations (includes qualifying overseas entities of a similar type in jurisdictions with appropriate AML regimes). A reporting entity may also conduct simplified customer due diligence on a person who purports to act on behalf of a customer when the reporting entity already has a business relationship with the customer at the time the person acts on behalf of the customer; and the reporting entity has conducted one of the specified types of customer due diligence on the customer. A reporting entity may conduct simplified customer due diligence if: a) it establishes a business relationship with one of the aforementioned categories of customers particularised in section 18(2) AMLCFTA; b) one of the categories of customers particularised in 18(2) conducts an occasional transaction through the reporting entity; or c) a customer conducts a transaction or provides a product or service specified in regulations through the reporting entity. In the case of simplified due diligence, reporting entities are not required to conduct identification or verification of a beneficial owner of a customer.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Under AMLCFTA a reporting entity must conduct enhanced customer due diligence in accordance with sections 23 and 24 of the Act in the following circumstances: a) if the reporting entity establishes a business relationship with a customer that is: a. a trust or another vehicle for holding personal assets; b. a non-resident customer from a country that has insufficient anti-money laundering and countering financing of terrorism systems or measures in place; or c. a company with nominee shareholders or shares in bearer form; b) if a customer seeks to conduct an occasional transaction through the reporting entity and that customer is: a. a trust or another vehicle for holding personal assets; b. a non-resident customer from a country that has insufficient anti-money laundering and countering financing of terrorism systems or measures in place; or c. a company with nominee shareholders or shares in bearer form; c) if a customer seeks to conduct, through the reporting entity, a complex, unusually large transaction or unusual pattern of transactions that have no apparent or visible economic or lawful purpose; or d) when a reporting entity considers that the level of risk involved is such that enhanced due diligence should apply to a particular situation; or e) any other circumstances specified in the regulations. Wire Transfers: A reporting entity must conduct enhanced due diligence in accordance with Section 27 and 28 of the Act if it is an ordering institution, an intermediary institution, or a beneficiary institution in relation to a wire transfer. New/developing technologies: A reporting entity must conduct enhanced due diligence in accordance with Section 30 if: a) it establishes a business relationship with a customer that involved new or developing technologies, or new or developing products, that might favour anonymity; or b) a customer seeks to conduct an occasional transaction through the reporting entity that involves new or developing technologies, or new or developing products, that might favour anonymity.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	AML CFTA requires foreign Politically exposed persons to undergo enhanced due diligence in accordance with Section 26 of the act if: a) it establishes a business relationship with a customer who it has determined is a politically exposed person; or b) a customer who it has determined is a politically exposed person seeks to conduct an occasional transaction through the reporting entity.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Under Section 29 of AMLCFTA, the correspondent must: - gather enough information about the respondent to understand fully the nature of the respondent's business; - determine from publicly available information the reputation of the respondent and whether and to what extent the respondent is supervised for AML/CFT purposes, including whether the respondent has been subject to a money laundering or financing of terrorism investigation or regulatory action; - assess the respondent's money laundering and countering financing of terrorism controls to ascertain that those controls are adequate and effective; - obtain approval from its senior management before establishing a new correspondent banking relationship; - document the respective AML/CFT responsibilities of the correspondent and the respondent; and - be satisfied that, in respect of those of the respondent's customers who have direct access to accounts of the correspondent, the respondent: - has verified the identity of, and conducts ongoing monitoring in respect of, those customers; and - is able to provide to the correspondent, on request, the documents, data, or information obtained when conducting the relevant customer due diligence and ongoing customer due diligence.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, see section 39 AMLCFTA.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Under AMLCFTA for non-face-to-face transactions, identity documents can be endorsed by one of a number of nominated persons (see A10).

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Suspicious Transaction Reports ("STRs") are made to the New Zealand Police's Financial Intelligence Unit (FIU): http://www.police.govt.nz/advice/businesses-and-organisations/fiu/about

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – approx. 12,000 SARs Comparative GDP date is not available for this specific period.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No. New legislation requiring the mandatory reporting of wire transfers over NZ\$1000 (approx. USD654) is expected to come into force in 2017.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	It is an offence to: a) fail to report a suspicious transaction; b) provide false or misleading information; c) unlawfully disclose a STR; d) fail to keep adequate records in relation to filing of STRs; e) obstruct the investigation relating to a STR; f) disclose information in judicial proceedings; or g) structure transactions to avoid AML/CFT requirements. Penalties are: a) in the case of an individual, either or both of the following: a. a term of imprisonment of not more than two years, b. a fine of up to NZD300,000 (approx. USD196,200); and b) in the case of a body corporate, a fine of up to NZD5m (approx. USD3.2m). There are various other offences relating to non-compliance.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No, but it is encouraged. The FIU does not accept manual STR submissions. Submissions must be electronically submitted using "goAML", the Police's system, except in urgent circumstances: http://www.police.govt.nz/sites/default/files/publications/fiu-goaml-schema-introduction-v2-0-dec-2012.pdf
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No. AML Risk Assessments and Programmes must be audited, but not necessarily by an external party. This applied to all Reporting Entities, which includes Banks. Section 59(5) of the Act outlines that a person appointed to conduct an audit must not have been involved in: a) the establishment, implementation, or maintenance of the reporting entity's AML/CFT Programme; or b) the undertaking of the reporting entity's risk assessment.
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) a Reporting entity is required to complete an annual report on the entity's AML compliance and be submitted to the AML Supervisor (regulator). An audit must be conducted every two years, or at the request of the Supervisor. b) the Audit report is to be submitted to the reporting entity. The Entity must provide the audit opinion at the request of the supervisor. The annual report requires the entity to report the result (issues) from the Audit; and c) not necessarily, but it could be.
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	The Act does not specify what the Audit (external report) should contain. The Supervisor guidance referred to above gives guidance. a) no, but testing is completed by PwC NZ in accordance with international auditing standards b) no, but testing is completed by PwC NZ in accordance with international auditing standards; and c) yes the audit is also of the reporting entity's risk assessment.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	The AML/CFTA provides protection for the privacy of personal information when KYC or other functions are carried out by third parties. The protections must at least be equivalent to the protections in the Privacy Act 1993. The Privacy Act 1993 governs how agencies collect, use, disclose, store and give access to personal information. a) personal data is "<i>Personal information</i>" under the Act and defined as information about an identifiable individual; and includes information relating to a death that is maintained by the Registrar General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act. The definition covers material likely to be held for KYC purposes. b) the Privacy Act only applies to personal information and does not apply to corporate data; and c) there is no separate definition of sensitive data. No differentiation is made between how different types of personal information are to be treated under the Act. See: http://www.privacy.org.nz
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	The Privacy Commissioner is given the power to prohibit a transfer of personal information from New Zealand to another state, territory, province or other part of a country ("State") by issuing a transfer prohibition notice ("Notice") if it is satisfied that information has been received in New Zealand from one State and will be transferred by an agency to a third State which does not provide comparable safeguards to the Act and the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the OECD Guidelines and set out in schedule 5A. See: http://www.legislation.govt.nz/act/public/1993/0028/latest/whole.html#DLM3242810 There are further codes (enforceable by legislation) in place that prohibit some transfer of credit reports, criminal records and medical data. They are: a) Credit Reporting Privacy Code; b) Health Information Privacy Code; and c) Justice Sector Unique Identifier Code.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Specialist advice will be required.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No specific bank secrecy laws.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Pakistan

Key contact: Syed Faraz Anwer
Email: syed.faraz.anwer@pk.pwc.com
Tel: +92 21 32426711

Postal address: State Life Building
1-C; I.I.Chundrigar Road
Karachi

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Anti-Money Laundering Act was enacted in Mar 2010 after its approval by the Parliament of Pakistan. In addition, local banking regulator, the State Bank of Pakistan ("SBP"), has issued detailed AML and CFT regulations, together with guidelines on a risk based approach in 2012; both of which have subsequently been amended, and revised regulations issued in 2015. These guidelines can be found at the following links: http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf and http://www.sbp.org.pk/l_frame/AML-CFT-Guidelines-RiskBasedApproach.pdf
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The AML Ordinance was issued in 2007 followed by the Anti-Money Laundering Act in 2010. Subsequently AML and CFT regulations were issued in 2012 which were subject to amendments that have been incorporated in the revised regulations issued in 2015. The previous regulations required the following (which have now been stringently amended for inclusion in the revised regulations): a) verification of the identity of the customers shall be completed as soon as it is reasonably practicable but not later than five business days from the date of opening of the account; b) half yearly list is to be maintained by banks/DFIs highlighting all accounts/deposits where the business relationship needed to be closed on account of negative verification; c) obtain copy of CNIC from occasional customers/walk-in customers conducting cash transactions above INR1m (approx. USD15,000) whether carried out in a single operation or in multiple operations that appear to be linked; and d) currency Transaction Reports should be reported above the threshold of INR2.5m (approx. USD38,000).
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non-financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	The SBP is the regulator for AML controls for banking and related services while the Securities and Exchange Commission ("SECP") is the regulator for all other entities (http://www.sbp.org.pk/ http://www.secp.gov.pk/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The SBP has issued detailed guidelines on AML/CFT regulations, together with guidelines on risk based approach. The guidelines can be found at the following links: http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf and http://www.sbp.org.pk/l_frame/AML-CFT-Guidelines-RiskBasedApproach.pdf
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. SBP has issued detailed guidelines on AML/CFT regulations, together with guidelines on the risk based approach. The following is a link to these guidelines (http://www.sbp.org.pk/l_frame/AML-CFT-Guidelines-RiskBasedApproach.pdf). These contain detailed instructions on quantification of risk through a defined risk matrix, specific risk profiling of customers, specific high risk elements and recommendations for EDD, general high-risk scenarios/factors and general low risk scenarios/factors.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No. The latest Mutual Evaluation Report was performed by Asia Pacific Group on Money Laundering and is dated 09 Jul 2009 and is available on the following link (http://documents.worldbank.org/curated/en/2009/07/16413202/pakistan-mutual-evaluation-report-anti-money-laundering-combating-financing-terrorism). This report provides a summary of the AML/CFT measures in place in Pakistan and sets out Pakistan levels of compliance with the FATF recommendations.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	The AML and CFT regulations of 2015 are available at the following link (http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf) which specifies monetary thresholds for transactions executed by occasional customers/ walk-in customers and online transactions. Organisations however, have defined their own internal monetary thresholds.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	As per SBP AML/CFT Regulations (para 3 of Regulation 1: Customer Due Diligence), for identity and due diligence purposes, at the minimum, the following information shall also be obtained, verified and recorded on KYC/CDD form or account opening form: a) full name as per identity document; b) CNIC/Passport/NICOP/POC/ARC number or where the customer is not a natural person, the registration/incorporation number or business registration number (as applicable); c) existing residential address, registered or business address (as necessary), contact telephone number(s) and e-mail (as applicable); d) date of birth, incorporation or registration (as applicable); e) nationality or place of birth, incorporation or registration (as applicable); f) nature of business, geographies involved and expected type of counter-parties (as applicable); g) purpose of account; h) type of account; i) source of earnings; j) expected monthly credit turnover (amount and no. of transactions); and k) normal or expected modes of transactions. Verification of the identity of the customers shall be completed before business relations are established including verification from NADRA wherever required. In addition, there are defined documentation requirements to be fulfilled in relation to different categories of customers. For details please refer to Annexure I of SBP AML/CFT Regulations available on the link (http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf)

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	As per paragraph 4 of Regulation 1 of SBP AML and CFT regulations available on the link (http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf) the Bank/DFI shall verify identity documents of the customers from relevant authorities/document issuing bodies and where necessary using other reliable, independent sources and retain on record copies of all reference documents used for identification and verification. The particulars/CNIC of such persons must be verified from the National Database Registration Authority ("NADRA") through VeriSys or bio-metric technology. Verification of the identity of the customers and beneficial owners shall be completed before business relations are established including verification of CNIC/NICOP/POC from NADRA wherever required for customers under these regulations.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	As per paragraphs 7 and 8 of Regulation 1 of SBP AML and CFT regulations available on the link (http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf) Banks/DFIs shall take reasonable measures to obtain information to identify and verify the identities of the beneficial owner(s). Where the customer is not a natural person, the bank/DFI shall (i) take reasonable measures to understand the ownership and control structure of the customer for obtaining information required and (ii) determine the natural persons who ultimately own or control the customer. Verification of the identity of the beneficial owners shall be completed before business relations are established including verification from NADRA wherever required.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Detailed guidelines on general low risk scenarios/factors and their disposition are available in section 'F' (paragraphs 7-9) of SBP's AML/CFT Guidelines on Risk Based Approach available on the link (http://www.sbp.org.pk/l_frame/AML-CFT-Guidelines-RiskBasedApproach.pdf).
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Section 'D' of SBP's AML/CFT Guidelines on Risk Based Approach (paragraph 4-6) available on the link (http://www.sbp.org.pk/l_frame/AML-CFT-Guidelines-RiskBasedApproach.pdf) provides specific high risk elements and recommendations for EDD such as NPOs, NGOs, charities, associations, house wife accounts, landlords, proprietorships, self-employed professionals, on-line transactions, cash, wire transfers etc. Paragraph 5 provides high risk elements/factors bifurcated into customers, products and delivery channels, geography or locations.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Paragraph 29 of Regulation 1 of the SBP AML/CFT regulations available on the link (http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf) covers in detail the treatment for PEPs. In relation to PEPs and their close associates or family members, banks/DFIs shall: a) implement appropriate internal policies, procedures and controls to determine if a customer or beneficial owner is a PEP; b) obtain approval from the bank's senior management to establish or continue business relations where the customer or a beneficial owner is a PEP or subsequently becomes a PEP; c) establish, by appropriate means, the sources of wealth or beneficial ownership of funds, as appropriate; including bank/ DFI's own assessment to this effect; and d) conduct during the course of business relations, enhanced monitoring of business relations with the customer.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Regulations 2 of SBP AML/CFT regulations available on the link (http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf) cover this topic in detail.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes. As per Regulation 2 of SBP AML/CFT regulations (paragraph 4) available on the link (http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf). No bank/DFI shall enter into or continue correspondent banking relations with a shell bank and shall take appropriate measures when establishing correspondent banking relations, to satisfy them that their respondent banks do not permit their accounts to be used by shell banks.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In dealing with non-face-to-face transactions and/or relationships, adequate measures have been adopted by organizations. Additional due diligence may be required when: a) transactions do not make economic sense or are inconsistent with customer's business or profile; b) transactions involving locations of concern & wire transfer; and c) transactions involving unidentified parties.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	For banking organizations, to the local regulator i.e. State Bank of Pakistan (http://www.sbp.org.pk/) As per paragraph 8 of Regulation – 4 of the AML/CFT regulations available on the link (http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf). Banks/ DFIs, without disclosing the contents of Suspicious Transactions Reports ("STRs"), shall intimate the State Bank of Pakistan on bi-annual basis the number of STRs reported to the Financial Monitoring Unit ("FMU") established under the AML Act. The status report (indicating number of STRs only) shall reach the Director, BPRD within seven days of close of each half year.

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	As per paragraph 7 of Regulation – 4 of the AML/CFT, the regulations are available on the following link (http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf). Currency Transaction Reports ("CTRs") should be reported for transactions of INR2m (approx. USD30,000) and above as per requirements of the AML Act. This is also stated in the SBPs BPRD Circular Letter No. 04 of 2015 available on the link (http://www.sbp.org.pk/bprd/2015/CL4.htm)

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	As per paragraph 7 of Regulation - 4 of SBP AML/CFT regulations available on the link (http://www.sbp.org.pk/l_frame/Revised-AML-CFT-Regulations.pdf). Banks/DFIs should note that STRs, including attempted transactions, should be reported regardless of the amount of the transactions; and, the CTRs should be reported for transactions of INR2m (approx. USD30,000) and above as per requirements of the AML Act.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Liability for failure to file a suspicious transaction report and for providing false information is provided in paragraph 33 of the AML Act, 2010 available on the link (http://www.sbp.org.pk/about/act/Anti-Act-2010.pdf). Paragraph 34 of this Act lays out requirements with respect to non-disclosure of information and consequences of violation.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Yes by SBP. The following are extracts from SBP AML/CFT Regulation No. 4 (paragraph 5) available on the link (http://www.sbp.org.pk/frame/Revised-AML-CFT-Regulations.pdf) Banks/DFIs are advised to make use of technology and upgrade their systems and procedures in accordance with the changing profile of various risks. Accordingly, all banks/DFIs are advised to implement automated Transaction Monitoring Systems ("TMS") capable of producing meaningful alerts based on pre-defined parameters/thresholds and customer profile, for analysis and possible reporting of suspicious transactions. Further, banks/DFIs shall establish criteria in their AML/CFT Policies and/or Procedures for management of such alerts.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.
Q27.	If an external report on the bank's AML systems and controls is required: a) How frequently must the report be provided? b) To whom should the report be submitted? c) Is it part of the financial statement audit?
A27.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) Sample testing of KYC files? b) Sample testing of SAR reports? c) Examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) Does the definition of "personal data" cover material likely to be held for KYC purposes? b) How do the laws apply to corporate data? c) Does this country have a separate definition of "sensitive data"? How it defined and what is are the additional protections?
A29.	There are no specific laws on data protection except for certain data confidentiality clauses in specific arrangements/ transactions/ account types under the Banking Companies and Economic Reforms Act.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	None except for those specified above.

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	None except for those specified above.

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	None except for those specified above.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Philippines

Key contact: Rodel Acosta / Ma. Corazon Echavez
Email: rodel.acosta@ph.pwc.com / ma.corazon.echavez@ph.pwc.com
Tel: +63 (2) 845 2728 3012 3171

Postal address: 29th Floor, Philamlife Tower,
8767 Paseo de Roxas,
Makati City 1226, Philippines

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Philippine Republic Act ("R.A.") No. 9160 otherwise known as The Anti Money Laundering Act of 2001 ("AMLA") was signed into law on 29 Sept 2001 and took effect on 17 Oct 2001. The Implementing Rules and Regulations took effect on 2 April 2002. On 7 March 2003, R.A. No. 9194 (An Act Amending R.A. No. 9160) was signed into law and took effect on 23 March 2003. The revised Implementing Rules and Regulations took effect on 7 Sept 2003. R.A. 10365, which amends certain provisions of R.A. 9160, was signed into law on 15 Feb 2013 and took effect on 19 April 2013.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	The Anti Money Laundering Council ("AMLC") of the Philippines: http://www.amlc.gov.ph/
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	"Anti Money Laundering Act ("AMLA") at a Glance" summary: http://www.amlc.gov.ph/amla.html The Bangko Sentral ng Pilipinas ("BSP" (local central bank)) issues "Key Prudential Regulations" on Money Laundering for bank and non-bank financial institutions regulated by the BSP: http://www.bsp.gov.ph/regulations/key_aml.asp

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No. It should be noted that under R.A. 9160, only Covered Institutions are mandated by the AMLA to submit covered and suspicious transaction reports to the AMLC. These are: a) banks and all other entities, including their subsidiaries and affiliates, supervised and regulated by the BSP (or Philippine Central Bank); b) insurance companies and all other institutions supervised or regulated by the Insurance Commission; and c) securities dealers, "pre-need" companies, foreign exchange corporations and other entities supervised or regulated by the Philippine Securities and Exchange Commission. In addition to the above list per R.A. 9160, Covered Institutions under R.A 10365 now also include the following: a) jewellery dealers in precious metals and stones for transactions in the amount of PHP1m (approx. USD21,280) and above; b) company service providers which, as a business, provide any of the following services to third parties: a. acting as a formation agent of juridical persons; b. acting as a director or corporate secretary of a company, a partner of partnership, or a similar in relation to other juridical persons; c. providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal persons or arrangements; and d. acting as a nominee shareholder for another person; c) Persons who provide any of the following services: a. managing of client money, securities or other assets; b. management of bank, savings or securities accounts; c. organization of contributions for the creation, operation or management of companies; and d. creation operation or management of juridical persons or arrangements, and buying and selling business entities. Only Covered Institutions are required to establish and record the true identity of their clients based on official documents. They shall maintain a system of verifying their legal existence and organisational structure, as well as the authority and identification of all persons purporting to act on their behalf. Covered Institutions shall establish appropriate systems and methods based on internationally compliant standards and adequate internal controls for verifying and recording the true and full identity of their customers.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	None stated in local regulations or guidance.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	None. The AMLA defines 'covered transactions' as single transactions in cash or other equivalent monetary instruments involving a total amount in excess of PHP500,000 (approx. USD10,640) within one banking day, except for jewellery dealers in precious metals and stones who are required to report a single transaction equal to PHP1m (approx. USD21,280) or above. Regardless of whether these are covered transactions, the establishment and recording of the true identity of clients of Covered Institutions would cover all their clients.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: The following minimum information/documentation shall be obtained from individual customers: name; present address; permanent address; date and place of birth; nationality; nature of work and name of employer or nature of self-employment/business; contact numbers; tax identification number, social security system number or government services and insurance system number; specimen signature; source of funds; and names of beneficiaries in cases of insurance contracts. Corporate and Judicial Entities: The following minimum information/documentation shall be obtained from customers that are corporate or judicial entities, including shell companies and corporations: articles of incorporation/partnership; by-laws; official address or principal business address; list of directors/partners; list of principal stockholders owning at least 2% of the capital stock; contact numbers; beneficial owners, if any; and verification of the authority and identification of the person purporting to act on behalf of the client.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Individuals: Covered Institutions shall require customers to produce original documents of identity issued by an official authority, bearing a photograph of the customer. Examples of such documents are identity cards and passports. Corporate/Judicial Entities: Before establishing business relationships, Covered Institutions shall endeavour to ensure that the customer is a corporate or judicial entity which has not been or is not in the process of being dissolved or wound up, or that its business or operations have not been or are not in the process of being closed, shut down, phased out, or terminated. Applicable to all types: No new accounts shall be opened and created without face-to-face contact and full compliance with the above mentioned requirements. Though it is not defined in the local regulations or guidance, as a common business practice, banks and other institutions require copies of original documents to be certified as true copies by the issuing agency (e.g. copies of Articles of Incorporation/Partnership should be certified by the Securities and Exchange Commission), or by an independent lawyer or public notary (in the case of certifications and affidavits issued by an individual).
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	When dealing with customers who are acting as trustee, nominee, agent or in any capacity for and on behalf of another, Covered Institutions shall verify and record the true and full identity of the person(s) on whose behalf a transaction is being conducted. Covered Institutions shall retain accounts only in the true and full name of the account owner or holder. The provisions of existing Philippine laws regarding anonymous accounts, accounts under fictitious names, and all other similar accounts shall be prohibited.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	None stated in local regulations or guidance.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	None stated in local regulations or guidance.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	None stated in local regulations or guidance.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Nothing specific mentioned in local regulations or guidance for due diligence procedures performed for correspondent banking relationships. Nonetheless, when dealing with customers who are acting as trustee, nominee, agent or in any capacity for and on behalf of another, Covered Institutions shall verify and record the true and full identity of the person(s) on whose behalf a transaction is being conducted.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	No. However dealings with shell companies and corporations, being legal entities which have no business substance in their own right, but through which financial transactions may be conducted, should be undertaken with extreme caution.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	No new bank accounts shall be opened and created without face-to-face contact and full compliance with the above mentioned requirements. In case a Covered Institution has doubts when dealing with customers who are acting as trustee, nominee, agent or in any capacity for and on behalf of another, that they are being used as dummies in circumvention of existing laws, they shall immediately make the necessary inquiries to verify the status of the business relationship between the parties.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	AMLC: http://www.amlc.gov.ph/assistance.html
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Covered transactions are single transactions in cash or other equivalent monetary instruments involving a total amount in excess of PHP500,000 (approx. USD10,640) within one banking day, except for jewellery dealers in precious metals and stones which requires to report a single transaction amounting to PHP1m (approx. USD21,280) and above. Suspicious transactions are transactions with Covered Institutions, regardless of the amounts involved, where any of the following circumstances exists: a) there is no underlying legal/trade obligation, purpose or economic justification; b) the client is not properly identified; c) the amount involved is not commensurate with the business or financial capacity of the client; d) the transaction is structured to avoid being the subject of reporting requirements under the AMLA; e) there is a deviation from the client's profile/past transactions; f) the transaction is related to an unlawful activity/offense under the AMLA; and/or g) transactions similar or analogous to the above. The Land Transportation Authority and all its Registries of Deeds are required to submit to AMLC report on all real estate transactions involving an amount in excess of PHP500,000 (approx. USD10,640).
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Refer to A20 above.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Failure to keep records is committed by any responsible official or employee of a Covered Institution who fails to maintain and safely store all records of all transactions of the institution, including closed accounts, for five years from the date of the transaction/closure of the account. The penalty is six months to one year imprisonment or a fine of not less than PHP100,000 (approx. USD2,130) but not more than PHP500,000 000 (approx. USD10,640), or both. Malicious reporting is committed by any person who, with malice or in bad faith, reports/files a completely unwarranted report or false information relative to money laundering transaction against any person. Penalty is six months to four years imprisonment and a fine of not less than PHP100,000 (approx. USD2,130) but not more than PHP500,000 (approx. USD10,640), at the discretion of the court. The offender is not entitled to avail the benefits of the Probation Law. If the offender is a corporation, association, partnership or any judicial person, the penalty shall be imposed upon the responsible officers, as the case may be, who participated in, or allowed by their gross negligence, the commission of the crime. If the offender is a judicial person, the court may suspend or revoke its license. If the offender is an unknown, he shall, in addition to the penalties prescribed, be deported without further proceedings after serving the penalties prescribed. If the offender is a public official or employee, he shall, in addition to the penalties prescribed, suffer perpetual or temporary absolute disqualification from office, as the case may be. Breach of confidentiality: When reporting covered or suspicious transactions to the AMLC, Covered Institutions and their officers/employees are prohibited from communicating directly or indirectly, in any manner or by any means, to any person/entity/media, the fact that such report was made, the contents thereof, or any other information in relation thereto. In case of violation thereof, the concerned official and employee of the Covered Institution shall be criminally liable. Neither may such reporting be published or aired in any manner or form by the mass media, electronic mail or other similar devices. In case of a breach of confidentiality published or reported by media, the responsible reporter, writer, president, publisher, manager and editor-in-chief shall also be held criminally liable. The penalty is 3 to 8 years imprisonment and a fine of not less than PHP500,000 (approx. USD10,640) but not more than PHP1m (approx. USD21,280).

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No, however, Covered Institutions are required to register with the AMLC and enrol in the online transactions reporting module and covered/suspicious transaction reports module: http://www.amlc.gov.ph/archive.html#Registration Detailed guidance can be found here: http://www.amlc.gov.ph/archive/Reporting%20Procedures.pdf

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Authority to inquire into Bank Deposits: Notwithstanding the provisions of R.A. 1405 (Law on Secrecy of Bank Deposits), as amended, R.A. No. 6426, as amended, R.A. No. 8791, and other laws, the AMLC may inquire into or examine any particular deposit or investment with any banking institution or non-bank financial institution upon order of any competent court in cases of violation of this act when it has been established that there is probable cause that the deposits/investments are involved/related to an unlawful activity as defined in Sec. 3(i) of the AMLA or a money laundering offense under Sec. 4 thereof; except that no court order shall be required in cases involving kidnapping for ransom; drug trafficking and related offenses; and hijacking, destructive arson and murder, including those perpetrated by terrorists against non-combatant persons and similar targets.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	None.
Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	The Data Protection Act (Republic Act [RA] 10173) was signed into law 15 Aug 2012. It protects the integrity and confidentiality of individual personal information and communications systems in the government and the private sector, by penalising the unauthorised disclosure of personal information. It specifically exempts, however, information necessary for banks and financial institutions as part of anti-money laundering efforts, and personal data processed by central monetary authorities and law enforcement and regulatory agencies, among others: a) personal data as defined under Section 3(g) of RA 10173 refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual. From the definition it likely covers information used for KYC purposes, and the specific exemption only applies to agencies, etc. that are implementing anti-money laundering laws; b) there is no specific provision in the Data Protection law that covers corporate data. However, it provides that processing of personal information is regulated by the law and applies to natural and juridical persons involved in personal information processing; and c) the Data Protection law likewise provides a separate definition for "sensitive personal information" such that it refers to personal information: a. about an individual's race, ethnic origin, marital status, age, colour, and religious, philosophical or political affiliations; b. about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings; c. issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and d. specifically established by an executive order or an act of Congress to be kept classified. Lawful processing of personal information is allowed under the law, subject to certain conditions and requirements that must be complied with. On the other hand, processing of sensitive personal information is prohibited, except under specific exempt circumstances as provided under Section 13 of the Act. There is also a higher penalty imposed for unlawful processing of sensitive personal information (imprisonment ranging from 3 years to 6 years, and a fine of PHP500,000 (approx. USD10,640) to a maximum of PHP4m (approx. USD85,120).
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Transfer of credit records by duly authorised entities to non-authorised ones is regulated and prohibited, unless written consent or authorisation is obtained (See RA 9510, An Act Establishing the Credit Information System). With regards to criminal records and medical data, there are no specific provisions addressing these specific types of information/reports, other than those mentioned falling within the ambit of personal information and sensitive personal information. (Sections 3(g) and 3(l), RA 10173).

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Transfer of information is restricted and subject to the provisions of Presidential Decree (PD) No 1718, issued in 1980, that restricts the transfer of information vital to Philippine national interests to foreign jurisdictions. In this regard, prior approval from the Office of the President of the Philippines must first be obtained before any such transfer is made.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes, the Philippines has a Bank Secrecy Law (RA 1405), which provides that all deposits with banks or banking institutions in the Philippines are considered confidential, and may only be inquired into and examined upon written permission of the depositor, or upon order of the courts.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Singapore

Key contact: Kwok Wui San / Thangaraja Nada Raja
Email: wui.san.kwok@sg.pwc.com /
thangaraja.nada.raja@sg.pwc.com
Tel: +65 (0) 6236 3087 / +65 (0) 6236 3321

Postal address: 8 Cross Street,
17-00 PWC Building,
Singapore, 048424

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2007.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.)? Please include link to the regulator(s) website
A3.	In respect of (a) and (b), AML controls are regulated by the Monetary Authority of Singapore ("MAS"). Please refer to link: http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions.aspx (c) AML is regulated by the Casino Regulatory Authority for casinos, and generally, by the Commercial Affairs Department of Singapore. Please refer to the respective links: http://www.cra.gov.sg/cra/regulations.aspx/93 and http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	a) guidance on AML/CFT regulations (http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism.aspx); b) guidance on Trade Finance and Correspondent Banking (http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism/Guidance-Papers/2015/Guidance-on-AML-CFT-Controls-in-Trade-Finance-and-Correspondent-Banking.aspx); c) guidance on Private Banking Controls (http://www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-Terrorism-And-Targeted-Financial-Sanctions/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism/Guidance-Papers/2014/Guidance-on-Private-Banking-Controls.aspx); d) MAS designation of tax crimes as money laundering predicate offences in Singapore (http://www.mas.gov.sg/News-and-Publications/Consultation-Paper/2012/Consultation-Paper-on-Designation-of-Tax-Crimes-as-Money-Laundering-Predicate-Offences-in-Singapore.aspx); e) Casino Regulatory Authority regulations (http://www.cra.gov.sg/cra/regulations.aspx/93); f) Commercial Affairs Department AML/CFT handbook (http://www.cad.gov.sg/publications/cad-anti-money)

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes. Financial Institutions ("FIs") are required to perform customer due diligence measures in relation to their existing customers before the introduction of the new AML regime according to regulatory requirements, based on their own assessment of materiality and risk, taking into account any previous measures applied, the time when the measures were last applied to such existing customers and the adequacy of data, documents or information obtained.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. FIs are required to conduct an enterprise wide risk assessment to identify, assess and understand, their money laundering and terrorism financing risks in relation to - their customers; - the countries or jurisdictions its customers are from or in; - the countries or jurisdictions the FI has operations in; and - the products, services, transactions and delivery channels of the FI. FIs are also required to: - document their risk assessments; - consider all the relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation to be applied; - keep their risk assessments up-to-date; and - have appropriate mechanisms to provide its risk assessment information to the Authority. Additionally, FIs are required to: - develop and implement policies, procedures and controls, which are approved by senior management, to enable the FI to effectively manage and mitigate the risks that have been identified by the FI or notified to it by the Authority or other relevant authorities in Singapore; - monitor the implementation of those policies, procedures and controls, and enhance them if necessary; - perform enhanced measures where higher risks are identified, to effectively manage and mitigate those higher risks; and - ensure that the performance of measures or enhanced measures to effectively manage and mitigate the identified risks address the risk assessment and guidance from the Authority or other relevant authorities in Singapore.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes. FATF Mutual Evaluation undertaken in Feb 2008. Second follow-up report was performed in Feb 2011: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/FoR%20Singapore.pdf In Oct 2013, Singapore launched a National Risk Assessment ("NRA") to comprehensively assess money laundering and terrorist financing risks in the country. This is in line with the revised FATF standards which expect countries to identify and assess money laundering and terrorist financing risks, and to keep the assessment up-to-date. Please refer to the link (http://www.mas.gov.sg/~media/resource/news_room/press_releases/2014/Singapore%20NRA%20Report).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Customer due diligence is required. However the extent of due diligence performed may vary based on the risk. For example, in respect of simplified customer due diligence, the regulation states that a bank may perform such simplified customer due diligence measures as it considers adequate to effectively identify and verify the identity of the customer, a natural person appointed to act on the customer's behalf and any beneficial owner, if it is satisfied that the risks of money laundering and terrorist financing are low (certain conditions apply).
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Requirement to identify and verify customers, natural persons appointed to act on a customer's behalf and beneficial owners. This includes: a) identifying each natural person who acts or is appointed to act on behalf of the customer by obtaining at least the following information of such natural person: a. full name, including any aliases; b. unique identification number (such as an identity card number, birth certificate number or passport number); c. residential address; d. date of birth; and e. nationality. b) verifying the identity of each natural person using reliable, independent source data, documents or information. c) verifying the due authority of each natural person appointed to act on behalf of the customer by obtaining at least the following: a. the appropriate documentary evidence authorising the appointment of such natural person by the customer to act on his or its behalf; and b. the specimen signature of such natural person appointed. d) inquiring if there exists any beneficial owner in relation to a customer; e) where there is one or more beneficial owner in relation to a customer, identifying the beneficial owners and taking reasonable measures to verify the identities of the beneficial owners using the relevant information or data obtained from reliable, independent sources; and f) retaining copies of all reference documents used to verify the identity of these persons.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Where the customer is unable to produce an original document, FIs may consider accepting a copy of the document: a) that is certified to be a true copy by a suitably qualified person (e.g. a notary public, a lawyer or certified public or professional accountant); or b) if a member of the FI's staff independent of the customer relationship has confirmed that he has sighted the original document.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	There are requirements to take reasonable measures to enquire if any beneficial owner exists in relation to a customer. Where there is one or more beneficial owner(s) in relation to a customer, the FI needs to take reasonable measures to obtain information sufficient to identify and verify the identities of the beneficial owner(s), by identifying the beneficial owners and taking reasonable measures to verify the identities of the beneficial owners using the relevant information or data obtained from reliable, independent sources. The FI shall: a) for customers that are legal persons: a. identify the natural persons (whether acting alone or together) who ultimately own the legal person; b. to the extent that there is doubt under subparagraph (i) as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, identify the natural persons (if any) who ultimately control the legal person or have ultimate effective control of the legal person; and c. where no natural persons are identified under subparagraph (i) or (ii), identify the natural persons having executive authority in the legal person, or in equivalent or similar positions; b) for customers that are legal arrangements: a. for trusts, identify the settlors, the trustees, the protector (if any), the beneficiaries (including every beneficiary that falls within a designated characteristic or class), and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust (including through a chain of control or ownership); and b. for other types of legal arrangements, identify persons in equivalent or similar positions, as those described under subparagraph a. Where the customer is not a natural person, the FI shall understand the nature of the customer's business and its ownership and control structure.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	FIs may perform simplified customer due diligence measures it considers adequate to effectively identify and verify the identity of the customer, a natural person appointed to act on the customer's behalf and any beneficial owner, if it is satisfied that the risks of money laundering and terrorist financing are low. The assessment of low risks shall be supported by an adequate analysis of risks by the FI, and the simplified CDD measures shall be commensurate with the level of risk, based on the risk factors identified. However simplified customer due diligence arrangements are not allowed in certain circumstances, such as: a) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures; b) where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the bank for itself or notified to banks generally by the Authority, or other foreign regulatory authorities; or c) where the FI suspects that money laundering or terrorism financing is involved.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence measures are required to be taken in situations such as: a) when dealing with PEPs; b) when dealing with types of customers, business relations or transactions the FI assesses to present a higher risk for money laundering and terrorist financing; and c) when dealing with business relations and transactions with any person originating from or based in countries and jurisdictions known to have inadequate AML/CFT measures, or in a country or jurisdiction in relation to which the FATF has called for countermeasures.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	A bank may adopt a risk-based approach in determining whether to perform enhanced CDD measures or the extent of enhanced CDD measures to be performed for: a) domestic politically exposed persons, their family members and close associates; b) international organisation politically exposed persons, their family members and close associates; or c) politically exposed persons who have stepped down from their prominent public functions, taking into consideration the level of influence such persons may continue to exercise after stepping down from their prominent public functions, their family members and close associates. Except in cases where their business relations or transactions with the bank present a higher risk for money laundering or terrorism financing.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Generally, a bank shall satisfy itself of the money laundering risks and perform the following, in addition to CDD measures, when providing correspondent banking or other similar services: a) assess the suitability of the respondent FI by taking the following steps; a. gather adequate information about the respondent FI to understand fully the nature of the respondent FI's business, including making appropriate inquiries on its management, its major business activities and the countries or jurisdictions in which it operates; b. determine from any available sources the reputation of the respondent FI and the quality of supervision over the respondent FI, including whether it has been the subject of money laundering or terrorism financing investigation or regulatory action; and c. assess the respondent FI's AML/CFT controls and ascertain that they are adequate and effective, having regard to the AML/CFT measures of the country or jurisdiction in which the respondent FI operates; b) clearly understand and document the respective AML/CFT responsibilities of each FI; and c) obtain approval from the bank's senior management before providing correspondent banking or similar services to a new FI.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	It is prohibited to enter into or continue correspondent banking relations with a shell bank.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Where there is no face-to-face contact, the FI is required to carry out customer due diligence measures that are as stringent as those that would be required to be performed if there were face-to-face contact.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website?
A18.	Suspicious Transaction Reports ("STRs") are reported to the Suspicious Transactions Reporting Office ("STRO") of the Commercial Affairs Department of Singapore (http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office), and a copy should also be extended to the Monetary Authority of Singapore ("MAS") for information.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year?
A19.	Volume of SARs: 2014 – 29,082 SARs (Source: http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office/statistics) GDP (in current prices): 2014 – USD307,782m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD10.6m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Reports to the STRO must be made if there is any suspicion of money laundering or terrorist financing. A FI should consider if the circumstances are suspicious so as to warrant the filing of an STR and document the basis for its determination, including where: a) the FI is for any reason unable to complete customer due diligence measures as required by regulations; or b) the customer is reluctant, unable or unwilling to provide any information requested by the FI, decides to withdraw a pending application to establish business relations or a pending transaction, or to terminate existing business relations.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	There is no de-minimis threshold. The emphasis is on the suspicious nature of the transaction rather than the quantum.
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Yes. Under Section 39 of the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act (Cap. 65) ("CDSA"), it is mandatory for any person to lodge an STR as soon as is reasonably practicable if he knows or has reason to suspect that any property may be connected to a criminal activity. The failure to do so may constitute a criminal offence, and is liable on conviction to a fine not exceeding SGD20,000 (approx. USD13,870). Under Section 48 of the CDSA, tipping-off is a criminal offence punishable by on conviction to a fine not exceeding SGD30,000 (approx. USD20,800) or to imprisonment for a term not exceeding three years or to both.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No, there is no legal or regulatory requirement to use such technology. However, FIs are required to monitor on an ongoing basis, their business relations with customers, observing the conduct of the customer's account and scrutinise transactions undertaken throughout the course of business relations, to ensure that the transactions are consistent with the FI's knowledge of the customer, its business and risk profile and where appropriate, the source of funds. For the purposes of ongoing monitoring, the FI is required to put in place and implement adequate systems and processes, commensurate with the size and complexity of the FI, to: a) monitor its business relations with customers; and b) detect and report suspicious, complex, unusually large or unusual patterns of transactions.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes. Under the Terrorism (Suppression of Financing) Act (Chapter 325), every person who provides financial services, knowing or having reasonable grounds to believe that they will be used, for the purpose of facilitating or carrying out any terrorist act, or for benefiting any person who is facilitating or carrying out such activity, shall be guilty of an offence. FIs may apply to the Minister for an exemption, subject to various conditions being met.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes but subject to compliance with conditions and restrictions.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No. However, banks are required to maintain an audit function that is adequately resourced and independent, and that is able to regularly assess the effectiveness of the bank's internal policies, procedures and controls, and its compliance with regulatory requirements. A bank's AML/CFT framework should be subject to periodic audits (including sample testing). Such audits should be performed not just on individual business functions but also on a bank-wide basis. Auditors should assess the effectiveness of measures taken to prevent ML/TF. The frequency and extent of the audit should be commensurate with the ML/TF risks presented and the size and complexity of the bank's business.
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	No specific requirement.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	No specific requirement.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes: a) data protection laws were introduced in 2012 under the Personal Data Protection Act ("PDPA"). The PDPA protects "personal data" in relation to individuals. As such, personal data would cover material likely to be held for KYC purposes; b) all customer data, including corporate data, are subject to banking secrecy laws and regulations; c) however, our AML laws on suspicious reporting to the designated authority overrides secrecy provisions under PDPA and banking secrecy laws.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	There are banking confidentiality provisions under MAS requirements which protect customers' information. Customers' information may only be disclosed to specified parties under certain conditions. For example, to auditors in their annual audit of the bank, and under Singapore's Exchange of Information framework with its tax agreement partners etc.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Singapore's legal system is based on the English common law system. Apart from referring to written laws, the Courts may refer to case law or decisions, including taking guidance from those of Commonwealth jurisdictions such as Australia and Canada.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. As stated above, there are banking confidentiality provisions under MAS requirements which protect customers' information.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



South Korea

Key contact: Byoung-jin Park
Email: byoung-jin.park@kr.pwc.com
Tel: + 82 2 709 – 7927

Postal address: LS Yongsan Tower,
92, Hnagang-daero. Yongsan-gu,
Seoul 04386, Korea

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2001 (amended 2005, with stricter customer due diligence and money laundering regulations implemented in 2007).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	Under the 2005 amendment, responsibility for customer due diligence and filing of Cash Transaction Reports ("CTRs") was imposed. Customer due diligence has been self-controlled by each financial institution and is now compulsory in the 2007 regulations. In 2013, the requirement to report a specific amount of financial transactions as Suspicious Transaction Reports ("STRs") was abolished. In the case of sending money through wire transfers, financial institutions should report related information to the Korea Financial Intelligence Unit ("KoFIU"). An amendment of the 'Act on Reporting and Using Specified Financial Transaction Information' requires the identification of the beneficial owners and/or customers. Financial institutions may reject transactions with customers who refuse to provide information (Enforcement Date: Jan.1, 2016).
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	The Korea Financial Intelligence Unit ("KoFIU") (http://www.kofiu.go.kr/) is the AML regulator for financial institutions.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes. KoFIU has provided guidelines for regional AML Requirements (http://www.kofiu.go.kr/KOFIU/korean/sub03/law02_view.jsp?mm=3&sm=2&srl_no=11).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, financial institutions shall conduct CDD for customers with whom business relationships had already been established before the amendment of the Act took effect on 22/12/2008. CDD shall be conducted when: a) a transaction of high importance takes place; b) the standards of customer identification data changes significantly; c) there is a material change in the operation method of the account; or d) the financial institution becomes aware that customer information is not fully acquired.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. Prior to the 2007 amendments of the AML regulations, a risk based approach to customer due diligence was optional. Under the 2007 amendments, a risk based approach is compulsory and guidelines have been prepared. KoFIU released risk based approach ("RBA") guidelines to Korean banks in Nov. 2014. This was so a RBA could be applied to general AML compliance of financial institutions and to customers. According to these guidelines, Korean banks are in the process of developing a RBA AML structure
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No. In 2009, Korea was the subject of a FATF Mutual Evaluation. On June 2014, the 8th follow-up report on 2009 Mutual Evaluation report was issued. The relevant report is available on the FATF Website: http://www.fatf-gafi.org/topics/mutualevaluations/documents/follow-up-report-korea-2014.html There is a plan to have a mutual assessment in 2018.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes. Occasional financial transactions include not only one-off transactions above the threshold, but also occasional financial transactions made under the same name of a person with the accumulated amount over the period of 7 days exceeding the threshold. Here, the threshold refers to: a) USD10,000 or the amount denominated in another currency equivalent thereto, in the cases of foreign exchange transactions denominated in foreign currency; or b) KRW20,000,000 (approx. USD16,000), in the cases of any other financial transactions than provided for in subparagraph 1 of Article 10-3 of the Enforcement Decree.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	For individual customer verification: a) name; b) date of birth, gender (confined to foreign non-residents); c) identification number; d) nationality (confined to foreign non-residents); and e) address and contact information (in the case of foreign non-residents actual address and contact information). For legal entity customer verification: a) name of legal person (organisation); b) identification number; c) address and location of headquarters and offices (in the case of foreign legal person, actual location of office and contact information); d) business type (in the case of for-profit organisation); and e) purpose of establishment (in the case of non-profit organisation).
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	None stated in local regulations or guidance.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	If any suspicious fact about a beneficial owner is detected from a transaction, the regulations advise that the identity of the person and the purpose of the transaction be obtained, although there is no detailed guidance on this. Identification and verification processes of customers have been strengthened in the updated regulations and guidance, including verification of beneficial ownership.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Financial institutions may conduct simplified CDD when legal persons fall into each of the following categories: a) national and municipal governments and public organizations; b) financial institutions subject to supervision and inspection (excluding casino operators); and c) stock-listed or KOSDAQ-listed companies, which are subject to regulatory disclosure requirements.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	The updated regulations recommend that enhanced customer due diligence is applied in respect of customers that fall into major high risk categories specified by the FATF, such as PEPs, private banking, correspondent banking and terrorist facilitators/financiers.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Financial institutions shall conduct enhanced due diligence when customers (or beneficial owners) are identified as foreign PEPs, and take due measures to identify the source of funds or assets. Such measures include identifying the following additional information: a) identification information of family members with authority over account transaction or a person with a close relationship with foreign PEPs; and b) information of legal persons or organizations associated with foreign PEPs. Financial institutions shall obtain approval from senior management for any of the following purposes: a) to accept the account-opening transaction by a foreign PEP; and b) to maintain business relationships when customers, (or beneficial owners) who already opened accounts, are identified as foreign PEPs.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The following enhanced due diligence must be performed: a) financial institutions shall establish and operate procedures and control measures necessary for preventing and mitigating the risks of money laundering and terrorist financing related to correspondent banking services when entering into correspondent arrangements; b) the correspondent bank is prohibited from entering into or continuing correspondent arrangements with banks that have no physical presence or have been established in a country or jurisdiction where supervision is not available; c) the correspondent bank shall take appropriate measures to ensure that the respondent bank prevents its correspondent banking account from being used by shell banks; d) when entering into correspondent arrangements, the correspondent bank shall take each of the following measures with regard to the respondent bank: a. identifying the respondent bank's operational and business characteristics by collecting information on the respondent bank's governance structure, major business activity, and main location (or country); b. based on available and publicly disclosed information, evaluating the reputation of the respondent bank and level of supervision or regulation on the respondent bank including whether it is subject to investigation into cases of money laundering and terrorist financing; c. assessing the adequacy and effectiveness of AML/CFT measures for a jurisdiction or country where the respondent bank is mainly located and of AML/CFT control measures taken by the respondent bank; and d. documentation of AML/CFT obligations between correspondent and respondent bank; and e) when the service of providing a customer with direct access to a correspondent banking account is included in the correspondent arrangement, the following measures should be taken: a. The respondent bank shall perform CDD on the customer who intends to conduct a transaction using a payable-through account; and b. Upon request from the correspondent bank, the respondent bank shall provide customer identification information.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Financial institutions must ensure that all electronic financial services and products, such as ATM transactions, internet banking and telephone banking, are based on accounts established through face-to-face identification. Financial institutions must also have policies and procedures in place to address any specific risks associated with non face-to-face transactions, and must implement them when establishing new business relationships and conducting ongoing customer due diligence.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Suspicious activity reports are made to KoFIU (http://www.kofiu.go.kr).
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 – 378,742 SARs (Source: KoFIU) GDP (in current prices): 2013 – USD1,305,605m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD3.5m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, financial institutions in Korea have obligations to submit Currency Transaction Reports ("CTRs"), which is the requirement for reporting transactions above KRW20,000,000 (approx. USD16,000) to KoFIU.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Yes, imprisonment for a period not exceeding 1 year or a fine not exceeding KRW10 million (approx. USD8,000) per individual responsible for SAR reporting.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No, recommended to apply a transaction monitoring system.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes, on transaction monitoring progress, linked or individual transactions identified as suspicious should be reported to KoFIU.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No, local AML regulations prohibit SARs to be reported outside of Korea. Also, transferring information of individual and financial transactions is prohibited by the Korean Real Name Act.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, a), b), and c) are protected by Personal Protection Information Act.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Taiwan

Key contact: Eric Tsai
Email: eric.tsai@tw.pwc.com
Tel: +886 2 2729 6687

Postal address: 27F, 333 Keelung Road,
Section 1, Taipei,
Taiwan 110

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Taiwan's anti-money laundering legislation is embodied in The Money Laundering Control Act, 1996 (amended in 2003, 2006, 2007, 2008, and 2009, hereinafter the "Act").
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	Under Article 5 of the Act, banks, trust and investment corporations, credit cooperative associations, credit department of farmers' associations, credit department of fishermen's associations, Agricultural Bank of Taiwan, postal service institutions which also handle the money transactions of deposit, transfer and withdrawal, negotiable instrument finance corporations, credit card companies, insurance companies, securities brokers, securities investment and trust enterprises, securities finance enterprises, securities investment consulting enterprises, securities central depository enterprises, futures brokers, trust enterprises, and other financial institutions designated by the Financial Supervisory Commission (hereinafter the "FSC") fall within the definition of "financial institutions" and are thus subject to the Act. The FSC's website may be found at (http://www.fsc.gov.tw/en/index.jsp). In addition, jewellery, retail businesses and other institutions having the risk of being used for money laundering and having been designated by the Ministry of Justices in consultation with such institutions' competent authority are also subject to the Act. The website of Ministry of Justice may be found at (http://www.moj.gov.tw/mp095.html). However, the implementation and enforcement of the Act may involve several government agencies/departments. For instance: a) the FSC is in charge of adopting AML rules for financial institutions and for ongoing supervision; b) for AML issues concerning wire transfers, the Central Bank of Taiwan serves as a co-rule-making body along with the FSC. The Central Bank of Taiwan's website may be found at (http://www.cbc.gov.tw/mp2.html); c) the Anti-Money Laundering Division, previously Anti-Money Laundering Prevent Center, of the Investigation Bureau of Ministry of Justice, which serves as the financial intelligence unit of Taiwan, is in charge of receiving and compiling money transaction records. The Division's website may be found at (http://www.mjib.gov.tw/mlpc/); and d) the prosecutors and courts are responsible for the prosecution and trial of money laundering crimes.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	As of Nov 2014, each type of "financial institution" under Article 5 of the Act, except Agricultural Bank and securities central depository enterprises, has respective, standalone AML practical guidance. While Chinese versions of the practical guides are available through paid-databases, there is no public database that makes English versions of all of these practical guides comprehensively available.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	There is no requirement to retrospectively verify the identity of customers before the Act was adopted and became effective. However, in any of following events, financial institutions are required to verify a customer's identity even after the customer has a pre-existing relationship with the financial institution: a) any domestic transfer or remittance that exceeds TWD30,000 (approx. USD900); b) discovery of a transaction suspicious of money laundering or financing of terrorism, or remittance from countries or regions with high risk of money laundering or financing of terrorism; or c) suspicion of authenticity or sufficiency of customer identity information having previously acquired.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. The measures to verify customer identity and continuous monitoring are implemented in accordance with risk-based approach, under which verification of customer identity or continuous monitoring are strengthened for high risk circumstances and simplified measures are taken for low risk circumstances.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Taiwan has not been the subject of a FATF Mutual Evaluation since 2008. With respect to the IMF assessment, Taiwan was the subject of the "IMF Working Paper - A Quantitative Assessment of Financial Conditions in Asia" dated Jul 2011 (http://www.imf.org/external/pubs/ft/wp/2011/wp11170.pdf).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Under applicable practical guidance, customer due diligence is required upon: a) the establishment of business relationship; b) discovery of a transaction which raises suspicion of money laundering or financing of terrorism, or remittance from countries or regions with a high risk of money laundering or financing of terrorism; or c) suspicion of authenticity or sufficiency of customer identity information having previously acquired, regardless of any transaction threshold. In the case of one-off transactions, customer due diligence is required where: a) single receipt or payment of cash or exchange of new bills exceeds TWD500,000 (approx. USD15,000); or b) domestic cash remittance exceeds TWD30,000 (approx. USD900) but lower than TWD500,000 (approx. USD15,000). In addition, customer due diligence is also required for any domestic transfer or remittance that exceeds TWD30,000 (approx. USD900).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: a) identification of customer and verification of identity must be based on reliable, independent original copy, information or data, the photocopies of which must be kept in custody or on record; b) in cases where an agent carries out an account-opening or a transaction, the authority must be verified and the identity of the agent must be confirmed by way of a) above; c) reasonable measures to identify and verify the beneficiary of a customer must be adopted; and d) verification of customer identity should include inquiries on the purpose and nature of business. Legal entities: In case where a customer is a corporation, the following information must be acquired to identify the beneficiary of the customer: a) the identity of ultimate individual beneficiary in control (such as name, birth date, nationality, and ID number). Control means any person holding 25% or more of the shares or capital of a corporation; b) in case where there is no individual beneficiary in control or suspicion whether the individual beneficiary in control is the ultimate beneficiary, inquiries should be made as to whether there is any individual who exercise control over the customer in any other manner. When necessary, the customer must be required to issue declaration to verify the identity of ultimate beneficiary; and c) in case where no individual beneficiary in control is found in accordance with a) and b) above, a financial institution must adopt reasonable measures to verify the identity of individual holding high-level executive positions (such as director, president, or other equivalent or similar positions).
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	For purpose of account-opening or transaction, original copies of identification documentation must be provided for review and verification.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	When a customer is trustee of a trust, the identities of settlor, trustee, guardian, beneficiary and any other individual that has the power to effectively control the trust account must be acquired to verify the ultimate beneficiary of the customer.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	While practical guidance allows the adoption of simplified due diligence arrangements in low risk circumstances, there is no definition of what constitute low risk circumstances in practical guidance. On the other hand, simplified customer due diligence is prohibited in high risk circumstances, which are defined as: a) where customers are from a high risk country or region where no effective anti-money laundering or counter-financing terrorism measures are available; or b) where there is reasonable suspicion that the customer or transaction is implicated with money laundering or financing of terrorism.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Please see A12 above.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	In the case of an over-the-counter request for account-opening, a financial institution must conduct due diligence on whether a customer is a foreign PEP with a database established and maintained by the financial institution, or outside information sources. Secondly, practical guidance requires that heightened risk control measures and regular review thereof must apply to such foreign PEPs.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Banks are required to: a) gather sufficient information about a respondent institution to fully understand the nature of the respondent's business and to determine, from publicly available information, the reputation of the institution and the quality of supervision, including whether it complies with AML and counter financing of terrorism regulations; b) assess the respondent institution's AML and counter financing of terrorism controls and effectiveness thereof; c) obtain approval from senior management before establishing new correspondent relationships; d) document the respective AML and counter financing of terrorism responsibilities of each institution; e) where a correspondent relationship involves "payable-through accounts", it is necessary to ensure that the correspondent bank has strictly identified the customer's identity and is able to provide the relevant identity information if necessary; and f) not to establish correspondent relationships with any shell banks or any foreign financial institution which allows a shell bank to open an account with it.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Banks are prohibited from establishing a correspondent relationship with any shell banks or any foreign financial organisation which allows a shell bank to open an account with it.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Banks are required to implement procedures that allow them to verify a customer's identity for the purpose of non face-to-face transactions and/or relationships effectively conducted on a face-to-face basis.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	SARs are made to the Anti-Money Laundering Division, Investigation Bureau, Ministry of Justice at (http://www.mjib.gov.tw/mlpc/download-1.htm).
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 6,890 SARs (Source: Annual Working Report, Investigation Bureau of Ministry of Justice, September 2015) Comparative GDP data is not available for this specific period.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes. In addition to suspicious transactions, the following information must be reported: a) any currency transaction exceeding TWD500,000 (approx. USD15,000) (or the equivalent in foreign currency); and b) passengers or service crew on board who cross the border with the carrier and carry the following items shall make declarations to customs: a. cash of foreign currency with total amount exceeding a certain amount (approx. USD10,000); and b. securities with a face value exceeding a certain amount (approx. USD10,000). Customs shall report subsequently to the Investigation Bureau, Ministry of Justice.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	While in general only receipt or payment of cash or exchange of new bills that exceeds TWD500,000 (approx. USD15,000) must be reported, practical guidance further provides 20 specific circumstances under which transactions must be reported regardless of any amount threshold. In addition, regardless of any amount threshold or whether the transaction is completed, financial institutions have the obligation to report where there is suspicion of money laundering or financing of terrorism.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes: a) any financial institution which violates its reporting obligation for failure to report any currency transaction exceeding TWD500,000 (approx. USD15,000), as required by relevant laws and regulations, shall be punished by a fine between TWD200,000 (approx. USD6000) and TWD1 million (approx. USD30,000); b) any financial institution which violates its reporting obligation for failure to report any suspicious transaction as required by relevant laws and regulation, shall be punished by a fine between TWD200,000 (approx. USD6,000) and TWD1 million (approx. USD30,000). However, if the violating financial institution is able to prove that the cause of this violation is not attributable to the intentional or negligent act of its employee(s), no fine shall be imposed.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Although there are no requirements to obtain authority in order to proceed with a current/ongoing transaction that is identified as suspicious, practical guidance requires that in case of abnormal transactions, the person designated as the AML responsible person (must be vice President or equivalent level of personnel) must submit such transactions as the report of the financial institution to the Investigation Bureau.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Under Taiwan’s Personal Data Protection Act, in order for transactions to be monitored outside Taiwan’s jurisdiction, either the prior written consent of the data subject must be obtained, or such monitoring outside the jurisdiction must be specifically required by law or to advance public interests. As of Nov 2014, there is no express law or regulation in Taiwan that authorises or requires the monitoring of transactions outside Taiwan’s jurisdiction. However, since Taiwan is a member of the Egmont Group and the Asia/Pacific Group on Money Laundering, and has executed cooperative memorandum of understanding with a number of countries for information exchange purpose, Taiwan’s Investigation Bureau, after receiving reports from financial institutions, has the discretion to share such information and transactions outside Taiwan’s jurisdiction. Therefore, while there is not yet express law or regulation in Taiwan that allows the monitoring of transactions outside Taiwan, such information is monitored outside Taiwan in practice by operation of law.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.
Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of “personal data” cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of “sensitive data”? How is it defined and what are the additional protections?
A29.	The Personal Data Protection Act was amended on 26 May 2010 in Taiwan: a) yes, for example, name, birthdate, ID card number, passport number, contact information, criminal records, and financial condition; b) Taiwan’s Personal Data Protection Act only applies to personal data. However, corporate data may be covered by a financial institution’s duty of confidentiality such as under the Banking Act; c) although there is no specific definition of “sensitive data” under Taiwan’s Personal Data Protection Act, the Personal Data Protection Act categorises medical data, genetic data, sex life, health examination or criminal records as having heightened sensitivity, which may not be collected, processed, or used unless with one of the four conditions below: a. express written legal requirement; b. necessary for the performance of duties by data controller which has adopted appropriate safety maintenance measures; c. personal data having been published by data subject or by way of other legal manner; or d. necessary to statistics and academic research within the purpose of medical, health or criminal prevention by public authority or academic research institutions, which has been collected, processed or used by way of standardised procedure.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Criminal records and medical data shall not be used with the exceptions of the following: a) when in accordance with law; b) when it is necessary for the government agency to perform its duties or for the non-government agency to fulfil the legal obligation, and when there are proper security measures; c) when the individual has disclosed such information by himself, or when the information concerned has been publicised legally; and d) when the personal information is collected, processed or used under certain methods by a government agency or an academic research institution based on the purpose of medical treatment, personal hygiene or crime prevention statistics and/or study. For a government agency, credit reports shall be used in accordance with the scope of its job functions provided by laws and regulations, and in compliance with the specific purpose of collection. However, the information may be used outside the scope upon the occurrence of one of the following conditions: a) where in accordance with law; b) where it is for national security or to promote public interests; c) where it is to prevent harm on the life, body, freedom or property of the individual; d) where it is to prevent harm on the rights and interests of other people; e) where it is necessary for public interests on statistics or the purpose of academic research conducted by a government agency or an academic research institution, respectively. The information may not lead to the identification of a certain person after the treatment of the provider or the disclosure of the collector; f) where such use may benefit the individual; or g) a written consent of the individual has been obtained. For a non-government agency, credit reports shall be used in accordance with the scope of the specific purpose of collection provided. However, the information may be used outside the scope upon the occurrence of one of the following conditions: a) where in accordance with law; b) where it is to promote public interests; c) where it is to prevent harm on the life, body, freedom or property of the individual; d) where it is to prevent harm on the rights and interests of other people; e) where it is necessary for public interests on statistics or the purpose of academic research conducted by a government agency or an academic research institution, respectively. The information may not lead to the identification of a certain person after the treatment of the provider or the disclosure of the collector; or f) where a written consent of the individual has been obtained.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Article 48 of Taiwan's Banking Act requires that a bank keep confidential record of a customer's deposit, loan, or remittance information, unless with exceptions specified under the same article.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Thailand

Key contacts:

Vorapong Sutanont / Khwanhathai Lungcharoen

Email: vorapong.sutanont@th.pwc.com /

khwanhathai.lungcharoen@th.pwc.com

Tel: +66 2344 1429 / +66 2344 1293

Postal address: 15th Floor, Bangkok City Tower;

179/74-80 South Sathorn Road;

Bangkok 10120; Thailand

Last updated:

January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The AML Act was first enacted in 1999. It was subsequently amended in 2008, 2009 and more recently in 2013 to meet international standards e.g. setting requirements on conducting CDD, adding predicate offences.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.)? Please include link to the regulator(s) website
A3.	The Anti-Money Laundering Office ("AMLO"). Please refer to the following website: http://www.amlo.go.th/amlofarm/farm/en/index.php?lang=en
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, please refer to the following document links from the AMLO website: http://www.amlo.go.th/amlofarm/farm/en/files/MR_1(1).pdf and http://www.amlo.go.th/amlofarm/farm/en/files/MR_2(2).pdf
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes. There is a requirement to conduct CDD on existing customers where a relationship was established before the CDD regulation was stipulated and the relationship still exists (refer to item 26 of the revised Ministerial Regulation on CDD dated 11 Jul 2013). The AMLO issued more detailed guidelines on how to conduct CDD for existing clients (Refer to AMLO notification dated 11 Oct 2013 and effective from 9 Nov 2013).
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. It's a principle that the bank shall take into account risk factors from the client and the area/country, in order to assess the ML risk.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes. A full assessment was conducted in 2007. The subsequent report was issued on 24 Jul 2007 and is available online at the following links: http://www.amlo.go.th/amlofarm/farm/en/files/DAR_thai.pdf and http://www.apgml.org/documents/default.aspx?s=date&c=5&pcPage=5 In Apr 2013, FATF conducted an assessment by interviewing the authorities and some banks in order to assess improvement of AML Law in order to comply more with international standards after Thailand issued the Counter Terrorism Financing Act and amended the AML Act in Feb 2013.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes. There is a minimum threshold for temporary transactions (Refer to Section 18 of the Ministerial Regulation on CDD dated 11 Jul 2013): a) One-off transactions or many transactions with an aggregate amount below THB700,000 (approx. USD19,290); and/or b) Electronic payment transactions valued under THB50,000 (approx. USD1,380). This applies to financial institutions and designated non-financial businesses in Section 16(1) and 16(9) as mentioned in the AML Act.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Institutions should verify the original version of all identification documents; e.g. identity card, passport, household registration book, full name. Legal entities: Institutions should obtain company registration documents as well as examining the type of business, the sources of high value transactions or unusual characteristics or those that are not related to the business of customers. Institutions shall examine and verify the following identification information and evidence of the following persons associated with such juristic person or legal arrangement: (1) the person authorised to establish a business relationship; (2) the director authorised to conduct a transaction on behalf of the juristic person or legal arrangement; and (3) the ultimate beneficial owner of the juristic person or legal arrangement (per Ministerial Regulation Prescribing Rules and Procedures for Customer Due Diligence B.E. 2555 (2012) effective from 22 Aug 2012). The institution should maintain copies of verified identification documents for a period of five years.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Financial institutions and designated non-financial businesses and professions shall verify customer identification during the first transaction and periodically perform reviews until the account is closed or the relationship is terminated. The verification shall be completed with professional care, good faith and without gross negligence. Using an alias is not permitted. In general, where copies of identification documents are provided, such copies shall normally be verified as true and correct by the owner of the document and/or by verification against the original. Where foreign documents are provided, certification by a public notary and authentication by the embassy of the country that the document is originally issued may be required.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Identify and verify the real ultimate beneficial owners with reliable sources/methods.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Financial institutions and non-financial businesses in Section 16(1) and 16(9) can simplify CDD measures for low risk customers. Please see item 16 of Ministerial regulation on CDD dated 11 Jul 2013 at (http://www.amlo.go.th/amlofam/fam/web/files/MR%20CDD%202013.pdf). Article 16 subject to Article 14, financial institutions and persons engaging in professions under section 16 (1) and (9) may apply simplified CDD measures for low-risk customers. These measures may include, but are not limited to: a) reducing the requirements of identification information, taking into consideration types of customers, types of transactions or financial products, transaction size and movements of transactions or business relationships; b) reducing the requirements of examination and review of movements of transactions or business relationships; and c) reducing the requirements of verification of the customer's current information. Factors in considering customers as low-risk customers under paragraph one shall be set out in a Notification issued by the Secretary-General. Also, the AMLO notification regarding guidelines on factors and characteristics for low risk customers dated 11 Oct 2013 can be referred to (only available in Thai at this time).
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	This comes under item 14 of the revised Ministerial regulation on CDD dated 11 Jul 2013, which states that enhanced CDD must be conducted for high risk customers: http://www.amlo.go.th/amlofam/fam/web/files/MR%20CDD%202013.pdf Article 14 Financial institutions and persons engaging in professions under section 16 (1) and (9), while conducting money laundering and terrorist financing risk management in accordance with Articles 4 and 5, shall have regard to money laundering and terrorist financing risks. Customer risk factors include the following: a) Where information or results of identification of the customer or the beneficial owner indicate that the customer or the beneficial owner has one or more of the following attributes: a. having a shareholding structure which is unusual or more complex than the normal business conduct; b. matching the information of persons the Office notifies as subject to being designated as high-risk customers who deserve a close watch; c. engaging in a high-risk profession as prescribed by the Secretary General; d. being a politically exposed person; or e. being otherwise considered as posing a high money laundering or terrorist financing risk. b) Where it is found that the business relationship or the customer's transactions are conducted in unusual circumstances. Country or geographic risk factors exist where a customer resides either temporarily or permanently; engages in an occupation; has an income source from - or conducts transactions in - a geographical area or country which has been notified by the Secretary General as an area or country with a high risk of money laundering and terrorist financing.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Client or ultimate beneficial owner is PEP.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Request policy and guidelines on AML/CFT, as well as consider credibility of correspondent banks, prior to creating a relationship. Please see details in items 42-46 of Ministerial regulation on CDD dated 11 Jul 2013 at (http://www.amlo.go.th/amlofarm/farm/web/files/MR%20CDD%202013.pdf). Article 42: Financial institutions shall refuse to enter into a correspondent banking relationship or to conduct a transaction and shall end a business relationship with respondent financial institutions with any one of the following attributes: a) established with authorisation but without real management located within the authorising country or with real management located within the authorising country but conducting no business within that country and not in a position to be supervised; and/or b) having entered into a correspondent banking relationship with, or providing financial services for, or holding an account with a financial institution under b). Article 43: Where a financial institution enters into a business relationship with a respondent financial institution, whether such relationship is established for securities transactions or electronic fund transfers, whether for a cross-border financial institution as principal or for its customer, the financial institution shall identify and obtain information of that respondent financial institution in accordance with Article 19 (1), (2) and (3) and shall verify the trustworthiness of the respondent financial institution as well as considering the reliability of the agencies responsible for its anti-money laundering and counter financing of terrorism supervision. Article 44: When establishing a business relationship with a respondent financial institution with respect to 'payable-through accounts', a financial institution shall conduct risk management and CDD on the customers having direct access to accounts of the correspondent financial institution, and it shall be able to provide relevant risk management and CDD information upon request to the correspondent financial institution. Article 45: Where a respondent financial institution is located in an area or country with money laundering and terrorist financing risk, a financial institution shall obtain information regarding its anti-money laundering and countering the financing of terrorism policy and action guidelines and shall verify the trustworthiness of such respondent financial institution. A financial institution shall consider refusing to enter into a business relationship, or to conduct a transaction and ending the business relationship if a respondent financial institution does not have in place effective anti-money laundering and countering the financing of terrorism policy or measures, or if that respondent financial institution or its ultimate beneficial owner(s) are involved in money laundering or terrorist financing. Article 46: Where a financial institution has a business relationship with a respondent financial institution located in an area or country with money laundering and terrorist financing risk, the financial institution shall take caution in conducting the business relationship and shall regularly verify information on the respondent financial institution and shall consider immediately ending the business relationship if it finds that the respondent financial institution is involved with money laundering or terrorist financing.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes. Please see details in item 42 of the Ministerial regulation on CDD dated 11 Jul 2013 at (http://www.amlo.go.th/amlofarm/farm/web/files/MR%20CDD%202013.pdf). Article 42: Financial institutions shall refuse to enter into a correspondent banking relationship or to conduct a transaction and shall end a business relationship with respondent financial institutions with any one of the following attributes: a) established with authorisation but without real management located within the authorising country or with real management located within the authorising country but conducting no business within that country and not in a position to be supervised; or b) having entered into a correspondent banking relationship with, or providing financial services for, or holding an account with a financial institution under a).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Institutions should establish risk mitigating procedures and measures for account openings for non face-to-face customers and should have effective monitoring procedures as stringent as those for customers who are physically present. Please see details in item 47 of the Ministerial regulation on CDD dated 11 Jul 2013: http://www.amlo.go.th/amlofarm/farm/web/files/MR%20CDD%202013.pdf Article 47 Financial institutions and persons engaging in professions under section 16 (1) and (9) may rely on third parties in verifying the customer identification in accordance with Article 19 (1), (2), (3) and (4), Article 20 and Article 22 or to introduce business provided that the following criteria are met: a) it obtains the necessary information relating to the requirements under Article 19 (1), (2), (3) and (4), Article 20 and Article 22 from the third party; b) copies of documents or identification information and other relevant documentation and information of customers relating to the requirements under Article 19 (1), (2), (3) and (4), Article 20 and Article 22 shall be made available from the third party upon request without delay; c) the third party is under proper supervision and monitoring, and has measures in place for compliance with CDD and record keeping requirements in accordance with the rules and procedures set out in this Ministerial Regulation; and d) in the case of a third party being subject to rules of many countries, consideration is given to the reliability of those countries based on their level of money laundering and terrorist financing risk. In the case where a third party is a financial institution, and persons are engaging in professions under section 16 (1) and (9) that is part of the same financial group and financial institution and persons engaging in professions under section 16 (1) and (9) apply CDD measures and record-keeping requirements, and act in line with Article 49, Article 50 and Article 51, and where the effective implementation of those requirements is supervised by a competent authority, it shall be deemed that the financial institution and persons engaging in professions under section 16 (1) and (9) apply measures under (3) and (4) above through its group programme. The above provisions do not apply to an outsourcing or agency relationship. Reliance on third parties means reliance (on the third party) for performing the requirements under paragraph one and record-keeping requirements under the supervision and monitoring of the competent authority within the Ministerial Regulation. The third party may have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform the CDD measures. This reliance on a third party is contrasted with an outsourcing/agency relationship, in which the outsourced entity applies the CDD measures on behalf of the delegating financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control. Financial institutions and persons engaging in professions under section 16 (1) and (9) shall be held responsible where a third party fails to apply CDD procedures or recordkeeping requirements, or fails to fully comply with these procedures. A third party shall be a financial institution or person engaging in professions under section 16 (1) and (9) under the supervision of the competent authority.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	AMLO: http://www.amlo.go.th/amlofarm/farm/en/index.php?lang=en

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 13,963 SARs GDP (in current prices): 2014 – USD404,824m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD29m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes. The financial institution has a duty to report the transaction to the Office when it appears that such a transaction is: a) a transaction funded by an amount of cash equal or more than THB2 m (approx. USD55,120). Except in the case of an electronic fund transfer transaction, the financial institution shall have the duty to report if the transaction is equal or more than THB100,000 (approx. USD2,760); b) a transaction connected with the property worth equal or more than THB5 m (approx. USD137,860). Except in the case of movable property involving electronic fund transfer or payments, the financial institution shall have the duty to report if the transaction is equal or more than THB700,000 (approx. USD19,290); or c) a suspicious transaction; whether or not it is a transaction under a) or b). The following designated non-financial businesses and professions shall have the duty to report the transaction to the Office when it appears that such transaction is funded by an amount of cash equal to or more than THB2 m (approx. USD55,120): a) trader that is not a financial institution, engaging in the business involving the operation of or the consultancy or the provision of advisory services in a transaction relating to the investment or mobilisation of capital under the law on securities and stock exchange; b) trader dealing in the business of gems, diamonds, coloured stones, gold, or ornaments decorated with gems, diamonds, coloured stones, gold; c) trader dealing in the business of selling or leasing of cars; d) trader dealing in the business of immovable property broker or agent; e) trader dealing in the business of antiques traded under the law on Control of Sale by Auction and Antique Trade; or f) trader dealing in the business of credit cards that is not a financial institution under the Notification of the Ministry of Finance determining on credit cards or the law on financial institution business. The following designated non-financial businesses shall have a duty to report a transaction to the Office when it appears that such transaction is funded by an amount of cash equal or more than THB500,000 (approx. USD13,790): a) trader dealing in the business of personal loan under supervision for businesses that is not a financial institution under the Notification of the Ministry of Finance determining on Personal Loan Businesses under Supervision or under the law on financial institution business. The following designated non-financial businesses shall have the duty to report a transaction to the Office when it appears that such transaction is funded by an amount of cash equal or more than THB100,000 (approx. USD2,750): a) trader dealing in the business of electronic money cards that is not a financial institution under the Notification of the Ministry of Finance determining on electronic money cards or the law on financial institution business; or b) trader dealing in the business of electronic payment service under the law on the supervision of electronic payment service business.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Yes, see A20 above.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, any person who violates or does not comply with the AMLO regarding reporting and client identification shall be liable to a fine up to the amount of THB500,000 (approx. USD14,000); additionally, persons could incur a daily fine not exceeding THB5,000 (approx. USD140) through the period of violation, or until acting in accordance. Any person who reports or makes a notification by presenting false statements of fact or concealing the facts required to be revealed to the competent official shall be liable to imprisonment for a term not exceeding two years or to a fine of THB50,000 to THB500,000 (approx. USD1,380 to USD13,780) or to both.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes, subject to approval from the Bank of Thailand as lead regulator under outsourcing notifications (for commercial banks under BOT supervision).

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of “personal data” cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of “sensitive data”? How is it defined and what are the additional protections?
A29.	No specific Data Protection Law. For banks under supervision of the Bank of Thailand, Section 154 of the Financial Institutions Business Act prohibits the disclosure of customer information from financial institutions except under some specific circumstances.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes. Please see A29. For credit information that is obtained from the National Credit Bureau (“NCB”), database, financial institutions that are a member of the NCB can only use such credit information for the purpose of credit analysis and reviewing of credit, according to the Credit Information Protection Act. Hence, the transfer of such credit information is prohibited for other impermissible purposes.

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Please see A29 and A30.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Other than normal clauses in the AML Act, please see obligations as mentioned in A29 and A30.



'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Vietnam

Key contact: Annett Perschmann-Taubert
Email: annett.ingrid.perschmann@vn.pwc.com
Tel: +84 (8) 3823 0796 ext. 1519

Postal address: 4th Floor, Saigon Tower,
29 Le Duan Street
District 1, Ho Chi Minh City, Vietnam

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Criminal Law issued in 1999 (effective on 01 Jul 2000). Law No. 37/2009/QH12 amending and supplementing some articles of the Criminal Law issued in 1999 issued in 2009 (effective on 01 Jan 2010). Law on Credit Institutions issued in 2010 (effective on 01 Jan 2011). Law on anti-money laundering No. 07/2012/QH13 issued in 2012 (effective on 01 Jan 2013). Decree 116/2013/ND/CP issued on 04 Oct 2013. Circular 35/2013/TT-NHNN issued on 31 Dec 2013.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A. It is the first time regulations on anti-money laundering have been issued in the form of a law.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.)? Please include link to the regulator(s) website
A3.	Anti-Money Laundering Information Centre under the State Bank of Vietnam ("SBV"): http://www.sbv.gov.vn
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The new Decree 116/2013 and Circular 35/2013 provide some guidance regarding AML requirements (such as e.g. on customer identification, reporting). Homepage of SBV: http://www.sbv.gov.vn
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No. The Law on anti-money laundering however requests clients' information must be updated regularly.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The assessment body 'Asia Pacific Group on Money Laundering ("APG")' performed an assessment in 2009: http://www.apgml.org/documents/default.aspx?DocumentCategoryID=17

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Financial institutions must verify clients' information in certain circumstances such as: when clients open accounts, make transactions of high value, make suspicious transactions or if there is any doubt regarding the client's identification information. Certain non-financial institutions are required to identify customers: a) casino/gaming businesses; b) real estate management or property services companies, if brokerage services in relation to purchase, sale and management of properties is provided; c) organisations trading in precious metals and gemstones if they carry out transactions in relation to purchase/sale of precious metals/gemstones with large value of cash; d) notaries, accounting and legal services companies, if they carry out certain transactions, e.g. if they act on their customers behalf to make transactions, such as transfer of land use rights, or management of customer's bank accounts; and e) organisations providing trust services if they carry out certain transactions, such as providing services such as establishment of companies.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Article 9 of the Law on anti-money laundering stipulates that the clients' information must include: a) for individual Vietnamese clients: full name, date of birth, nationality, occupation, position; phone number, identity card number or passport number, date and place of issue and permanent/current address; b) for individual foreign clients: full name, date of birth, nationality, occupation, position; passport number, date and place of issue, visa, overseas/Vietnam address; for corporate clients: full and abbreviated trading name, address of head office, phone number, fax number, areas of operations and business, information on the founder and representatives; and c) information regarding beneficiary. In case of corporate beneficiary: information regarding ownership and control rights.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Article 11 of the Law on anti-money laundering allows engagement of other organisations to conduct the verification.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Under Article 9.2 of the Law on anti-money laundering, it is required to verify the beneficial ownership and apply necessary measures in order to know and update information of beneficial ownership. For corporate clients, it is required to collect information on ownership and control structure to determine the individual with the controlling interest and who has the control of the corporate.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	None stated in local regulations or guidance.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	None stated in local regulations or guidance. Cir.35/2013, article 3 states the conditions on "intensive evaluation" (i.e enhanced due diligence) applicable to high risk customers.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Article 13 of the Law on anti-money laundering requests financial/specified non-financial institutions to have internal systems to control account opening/transactions with foreign PEPs (including their related persons) and to take measures to identify sources of clients' assets and to enhance monitoring business relationship/transactions with clients. Article 4 of Cir.35/2013 mentioned the list of foreign Politically Exposed Persons as posted on the SBV's website (http://www.sbv.gov.vn), and the reporting entities must register with the SBV's inspection body, with the access to and exploitation of the list of foreign individuals being in compliance with their guidance.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Article 14 of the Law on anti-money laundering requests the following measures upon establishment of agent bank relationships: a) collecting information about the banking partner to identify the nature of business, the partner bank's reputation and ensure the partner bank is subject to supervision and management of the foreign competent management agencies; b) assessing the implementation of measures on prevention of money laundering at the partner bank; c) must be approved by the General Director (Director) or authorised persons before setting up the agent bank relationship; and d) in case the partner bank's clients can make payment through the partner bank's accounts opened at the institution, the institution must ensure the partner bank has fully implemented the identification process, updated the client information and that they are able to provide client identification information as required by the institutions.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Not stated in local regulations.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Not specifically mentioned in the regulations. However the Law on anti-money laundering refers in Article 17 to business through "introduction" by a third party.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting	
Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	SBV: http://www.sbv.gov.vn/portal/faces/vi/vim/vipages_trangchu
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Under the Law on anti-money laundering, in addition to suspicious transactions, the following transactions should be reported: a) high value transactions (level of value to be stipulated by the Prime Minister); b) electronic money transfer with value exceeding the threshold stated by the SBV; and c) individuals bringing in currency/gemstones/valuable papers exceeding the threshold stated by the SBV. Based on the Prime Minister's Decision 20/2013/QĐ-TTg dated 18 Apr 2013, the value of high value transactions subject to reporting is VND300m (approx. USD14,000). Decree 116/2013, article 3 stipulates that irregular transactions with great value means transactions with the total value of VND 300m or more in a day, conducted by customers who have no account, or who have a settlement account but do not carry out transactions within six months or more.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Yes, values below the stipulated values as set out in A20.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, there are penalties for administrative violations.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No. The Law on anti-money laundering however requires the reporting entity to exercise special supervision of certain transactions, such as transactions with high value or transactions with individuals in countries or territories included in the list published by FATF.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No. The Law on anti-money laundering requests the related institutions to delay the suspicious transaction and report immediately to the authorities.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No legal requirements. However, within the auditors' responsibility, the auditors may report any material AML issues in the management letter which is mandatory reported to the SBV by the bank.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Vietnam has regulations on "personal data protection", but not "corporate data protection". There is no clear definition of "personal data" as well as no definition of "sensitive data".

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	The Civil Code provides that the use of a personal image and information/data of a person by an organisation(s)/other individual(s) must be agreed by such person in advance. An organisation that unlawfully discloses such image/information as referred above may be taken to court and may be required to pay compensation to the complainant. However, there are no criminal sanctions in this case.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Argentina

Key contact: Karin Reise
Email: karin.reise@ar.pwc.com
Tel: +54 11 4850 6818

Postal address: Bouchard 557 - P.7; C1106ABG,
Ciudad de Buenos Aires,
Argentina

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1996.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	Unidad de Información Financiera ("UIF") for a), b) and c) (www.uif.gov.ar). Also for banking, the Banco Central de la Republica Argentina ("BCRA") have additional requirements: www.bcra.gov.ar
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The UIF provides information and guidance: www.uif.gov.ar and http://www.uif.gov.ar/uif/index.php/es/sobre-el-lavado-de-activos
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, although local regulators require certain procedures to be performed without taking into account the risk profile of the transaction or customer.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes: http://www.fatf-gafi.org/topics/mutualevaluations/documents/mutualevaluationofargentina.html

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: The law established two types of customers: 'permanent' and 'not frequent'. For each type of customer specific documentation is required, which varies from a simple identification to a tax declaration. Names are verified against original documents for both individuals and entities. 'Not frequent' customers who are individuals need to provide full name, birth place and date, citizenship, etc. Entities must provide: name, identification number, tax identification number, Constitution Act and date, etc. Legal officers and shareholders must provide the same information. In addition, 'Permanent' customers need to provide: information on sources of income and financial information of accounts/investments in other financial entities. All information must be supported by proper documentation.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	There is no information on independent verification of documentation in local guidance. Original documents must be seen by financial institutions.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Beneficial Owners are treated the same as 'permanent' clients, therefore beneficial ownership must be identified.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Firms are not allowed to avoid the identification requirements in connection with the KYC regulations. For 'not frequent' customers, a reduced level of due diligence is allowed.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence procedures are required for transactions over USD10,000 and some additional information is required for 'permanent' customers (see A9).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	The banking regulation has a specific paragraph on PEPs, requiring special attention to be taken in such cases. For all individuals considered to be PEPs, the KYC regulations apply, including enhanced due diligence in accordance with the client's profile.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	None stated in local regulations or guidance.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	No.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Based on regulations issued by the Unidad Information Financiera, additional due diligence for non face-to-face transactions and/or relationships is required. Clients must provide information verified by other entities (for example credit card companies and other banks).

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	UIF: http://www.uif.gov.ar/uif/index.php/es/
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 – 36,079 (Source: http://www.uif.gov.ar/uif/index.php/es/estadis) GDP (in current prices): 2013 – USD614,383.5m (Source: data.worldbank.org) This results in a ratio of 1 SAR for every USD17m of GDP.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, in certain circumstances dependent on the industry, there are monthly reports of normal transactions.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	ARS50,000 (approx. USD3,560).

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	It is suggested in the regulations but not mandatory.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes, an external auditor must audit the AML process and make a report in a quarterly basis for the BCRA regulator. The report is for the bank and for internal use. It is not a public report.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) quarterly basis; b) bank internal use as part of the statement audit; and c) yes.
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) no; b) no; and c) no.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	The personal data protection law is Law 25.536 a) no; b) it is a comprehensive protection of personal information recorded in files, records, databases, databanks or other technical means of data treatment, either public or private for purposes of providing reports, in order to guarantee the right of individuals to their honour and privacy; and c) no, this law includes personal data, sensitive data, Datafile, register, database or databank.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes, Law 25326.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes, Financial Institution Law 21.526 includes bank secrecy obligations.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Bolivia

Key contact: Boris Mercado
Email: boris.mercado@bo.pwc.com
Tel: +591 2-240 8181

Postal address: Ed. Ana María, Pisos 1, 2, 3
Pinilla, Esq. Campos,
La Paz, Bolivia

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1997.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	For the Financial Sector, the Autoridad de Supervision del Sistema Financiero ("ASFI") is responsible for analysing suspicious financial activities: https://www.asfi.gob.bo/
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, ASFI provides guidance for external auditors to perform AML reviews.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	No, every financial institution is an independent organisation. The methodology used to determine whether a risk based approach is used or not is their responsibility.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes. All transactions below USD5,000 do not require customer due diligence. Transactions above this limit must provide information regarding the fund source and other information based on the UIF policy (Unidad de Investigaciones Financieras ("UIF") – Financial Investigation Unit).
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Law and its procedures define minimum requirements to identify customers: Individuals: birth date, nationality, National Identification number (carné de identidad) or passport number, Número de Identificación Tributaria ("NIT") (if applicable, which is the Taxpayers Identification Number), marital status and spouse name (if applicable), home and business address, telephone number, profession, occupation and commercial references. Legal entities: entity name, activity, NIT, business address, telephone number, shareholders list, executives list, commercial references and entity constitution documents.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	According to law, financial institutions should always verify original identification documents at any transaction. However, for legal entities, there are some documents that can be provided as copies, if those copies are certified by a notary public office.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The following situations require financial institutions to collect additional information about beneficial ownership: a) when the client informs the institution that the final beneficiary is another person or entity; b) when the financial institution has doubts about the final beneficiary; c) when the customer engages in commercial, financial or industrial transactions in a location where they have no operations; d) when transactions are greater than USD 5,000 or its equivalent in local currency in current accounts, saving accounts, long term deposits, money exchange, among others; or e) when the total of multiple linked transactions is an amount greater than USD5,000, or its equivalent in local currency.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence arrangements are available for transactions below the USD5,000 threshold.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence arrangements are required for transactions above the USD5,000 threshold.

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	None stated in local regulations or guidance.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	None stated in local regulations or guidance.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	No.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	None stated in local regulations or guidance.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Banks and financial institutions prepare periodic reports for the UIF at: www.uif.gob.bo

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: January to June 2015 – 884 SARs (Source: www.uif.gob.bo) Comparative GDP data is not available for this specific period.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, all transactions above USD5,000 and also formal requirements made by regulators or government entities or legal processes.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Yes, below USD5,000.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	The regulator establishes the appropriate penalties to be charged according to the degree of non-compliance.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	ASFI requires external auditors to assess the automated Suspicious Transaction monitoring technology.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	The regulator establishes the appropriate procedure for suspicious activities.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	For any transaction (remittances, drafts, etc.) above USD5,000 the form PCC01 will need to be completed that details origin, reason and destination for the transaction. In addition, financial institutions must adhere to the requirements of correspondent banks in cross-border relationships. However, regulation is silent on whether transactions can be monitored outside the country.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	This type of information is usually included in the external auditor's review.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	It is not required to have an external report on the bank's AML systems. ASFI may request to analyse as part of the Environmental Control Assessment some specific aspects relating to AML systems and controls as part of the external audit review.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	It requires sample testing, controls identification and walkthroughs.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	The country has established data protection laws.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Information cannot be transferred unless it is authorised by a competent body.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Case law must be treated with sensitivity and confidentiality and properly authorised by a competent body.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	There are bank secrecy and law obligations for information confidentiality.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Brazil

Key contacts: Alfredo Sneyers / Marcus Manduca /
Harry Holdstock
Email: alfredo.sneyers@br.pwc.com /
marcus.manduca@br.pwc.com / harry.holdstock@br.pwc.com
Tel: +55 (0) 11 3674 3686

Postal address: Centro Empresarial Agua Branca,
São Paulo,
Brazil

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Law 12,683 amended in Jul 2012. The previous law was issued in 1998 and updated in 2002 (Law 9.613).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The 2012 law is more wide-ranging with regards to the types of illicit activity that fall under the law (now "any harmful act") and the types of business that are now subject to it (now includes notaries, real estate firms, sports agents, consultants, factoring companies etc.). Furthermore, the maximum value of fines that can be levied under the law has increased from BRL200,000 (approx. USD50,000) to BRL20m (approx. USD5m). The other significant change is the law concerns the reporting of suspicious activities and transactions to regulators – the new law now specifies that such reporting must be to the Conselho de Controle de Atividades Financeiras ("COAF") and that the submission of such reports must not be discussed with anyone (not just the entity referred to in the report).
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	The principal regulator is the Conselho de Controle de Atividades Financeiras ("COAF"): (https://www.coaf.fazenda.gov.br/) However, many other regulators also issue regulations/guidance for relevant sectors, including the: a) Banco Central do Brasil ("BCB") (http://www.bcb.gov.br/); b) Comissão de Valores Mobiliários [Securities regulator] ("CVM") (www.cvm.gov.br); c) Conselho Federal de Contabilidade [Accountancy profession regulator] ("CFC") (www.cfc.org.br); d) Ministério da Previdência Social [Pension regulator] ("PREVIC") (www.previdencia.gov.br/previc/); e) Superintendência de Seguros Privados [Insurance regulator] ("SUSEP") (www.susep.gov.br/); and f) Conselho Federal de Corretores Imobiliários [Real Estate Agencies regulator] ("COFECI") (www.cofeci.gov.br/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes. Practical guidance can be found at: (https://www.coaf.fazenda.gov.br/)

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	All entities subject to the law are required to identify their clients (and ultimate beneficial owners) and keep each client's KYC profile up-to-date. Whilst the law does not directly require retrospective review/remediation of clients, it does expect firms to be able to identify their clients.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Whilst the law does not specifically permit a risk-based approach, it does state that KYC/AML policies established by firms should be compatible (i.e. proportional) to the nature and scale of the firm's operations.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The FATF published an executive summary of the mutual evaluation report which summarises the AML/CFT measures in place in the Federative Republic of Brazil (hereinafter "Brazil") as at the time of the on-site visit (26 Oct 2009 to 7 Nov 2009), and shortly thereafter: http://www.fatf-gafi.org/topics/mutualevaluations/documents/mutualevaluationreportofbrazil.html On 12 Mar 2012, the Central Bank amended the rules applicable to procedures that must be adopted by financial institutions in the prevention and combat of money laundering and terrorism financing, as a response to the recommendations of FATF. The main measures include: a) enactment of Circular No. 3,583, which sets forth that: a. financial institutions shall not initiate any relationship with clients, or proceed with existing relationships, if it is not possible to fully identify such clients; and b. anti-money laundering procedures are also applicable to agencies and subsidiaries of Brazilian financial institutions located abroad. b) enactment of Circular No. 3,584, establishing that the institutions authorised to operate in the Brazilian foreign exchange market with financial institutions located abroad must verify if the other party is physically present in the country where it was organised and licensed or is object of effective supervision; and c) enactment of Letter 17 Circular No. 3,542 ("Letter Circular No. 3,542"), which increases the list of examples of transactions and situations which may characterise evidence of occurrence of money laundering, tending to improve the communication between financial institutions and the COAF.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No. The thresholds highlighted in the law relate to the reporting of suspicious activities or transactions to COAF. These include: a) actual or proposed issuance or recharge of one or more store value cards totaling BRL100,000 (approx. USD24,790) in a given calendar month; b) actual or proposed cash transactions exceeding BRL100,000 (approx. USD24,790); c) suspected transactions above BRL10,000 (approx. USD2,480) (i.e. those involving suspicious parties or values, or without economic reasons, etc.); d) transactions apparently intended to sidestep identification mechanisms or controls; and e) actions suspected of financing terrorist activity.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The law requires the following to be gathered for the purposes of identification and verification of clients: Individuals: Full name, nationality, date and place of birth, address, official ID document (type, number, date of emission and emitting institution), number of inscription on the Cadastro de Pessoa Física (“CPF”) etc. Full name is to be verified against a local identification document. Corporations: Full name, type and date of constitution, address, documents containing the same information required for individuals who qualify and authorise the representatives to use the account, number of inscription on the Cadastro Nacional de Pessoa Jurídica (“CNPJ”) etc. Names of legal entities are verified against the Register of Certification (there are also other detailed requirements).
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Original documentation is required to be presented as part of the identification and verification process. The law is silent on when firms can or cannot accept independently verified or authenticated copies of original documentation.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The law states that, where the client is legal entity (as opposed to a private individual), it is necessary to identify the beneficial owners and other individuals or entities that are authorised to represent that entity. The same identification and verification requirements, as set out in response to Q9, apply to all such individuals/entities.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	N/A – The law does not permit reduced/simplified due diligence in any circumstances.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	N/A – The law does not require enhanced due diligence in any circumstances.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	N/A – Firms are required to identify and verify identity of all clients, representatives and beneficial owners. Where there is a PEP relationship, firms are required to record that relationship as a PEP relationship, but the law does not require specific additional due diligence on top of that.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The main measures include: a) enactment of Circular No. 3,583, which sets forth that: a. financial institutions shall not initiate any relationship with clients, or proceed with existing relationships, if it is not possible to fully identify such clients; and b. anti-money laundering procedures are also applicable to agencies and subsidiaries of Brazilian financial institutions located abroad. b) enactment of Circular No. 3,584, establishing that the institutions authorised to operate in the Brazilian foreign exchange market with financial institutions located abroad must verify if the other party is physically present in the country where it was organised and licensed or is the object of effective supervision; and c) enactment of Letter 17 Circular No. 3,542 ("Letter Circular No. 3,542"), which increases the list of examples of transactions and situations which may characterise evidence of occurrence of money laundering, intending to improve the communication between financial institutions and the COAF.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	No. Although they are not prohibited, they are closely monitored.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	None stated in local regulations or guidance.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Conselho de Controle de Atividades Financeiras ("COAF"): www.coaf.fazenda.gov.br

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 - 1,129,421 SARs GDP (in current prices): 2014 - USD2,346,076.3m (Source: data.worldbank.org) This results in a ratio of 1 SAR for every USD2.1m of GDP.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes. All of the following must be reported: a) actual or proposed issuance or recharge of one or more store value cards totaling BRL100,000 (approx. USD24,890) in a given calendar month; b) actual or proposed cash transactions exceeding BRL100,000 (approx. USD24,890); c) suspected transactions above BRL10,000 (approx. USD2,490) (i.e. those involving suspicious parties or values, or without economic reasons, etc.); d) transactions apparently intended to sidestep identification mechanisms or controls; and e) actions suspected of financing terrorist activity.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Yes, for activities below BRL5,000 (approx. USD1,240).
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes. The law provides for the following sanction/fines for non-compliance (including non-compliance with reporting requirements): a) warning; b) fine (up to BRL20m (approx. USD5m); and/or c) suspension/ban (private individuals and legal entities).
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes, in some cases the COAF requests the Bank does not terminate the account or relationship with the client so that the COAF can best investigate the transactions of a particular customer. In this case all monitoring between the COAF and the Bank is documented.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	The bank secrecy law prevents a client's activities from being monitored or reported outside the country.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No. However, there is a legal requirement (Resolution CFC 1445/13) which requires external auditors to communicate to COAF if they suspect issues at their clients. The main objective of the Resolution is to protect the activities of external auditors.
Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	There is not yet a specific statutory regulation governing data transfers in Brazil, nor is there yet a specific data protection authority. Nevertheless, several laws, as well as the Brazilian Constitution provide Brazilians with some rights with regard to data collection. There are also laws governing protection in specific areas (e.g. bank secrecy, medical ethics, consumer protection, credit, and telecommunications). Article 5 of the Brazilian Constitution provides that the "privacy, private life, honor and image of persons are inviolable, and the right to compensation for property or moral damages is ensured." Article 5 also grants habeas data. It guarantees the right of privacy and ensures consumers have the right to know what data are held about them and they have the right to correct that data. However, these rights of knowledge and correction under the Constitution currently exist only with respect to records or databases of government agencies or agencies of a public character. The Consumer Protection Law of 1990 regulates consumer databases held by banks, credit agencies, and other companies. "Consumer" is defined broadly under the Law as "any individual or body corporate who acquires or uses any product or service as an end user." The law requires that any consumer data stored in a database should be truthful, objective, and easily understood, and prohibits containing the same piece of the storage of any negative information about a consumer for more than five years. If the consumer did not request that his or her information be stored, the collector must notify the consumer in writing of the inclusion of his or her name in a database. Additionally, consumers are given the right to correct information about themselves. Article 43 of the Consumer Protection Law grants consumers free access of any of their own information stored in a database. It also gives consumers the right to request the prompt correction of an inaccuracy in his information and requires that the requested correction must be made within five days. The Constitution and the Civil Code apply to all individuals and legal entities. The Consumer Protection Code applies to relationships between consumers and service/product providers, including those performed on the internet.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	The Credit Information Law ("CIL") of 2011 imposes several requirements on the creation and access to databases related to credit information. The law forbids the processing of data that is unnecessary in deciding whether to grant credit. This prohibition specifically applies to sensitive data such as political, religious, sexual, and health information. Data subjects have the right to access, rectify, and erase data and be informed of the database manager's identity and the identity of third parties that will have access to the data. Lastly, the law imposes data quality obligations on the data processors. The CIL regulates "the creation and the access to databases related to credit information of citizens and companies". We highlight that this legal instrument enacts principles and rules related to data quality as objectivity, clearness, truthfulness and comprehensibility of data. It forbids the processing of excessive information (data not necessary to credit granting or other banking services) and sensitive information (understood as related to social and ethnic origins, health, genetics, sexuality, and political, religious and philosophical convictions) (Article 3°). It covers the purpose principle and rights to the data subjects, so the right to access, the right of rectification and erasure of data, the right to know the criteria used by the banks in order to evaluate the credit's risk, the right to be informed previously about the existence of the data storage, the data base manager's identity and about the identity of the third parties that will have access to data, finally the right to be informed about the purpose of the processing and to have a second analysis of a decision based on automatic means (Articles 5° and 7°). Database managers are obliged to inform citizens about all the stored or obtained personal information as well as about the sources through which this information was obtained, to provide information about third parties that have access to personal data and to provide information about citizens' rights (Article 6°). Last point, CIL also imposes data quality obligations to processors (Article 8°). Medical data may be protected by patient-doctor confidentiality, as well as by individual privacy and personal rights set out in the Constitution. Employment law regulates the use of information collected in background checks (concerning criminal convictions, political beliefs, sexual preferences, and so on). The use of this information may be illegal if used for discriminatory purposes.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	There are no restrictions on the international transfer of data, provided the subject consented to the initial gathering and processing. It is advisable, when consent is obtained, for the data subject to be informed that data could eventually be transferred.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. Any personal data submitted by or obtained from a data subject may be regulated under the general provisions of the Constitution, Civil Code and Consumer Protection Code (see A29), including: name, personal address, identification number, income, bank account, credit card number and any personal communication exchanged without any intent to go public (such as personal e-mails, internet logs and messaging).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Canada

Key contact: Marie-Chantal Dréau / Sarah MacGregor
Email: marie-chantal.dreau@ca.pwc.com /
sarah.e.macgregor@ca.pwc.com
Tel: +1 514 205-5407 / +1 416 814-5763

Postal address: 1250 René Lévesque West Suite 2800,
Montréal, Québec, H3B 2G4, Canada /
18 York Street, Suite 2600, Toronto, Ontario, M5J 0B2,
Canada

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PCMLTFA") was passed in 2000, and amended in 2001, 2006, 2008, 2010, 2013 and 2014.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	In 2000, the Financial Transactions Reports Analysis Centre of Canada ("FINTRAC") was established under the PCMLTFA to serve as Canada's financial intelligence unit. FINTRAC is responsible for ensuring compliance with AML/AFT requirements by all Reporting Entities, including financial entities (banks, trust companies, credit unions, etc.), life insurance companies, securities dealers (including asset managers/investment advisers), casinos, money services businesses, dealers in precious metals and stones, real estate agents and certain developers, accountants and notaries public based in the province of British Columbia (http://www.fintrac.gc.ca/). The Office of the Superintendent of Financial Institutions ("OSFI"), established in 1987, is the federal agency responsible for the supervision and regulation of all federally incorporated or registered banks, life insurance companies, property and casualty insurance companies, and federally regulated private pension plans (http://www.osfi-bsif.gc.ca/). The Canadian Securities Administrators ("CSA") is an umbrella organisation comprised of 13 provincial and territorial securities regulatory authorities. The CSA serves as a forum for coordinating and harmonising the regulation of Canadian capital markets. Securities regulators also delegate certain aspects of securities regulation to self-regulatory organisations including the Investment Industry Regulatory Organisation of Canada ("IIROC") (http://www.iiroc.ca/Pages/default.aspx). FINTRAC and OSFI report to the federal Minister of Finance. FINTRAC has in place Memoranda of Understandings ("MOUs") with both OSFI and IIROC, but does not delegate its supervisory role through MOUs to other regulators. Information obtained by other regulators through their own supervisory activities, including examinations, is provided to FINTRAC under the MOU and is taken into consideration by FINTRAC during its risk assessment process. In addition to the audits and examinations performed by the regulators under their own supervisory framework, the results of which, with respect to AML/CFT relevant issues are provided to FINTRAC, FINTRAC conducts examinations in each sector, whether or not it is covered by an MOU. In fact, FINTRAC has conducted examinations in every sector covered by the PCMLTFA with the exception of financial institutions supervised by OSFI. In 2013, OSFI and FINTRAC implemented a concurrent examination methodology where OSFI will focus on risk management processes and controls needed to ensure compliance and FINTRAC will focus on the quality, volume and timing of reports submitted by federally incorporated or registered financial institutions.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	FINTRAC has published plain language interpretations and guidelines as well as interpretation notices: http://www.fintrac.gc.ca/publications/pub-eng.asp and http://www.fintrac.gc.ca/publications/guide/guide-eng.asp OSFI Guideline B-8: Deterring and Detecting Money Laundering was issued in December 2008: http://www.osfi-bsif.gc.ca/Eng/Docs/b8.pdf IIROC issued Anti-Money Laundering Compliance Guidance in October 2010: http://www.iiroc.ca/documents/2010/6279890d-ecd8-4244-a8e3-8f8a23e80e4a_en.pdf
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No, however pursuant to the adoption of a Risk Based Approach to ML/TF governance, customers considered to be a higher ML/TF risk are required to be identified.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. Entities are required to assess and document the risk related to money laundering and terrorist activity financing in their business. This assessment must be tailored and should consider factors such as customers and business relationships, products, delivery channels and geographic areas where business is conducted, as well as other relevant factors. This assessment is in addition to the client identification, record keeping and reporting requirements.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	FATF released its third evaluation of Canada in February 2008: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Canada%20full.pdf The fourth evaluation of Canada is in process with on-site visits occurring in October and November 2015: http://www.fatf-gafi.org/countries/#Canada In 2014, FATF recognised that Canada had made significant progress in addressing deficiencies identified in the 2008 report and removed Canada from the regular follow-up process: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/FUR-Canada-2014.pdf

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Customer identification is not required for: a) electronic Funds Transfer ("EFT") transactions less than CAD1,000 (approx. USD710); b) foreign currency exchange transactions less than CAD3,000 (approx. USD2,130); c) issuance/redemption of traveller's cheques, money orders or other similar negotiable instruments less than CAD3,000 (approx. USD2,130); and d) cash transactions less than CAD10,000 (approx. USD7,100) (other than when multiple (two or more) transactions occur over a 24 hour time period aggregate to more than CAD10,000 (approx. USD7,100) and are believed to be conducted by or on behalf of the same individual or entity). Customer identification is not required when the transaction exceeds the thresholds noted above provided a signed signature card for an account exists with the institution. In 2014, amendments were introduced to require ongoing monitoring once a business relationship has been established. Non-account-based business relationships are established when the entity conducts two or more transactions in which the identity of an individual must be ascertained or the organization's existence must be confirmed.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Reporting Entities must obtain, verify and maintain the following records of an individual's identity: customer name, date of birth, address, the nature of the customer's principal business or occupation and intended use of the account. Regulations state that the identity of a person should be ascertained by referring to a birth certificate, driver's licence, passport, permanent resident card or any similar record. You can refer to a provincial/territorial health insurance card, but only if it is not prohibited by provincial/territorial legislation. The original document (not a copy) must be reviewed. Legal entities: Reporting Entities must confirm the existence, name and address of any legal entity for which it opens a business account by obtaining such legal documentation as Articles of Incorporation, Articles of Association, Partnership Agreement or other similar record. The record used to confirm the corporation's existence can be in paper or electronic format. If the record is an electronic version, entities must keep a record of the corporation's registration number, the type and source of the record. Furthermore, depending on legal entity type, additional documentation may be required. For example, in the case of a corporation, the name of the corporation's directors, the name, address and principal occupation of all individuals who directly or indirectly own or control 25% or more of the shares of the corporation and information on the ownership, control and structure of the corporation must also be obtained. The identity of up to 3 individuals authorised to transact on behalf of the legal entity must also be verified as well as the evidence of the individuals' authorisation to transact on behalf of the legal entity such as articles of incorporation or the bylaws.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Copies of identification documents are not permitted. In order for a document to be acceptable for identification purposes, it must be valid (i.e. not expired), have a unique identifier number and be issued by a provincial, territorial or federal government. Customer identification through attestation is also permitted, in which case confirmation must be obtained to demonstrate that the customer's ID has been certified to be true and correct by a commissioner of oaths or a guarantor. The attestation method requires that the document is a legible photocopy and contains the name, profession, address and signature of the commissioner of oaths or the guarantor, and the type and number of the identifying document. This method can only be used in conjunction with other prescribed methods of customer identification, including referring to an independent and reliable identification product, cleared cheque or deposit account. It is acceptable for a reporting entity to rely on the customer identification records of an affiliate or co-member when the customer is not physically present, provided that affiliate or co-member viewed the original identification documents. In this case, the reporting entity must verify the individual's name, address and date of birth against the information maintained by the affiliate.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	When a firm has to identify an entity, it must obtain, take reasonable measures to confirm and keep records of the information relating to the entity's beneficial ownership. For a corporation, this includes the name and address of all individuals who directly or indirectly own or control 25% or more of the shares of the corporation. In cases where there is no individual who owns or controls 25% or more of an entity, a record must be kept of the measures taken and the information obtained in order to reach that conclusion. If the information cannot be obtained or its accuracy confirmed, reasonable measures must be taken to ascertain the identity of the most senior managing officer of the entity and treat the entity as high-risk and subject to more frequent monitoring. A record must be maintained explaining why beneficial ownership could not be determined as well as the information pertaining to the most senior managing officer.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	s.62 of the PCMLTF Regulations provides certain exemptions allowing for reduced/simplified due diligence. These include: a) public bodies; b) corporations (and any consolidated subsidiaries) with minimum net assets of CAD75 million (approx. USD54m) on its last audited balance sheet and whose shares are traded on a Canadian stock exchange or a stock exchange that is designated under subsection 262(1) of the Income Tax Act and operates in a country that is a member of the Financial Action Task Force; c) regulated entities such as pension funds, financial entities, securities dealers, investment funds and life insurance companies; and d) the purchase of registered annuity policies or retirement income funds. Simplified due diligence is also permitted with respect to certain products/services, including credit card accounts.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	A firm's compliance program must include the development and application of policies and procedures to assess the risk of a money laundering offence or a terrorist activity financing offence. Special measures should be taken in high risk situations for identifying customers and monitoring transactions. When a risk assessment determines that the risk is high for money laundering or terrorist financing, policies and procedures to keep customer identification information up to date must be developed and more frequent monitoring must be performed. For a financial entity, a securities dealer, a life insurance company, broker or agent, or a money services business, this also applies to keeping beneficial ownership information up to date. All Reporting Entities must develop and apply policies and procedures to keep information on business relationships up to date. This information should be reviewed at a minimum at least every two years. OSFI Guidance states that federally registered or incorporated firms that conduct business in offshore jurisdictions or that have customers that operate in those jurisdictions, need to be especially vigilant. Certain customers may merit additional due diligence, and examples given include businesses that handle large amounts of cash or those that hold important public positions.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	When dealing with PEPs, the following additional due diligence measures must be taken: a) enhanced account monitoring; b) senior management approval to maintain the account or senior management review of transaction within 14 days of account activation or EFT transaction; and c) reasonable measures to obtain source of funds.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The following due diligence requirements are required for correspondent banking relationships: a) obtaining personal information about the foreign entity and its activities; b) ensuring that the foreign entity is not a shell bank; c) obtaining the approval of senior management; and d) setting out in writing the firm's obligations and those of the foreign entity in respect of the correspondent banking services.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Recent amendments have introduced a broader and more flexible set of identification requirements related to non-face-to-face transactions. The requirements set out the following two options for identification of individuals not physically present: a) Confirmation from an affiliated entity that they have ascertained the identity by referring to an original identification document and verify the name, address and date of birth received; or b) Combination of two of the following methods: referring to an independent identification product or, with the individual's permission, referring to a credit file; obtaining an attestation concerning an identification document for the individual from a Commissioner of Oaths or a guarantor; confirming that a cheque drawn on a deposit account with a financial entity (other than one that is exempt from identification requirements) has cleared; and confirming that the individual has a deposit account with a financial entity (other than one that is exempt from identification requirements).

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Suspicious transaction reports ("STRs") are filed with FINTRAC: http://www.fintrac.gc.ca/intro-eng.asp

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of Suspicious Transaction Reports (STRs): 2013 - 14 – 81,735 STRs (Source: FINTRAC http://www.fintrac-canafe.gc.ca/publications/ar/2014/1-eng.asp#s4) Comparative GDP data is not available for this specific period.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes. Under the PCMLTFA, all reporting entities are required to report to FINTRAC transactions for which they have reasonable grounds to suspect that the transactions are related to money laundering or terrorist financing (this includes attempted suspicious transactions). In addition, all reporting entities must report the following transactions to FINTRAC, unless stated otherwise: a) large cash transactions – receipt of an amount of CAD10,000 (approx. USD7,100) or more in the course of a single transaction, or multiple transactions over a 24 hour time period by or on behalf of the same individual or entity; b) electronic funds transfers – international ingoing and outgoing EFTs valued at CAD10,000 (approx. USD7,100) or more in the course of a single transaction, or multiple transactions in a 24 hour time period by or on behalf of the same individual or entity. This requirement applies to financial entities, MSBs (Money Service Business) and casinos; c) terrorist property – a report must be submitted to FINTRAC if a reporting entity has property in its control or possession that is owned or controlled by or on behalf of a terrorist, a terrorist group, or listed person. Nil reports must also be filed by certain reporting entities on a monthly basis with their principal regulators such as OSFI or IIROC. The monthly reporting requirement is separate and distinct from the requirements to immediately disclose detailed information to law enforcement agencies such as the Royal Canadian Mounted Police and the Canadian Security Intelligence Service; and d) casino disbursements – a casino must file a report when it makes a disbursement valued at CAD10,000 (approx. USD7,100) or more in the course of a single transaction, or over the course of multiple transactions in a 24 hour time period by or on behalf of the same individual or entity.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No. All suspicious transactions and attempted suspicious transactions need to be reported. However, s.50 of the Regulations allows for exceptions to reporting Large Cash Transactions (>CAD10,000 (approx. >USD7,100)) for businesses in industries identified in certain sectors of the North American Industry Classification System if a number of conditions have been satisfied.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes. There are criminal or administrative penalties associated with non-compliance with reporting requirements, including tipping off. Both criminal and administrative monetary penalties ("AMPs") cannot be issued against the same instance of non-compliance. AMPs violations are classified by the PCMLTF Regulations as "Minor", "Serious" or "Very Serious" and multiple violations can result in a total amount that exceeds the individual violation limits. a) minor violation: from CAD1 (approx. USD0.71) to CAD1,000 (approx. USD710) per violation; b) serious violation: from CAD1 (approx. USD0.71) to CAD100,000 (approx. USD70,990) per violation; and c) very Serious violation: from CAD1 (approx. USD0.71) to CAD100,000 (approx. USD70,990) per violation for an individual; and from CAD1 (approx. USD0.72) to CAD500,000 (approx. USD354,940) per violation for an entity. FINTRAC may disclose cases of non-compliance to law enforcement when there is extensive non-compliance or little expectation of immediate or future compliance. Criminal penalties may include the following: a) failure to report suspicious transactions: up to CAD2 million (approx. USD1.4m) and/or 5 years imprisonment; b) failure to report a large cash transaction or an electronic funds transfer: up to CAD500,000 (approx. USD354,940) for the first offence, CAD1 million (approx. USD709,870) for subsequent offences; c) failure to meet record keeping requirements: up to CAD500,000 (approx. USD354,940) and/or 5 years imprisonment; d) failure to provide assistance or provide information during compliance examination: up to CAD500,000 (approx. USD354,940) and/or 5 years imprisonment; and e) disclosing the fact that a suspicious transaction report was made, or disclosing the contents of such a report, with the intent to prejudice a criminal investigation: up to 2 years imprisonment.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	The regulations do not specify whether transaction monitoring can be performed outside of Canada.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No however, federally registered or incorporated financial institutions are required to test all key AML/ATF program components at least every two years.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	a) yes; b) does not apply – only personally identifiable information is covered under Canada's Privacy laws; and c) not explicitly defined, however examples are provided in the Schedule 1 PIPEDA, Section 4.3.4 (Canada's Privacy Law). Sensitivity of information is considered, in some cases, to be dependent on the situation.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Prohibited unless the customer allows the transfer of this information based on the premise of informed consent.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	None that we are aware of.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Cayman Islands

Key contact: Charles Bolland
Email: charles.bolland@ky.pwc.com
Tel: +1 345 914 8610

Postal address: P.O. Box 258, 18 Forum Lane,
Camana Bay, George Town, Grand Cayman
Cayman Islands KY1-1104

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1996. However the Proceeds of Crime Law, enacted into legislation in Sept 2008, repealed the previous Anti Money Laundering Law (the Proceeds of Criminal Conduct) in order to bring harmonisation with all other laws that could encompass money laundering. Additionally, and as a result of the introduction of the Proceeds of Crime Law, the Money Laundering Regulations (2015 revision) and the Guidance Notes ("Guidance Notes") on the Prevention & Detection of Money Laundering in the Cayman Islands (Aug 2015 revision) were also amended.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	The regulator for AML controls is the Cayman Islands Monetary Authority ("CIMA"): http://www.cimoney.com.ky
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, CIMA has issued the Guidance Notes which can be found at: http://www.cimoney.com.ky/AML_CFT/aml_cft.aspx?id=144
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, a risk based approach is facilitated both by way of certain exemptions for particular products, and an explanation within the Guidance Notes that a risk based, rather than a 'tick box' approach, should be adopted.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The country was subject to an IMF inspection in 2009, the results of the inspection can be found at: http://www.cimoney.com.ky/ext_coop_assess/eca.aspx?id=180

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, customer due diligence is not required for one-off transactions of less than KYD15,000 (approx. USD20,000).
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: certified photo identification (usually passport); verification of residential address (driving licence or utility bill etc.); source of funds and understanding of source of wealth. Corporates: must identify the company, its directors and beneficial owners of 10% or more of the company's holdings. Company items such as Memorandum and Articles of Association, Certificate of Incorporation, register of members, directors and officers, authorised signatory lists, financial statements etc. are required on acceptance of new business. Further, due diligence on at least two directors and due diligence on beneficial owners of greater than 10% as described for individuals or 'natural persons' as above.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Documents must be originals, notarised or certified copies. Examples of suitable certifiers are lawyers, accountants, notary publics or civil servants.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	All beneficial owners of 10% or greater of a company's holdings must be identified/verified. Beneficial owners below 10% should be identified if the entity appears structured to avoid this requirement. Note that certain entities are exempt, such as those listed on a recognised stock exchange.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced/simplified due diligence requirements exist for the following scenarios. Key exemptions include: a) non paying accounts, effectively covering mutual fund investments if the funds can only be returned to the beneficial owner from which they came; b) regulated financial institutions in certain jurisdictions listed in Schedule III of the Regulations; (Note: Appendix H to the Guidance Notes was amended in Aug 2015 to add the Gibraltar Stock Exchange, Dubai Financial Market and the NASDAQ Dubai to the list of Approved Markets and Exchanges. Further Section 3.104 (d) of the Notes was amended to simplify the process of adding stock exchanges to Appendix H. As a result of this, documentary evidence of identity will not be required if the client is a company or fund listed/quoted on these exchanges). c) potentially any circumstance in which a full eligible introducers form is used (and the party relying on the eligible introducer form remains liable for any failure of the person making the introduction to obtain and record satisfactory evidence of the identity of the third party); d) listed institutions on certain specified exchanges and their subsidiaries (evidence must be provided for use of exemption); and e) certain other bodies, for example governmental bodies and pension funds for professional associations.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Local guidance includes information on enhanced due diligence for PEPs, high risk countries or other higher risk businesses, such as not for profit associations (including charities).
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	Local guidance requires senior management approval, reasonable measures to establish source of wealth and funds and enhanced ongoing monitoring.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	No enhanced due diligence measures required for regulated correspondent banking relationships (see also response to A16 below).
Q16.	Are relationships with shell banks specifically prohibited?
A16.	The Money Laundering Regulations (2015) Revision state that no person conducting relevant financial business should form a business relationship or carry out a one-off transaction, with any institution that has no physical presence in the territory in which it is incorporated or in which it is carrying on such business and is unaffiliated with a regulated financial group that is subject to consolidated supervision. Further clarification on correspondent banking relationships with shell banks is provided in the Money Laundering Guidance Notes (http://www.cimoney.com.ky/AML_CFT/aml_cft.aspx?id=144).
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In response to a recommendation from the CFATF (“Caribbean Financial Action Task Force”) during their 2007 evaluation of the Cayman Islands’ money laundering regime, the Guidance Notes on Money Laundering have been amended to indicate that financial institutions should have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The Money Laundering Regulations require that Suspicious Activity Reports are made to the Financial Reporting Authority (the “FRA”): http://www.fra.gov.ky

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 558 SARs (Source: Cayman Islands Financial Reporting Authority). Comparative GDP data is not available for this specific period.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Other than SARs, payment service providers are required to report to the FRA if they restrict or terminate business relationships with its payee service providers due to the payee service provider regularly supplying insufficient information on the payee.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	See response to A8.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, per section 139 of the Proceeds of Crime Law, a person is guilty of an offence if they know or suspect that a report is about to, or has been made and discloses to any other person information which is likely to prejudice an investigation punishable under the law by a maximum prison term of five years, an unlimited fine or both.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	While the use of automated mechanisms to monitor suspicious transactions is suggested by the Guidance Notes as best practice, it is recognised that this may not be cost effective for all companies. As such there is no legal or regulatory requirement to use automated suspicious transaction monitoring technology.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	There is no requirement to obtain authorisation from the FRA to proceed with a current/ongoing transaction that is identified as suspicious unless criminal proceedings have commenced and the matter becomes subject to the Attorney General's direction and a resulting freeze order. In that case, direction would be required from the Attorney General prior to proceeding with the transaction.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	There is no explicit direction in local legislation on monitoring transactions outside the jurisdiction. However the Guidance Notes do recognise parent/subsidiary relations and also customer transactions for their own account and makes allowance for minimised KYC procedures when such transactions occur in countries with equivalent legislation as the Cayman Islands (also known as Schedule 3 countries).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	There is no legal requirement for the bank's external auditor or any other external organisation to report on the bank's AML systems and controls. However, per Section 13 (1) (e) (iii) of the Banks and Trust Companies Law (2013 Revision) if an auditor, in the course of carrying out an audit on the accounts of a licensee, obtains or suspects that the licensee is carrying on or attempting to carry on business without compliance with the Money Laundering Regulations (2013 Revision), the auditor shall give the Authority written notice of his information or suspicion and in the case of suspicion, his reason for that suspicion.
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, data protection specifically is covered by the Electronic Transactions Law 2000 and more broadly by the Confidential Relationships (Preservation) Law ("CRPL") (2009 Revision) which is covered in more detail in A32 below: a) the definition of personal data per the Electronic Transactions Law is defined as data which relate to a person who can be identified from those data; or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller. Thus the definition covers all data related to a person which infers coverage of KYC material; b) the above Law does not specifically address corporate data, however Section 26 (1) b states that information which relates to the private affairs of any individual or to any particular business shall be deemed to be confidential information for the purpose of the CRPL; and c) no separate definition of sensitive data exists.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes, the CRPL was originally enacted in 1976 to protect business dealings and impose strict penalties on those disclosing confidential information unlawfully. The CRPL defines confidential information as including information concerning any property which the recipient thereof is not, other than in the normal course of business, authorised by the principal to divulge. Property includes every present, contingent and future interest or claim direct or indirect, legal or equitable, positive or negative, in any money, money's worth, real estate etc. and all documents and things evidencing or relating thereto. Therefore, pursuant to the CRPL, divulging any confidential information otherwise than as expressly permitted by the Law is a criminal offence.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	There are several cases in the Cayman Islands on the application of CRPL, namely: a) Gippet v Cayman National Bank 2006 CILR Note 32; b) Ansbacher (Cayman) Limited (Grand Court) 2001 CILR 214; and c) Corporacion Nacional Del Cobre de Chile (In re Codelco) 1999 CILR 42. Further, the Cayman Islands has entered into various Tax Information Exchange Agreements ("TIEAs") or Bilateral Agreements and Arrangements with 36 governments, therefore it is possible that in instances where there are no TIEAs in place between a country and the Cayman Islands, this may impact transfer of information. In addition, Cayman has entered into a multilateral agreement, along with representatives from more than 50 jurisdictions, and implemented the Common Reporting Standards by introducing legislation and regulations effective 16 Oct 2015. The first reporting to the regulator by industry under the regulations is due 31 May 2017.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes, the CRPL as stated above codifies the common law duty of confidentiality owed by a bank to its customers and extends it to other professional relationships. Further, certain information in relation to companies under the Companies Law is confidential in the Cayman Islands. Exempted companies are required by Section 44 of the Companies Law to maintain a register of members at the registered office of the company, but this is not open to public inspection.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Chile

Key contacts: Carmen Gloria del Valle / Pedro Trevisan
Email: Carmen.gloria.del.valle@cl.pwc.com /
pedro.trevisan@cl.pwc.com
Tel: +56 2 29400182 / +56 2 29400574

Postal address: Av. Andrés Bello 2711
Piso 1, Las Condes,
Santiago, Chile

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	In 1995, money laundering was incorporated as a crime in the Chilean Penal System by law N°19.366. In December 2003, law N°19.913 was promulgated. This law created a specific Financial Analysis Unit "Unidad de Análisis Financiero" to prevent and stop money laundering. In December 2009, law N° 20.393 was published. This law established the penal responsibility of legal entities relating to the crimes of money laundering, financing of terrorism and bribery. In February 2015, law N° 20.818 was promulgated and published. This law established guidelines for public entities about Article 3 Law N°. 19.913.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.)? Please include link to the regulator(s) website
A3.	In Chile, the Financial Analysis Unit (Unidad de Análisis Financiero, ("UAF")) coordinates the national AML/CFT System. a) the banking sector is regulated by the "Superintendencia de Bancos e Instituciones Financieras", ("SBIF") (http://www.sbif.cl/sbifweb/servlet/Portada?indice=0.0); b) the main AML regulator for financial institutions (including the banking sector) is called "Unidad de Análisis Financiero" ("UAF") (http://www.uaf.cl/english/whatwedo.aspx). The insurance sector and brokers are also regulated by "Superintendencia de Valores y Seguros" ("SVS") (http://www.svs.cl/portal/principal/605/w3-channel.html); c) the main AML regulator for the non-financial sector is also "Unidad de Análisis Financiero" ("UAF") (http://www.uaf.cl/english/whatwedo.aspx); d) the casinos sector is regulated by the "Superintendencia de Casinos y juegos", ("SCJ") (http://www.scj.gob.cl/en/); and e) the pensions and social security by the "Superintendencia de Pensiones y Seguridad Social", ("SP") (http://www.safp.cl/portal/institucional/578/w3-propertyvalue-5925.html).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, there are several instructions given by the regulators that are mandatory for institutions. a) "Manual para la prevención del blanqueo de capitales" - published by the "Asociación de Bancos e Instituciones Financieras de Chile A.G." (http://www.abif.cl/about-the-association-of-banks/); b) "Recomendaciones para la identificación y procedimientos relacionados con Personas Expuestas Políticamente ("PEP")." (http://www.uaf.cl/legislacion/norm_sector.aspx); c) "Circular conjunta N° 50 de Unidad de Análisis Financiero y N° 57 de Superintendencia de Casinos de Juegos" (http://www.uaf.cl/legislacion/norm_sector.aspx). This link gives several guidelines for various industries.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	N/A
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, enhanced due diligence, know your customer, know your employee, know your supplier, are all systems that must be configured as a tool of risk management to prevent money laundering and the financing of terrorism.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	N/A (The last mutual evaluation was performed in 2010 (http://www.gafilat.org/UserFiles/documentos/en/evaluaciones_mutuas/Chile_3ra_Ronda_2010.pdf).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	UAF regulations establish that financial institutions and certain non-financial institutions must implement an AML System based on the KYC concept. This system must allow the understanding of the client's activities, relevant characteristics of operations and its reasonability. The following information and documentation is required to identify clients: a) individual / entity name; b) Rol Único Tributario ("RUT") number (the National Identification Number for individuals and legal entities, similar to Social Security Numbers for individuals or Employer ID Numbers for entities); c) individual profession or degree / entity economic activities; d) invoice number; e) address in Chile or in country of origin / residency; and f) email and / or phone number.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	According to SBIF regulations, banking institutions should apply appropriate procedures to verify that the information provided by clients is valid and accurate. If the information is not reliable or the client does not provide information for proper identification, the bank must evaluate the termination of the commercial relationship and send a suspicious operation report to UAF.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	UAF Regulations specifically require the reviewing of clients, prospective clients and UBOs to identify if any party is a PEP. Local regulation does not explicitly establish an ownership threshold to define UBOs.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	There is no reduced/simplified due diligence recognised in local regulations. Local regulations establish minimum KYC requirements for Enhance Due Diligence ("EDD").
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Special due diligence and KYC procedures must be applied to: a) PEPs (escalation to management for approval); b) electronic transfers (information about the transferor must be kept); c) individuals and members listed in "Comité de Sanciones ONU" (UN sanctions about N° 1.267 of 1999, N° 1.333 of 2000 and N°1.390 of 2002 resolutions) (continuous monitoring - information obtained must be reported to UAF); d) non-cooperative countries/jurisdictions/territories and tax havens (transactions with these countries/jurisdictions/territories must be reviewed and reported to UAF); and e) customer who exercises one of activities described in Article 3 Law N°19.913.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Financial institutions and certain non-financial institutions must implement special due diligence procedures for PEPs: a) establish risk management systems to determine if a prospective client, a client or a final beneficiary is a PEP or not; b) require and obtain senior management approval to establish a relationship with a PEP; c) take reasonable measures to determine the source of wealth and funds of clients and final beneficiaries identified as PEPs and the reasonability of the operations; and d) implement measures and procedures of continuous due diligence regarding the relationship with the PEP.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	According to RAN Chapter 1-14, the following additional KYC measures must be performed when establishing a correspondent banking relationship: a) gather sufficient information to fully understand the correspondent bank's business and verify its reputation and control quality; b) assess the policies and procedures performed by the correspondent bank to detect suspicious activities; c) document the responsibilities of each institution; and d) obtain management approval to establish a new correspondent banking relationship.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	According to RAN Chapter 1-14, banks must abstain from starting relationships or performing operations with shell banks.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	There is no specific mention in local AML regulations about this subject.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Financial Analysis Unit "Unidad de Análisis Financiero" (http://www.uaf.cl/entidades/como.aspx).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2015 – 2,356 SARs (Source: http://www.uaf.cl/estadisticas/) Comparative GDP data is not available for this specific period.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Cash transactions over USD10,000 must be reported.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	There are no thresholds for suspicious activity reports.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes. The failure to comply with the reporting requirements is considered an infraction to Law 19.913. Any entities and individuals involved may be sanctioned.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Yes. According to RAN Chapter 1-14, banks must have appropriate technological tools that allow them to develop warning systems, in order to identify and detect unusual transactions.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	According to local regulation, every suspicious operation must be reported as fast as possible and in an unobstructed manner to the UAF. Reports must be filed in an electronic format. Financial institutions and certain non-financial institutions must establish internal procedures to report suspicious operations opportunistically and under reserve.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No. According to RAN Chapter 1-14, if the bank has branches or subsidiaries abroad, the Board must ensure that the laws and regulations of the host country adequately meet the requirements of this chapter.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No, there is no legal requirement for an external auditor to provide an opinion or report on the bank's AML systems and controls. Information about suspicious activity reports and controls is not audited. During the financial statement audit, the external auditor is informed about the suspicious activity reports to evaluate if there is any impact on the audit process.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, Law No. 19.628 regarding Privacy Protection ("Protección de la vida privada") regulates the treatment and use of personal data. Among other matters, this legislation prevents the disclosure of certain financial information. Note that Law N° 19.628 defines "personal data treatment" as any operation or group of operations or technical procedures – whether automatic or not - that allows personal data to be collected, stored, recorded, organised, prepared, selected, extracted, compared, connected, separated, communicated, assigned, transferred, transmitted or cancelled, or utilised in any other form: a) yes, as "personal data" is defined by Law N° 19.628 as any data related to an identified or identifiable individual; b) it does not. Law N° 19628 applies only to data relating to individuals. However, professional secrecy regulations and contractual obligations mean such data must be kept as confidential information. Therefore, its disclosure or transfer can only be authorised by the entity that owns the data; and c) "Sensitive data" is defined by Law N° 19.628 as any personal data relating to physical or moral characteristics of individuals, or to facts or circumstances of their private life or intimacy. Note that according to Law N° 19.628, any kind of personal data treatment shall be expressly authorised by the data subject (individual), in writing, and prior to the data treatment. The data subject shall be informed about the purposes of its data treatment, and is entitled to revoke such authorisation, among other rights. As a general rule, "sensitive data" cannot be treated in any form, except: a. when it is expressly authorised by law; b. when the "sensitive data" is required for granting health benefits to the data subject; and c. when the data subject expressly authorises the "sensitive data" treatment as described immediately above.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Any transfer of personal data shall be authorised by the data subject as described in A29 c) above. Regarding credit reports, no data subject authorisation is required when the information comes from, or is collected by, public sources, as long as the data corresponds to economic, financial, banking and commercial information contained in lists referred to a category of individuals that only indicates certain information (individual's group, occupation, professional or technical degrees, birth date, address), or is needed for commercial communications requiring a direct answer or the direct sale of goods and services. On the other hand, article 17 of Law 19.628 allows the communication of economic, financial, banking and commercial liabilities when these are not duly paid, and are expressed in certain commercial instruments (e.g. unpaid checks, notes, banking loans, mortgages, etc.). In general, this kind of report cannot include: liabilities that have been renegotiated, are subject to negotiation or are subject to pending terms or conditions; utilities debts; debts incurred during unemployment periods; and, liabilities that became enforceable 5 years previously. Regarding criminal records, this information can be understood as "sensitive data", and its treatment is only allowed as described in A29 c). Although, if this data is treated by a government or public organisation (public services, public authorities, etc.) within its legal faculties, no data subject authorisation is needed for data treatment purposes. In relation to criminal records, administrative penalties or disciplinary faults, this information cannot be communicated after the statute of limitation period for pursuing those sanctions has elapsed, except in cases where such information is requested by the courts of justice or other competent authorities and such information is kept under secrecy. Regarding medical data, this information can be understood as "sensitive data", and its treatment is only allowed as described in A29 c). As mentioned in A29 c) b., the treatment of this kind of personal data is allowed when it is required for granting health benefits to the data subject, with no data subject authorisation.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Article 19 N° 4 of the Chilean Constitution set forth the constitutional right of respect and protection of private life and honour of an individual and their family. If this constitutional right is breached or threatened to be breached by anyone, the data subject can exercise protective actions or remedy (recurso de protección) before the high court of each judicial territory (Appeal Court, Corte de Apelación).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. Title XVI of "Ley General de Bancos" establishes the bank secrecy law. According to this law, deposits and investments are subject to bank secrecy. Other operations are under reserve.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Colombia

Key contact: Mónica Jiménez / Ana Milena Villareal
Email: monica.jimenez@co.pwc.com /
ana.milena.villareal@co.pwc.com
Tel: +571 6340555

Postal address: Calle 100 No 11-A-35;
9th. Floor; Bogotá;
Cundinamarca; Colombia

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1996. Financial institutions had to comply with the Integral System for the Prevention of Asset Laundering ("SIPLA") regulation by reporting financial transactions over defined limits. In 2008, the Superintendent of Finance of Colombia issued External Circular No. 022 2007, regarding the implementation of the System for Preventing Asset Laundering and Terrorism Financing ("SARLAFT") with a risk based approach. The 2009 regulation incorporates some new reporting standards that must be adhered to when reporting to the Regulator. Currently Circular Basica Juridica 029 de 2014 in its Título IV Capitulo IV regulates ("SARLAFT"). In 2014, the Superintendent of Corporations of Colombia issued External Circular No. 100-00005, regarding the implementation of the System for Preventing Assets Laundering and Terrorism Financing and was changed for the External Circular No. 100-00003 in Jun 2015.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The main features of the regulation included implementing adequate KYC procedures, monitoring transactions, investigating unusual transactions and reporting any suspicious transactions to the relevant authorities. The latest circular had no major changes compared to the previous one.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	SARLAFT requirements are issued by the regulators, the Superintendence of Finance of Colombia and Superintendence of Societies of Colombia. Entities have to report to the Financial Information and Analysis Unit ("UIAF") of Colombia. a) (https://www.superfinanciera.gov.co) in section Normativa/NormativaGeneral/CircularBasicaJuridica(C.E029/14)/ParteI/TituloIV/CapituloIV; b) (https://www.superfinanciera.gov.co) in section Normativa/NormativaGeneral/CircularBasicaJuridica(C.E029/14)/ParteI/TituloIV/CapituloIV; and c) (http://www.supersociedades.gov.co) in section Normatividad/circulares-externas/CircularExterna100-00005 Junio del 2014.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The regulation provides specific details of how the SARLAFT should be considered by financial institutions. Although the segmentation methodologies and activities related to risk management and transactional monitoring should be designed by each individual entity. For entities of the real sector there is a guide created by the United Nations Office on Drugs and Crime ("UNODC"), the British Embassy and the chamber of commerce of Bogotá "El Modelo de Gestion del Riesgo de LA/FT en el sector real". (https://www.superfinanciera.gov.co) in section Normativa/NormativaGeneral/CircularBasicaJuridica(C.E029/14)/Partel/TituloIV/CapituloIV/Anexos. (https://www.superfinanciera.gov.co) in section Normativa/Índice de Reportes/Guías para el reporte de información.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, new regulation establishes the parameters for KYC procedures which incorporate the requirement to update a customer's information.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, new regulation has a risk based approach regarding AML.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No. Colombia is a member of the Financial Action Task Force on Money Laundering in South America ("GAFISUD").

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, there are various thresholds depending on the type of transaction, including no customer due diligence for the transfer of electronic funds or foreign currency exchange transactions less than USD5,000, and if a signed signature card for an account with the institution also exists for such transactions over USD5,000. No due diligence is required for cash transactions of less than USD5,000 (other than when two or more transactions totalling more than USD5,000 are believed to be linked).
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: The regulator has defined the basic form each customer should complete. The requirements surrounding independent verification or authentication vary according to each customer. Individuals should provide identification, tax payment copy or yearly income certificate and other relevant financial information. Legal entities: The regulator has defined the basic form that legal entities should complete. Legal entities should provide Chamber of Commerce registration, details of partners with shares greater than 5%, an antitax payments certificate and other relevant financial information.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	There is no need for copies to be certified by a notary (this was a requirement previously). Entities compare the copy with the original identification when the customer brings in the required documentation.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Customers should be able to demonstrate the source of income and ownership by way of a copy of a tax payment or income certificate. Entities should monitor changes in income or properties of their clients, where information is available.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Entities should comply with the minimum requirements of the regulations, which include special additional tasks for PEPs. Reduced requirements apply to persons or companies that operate with significant cash amounts as a result of the business they are in. The entities should perform detailed due diligence so future controls can be omitted. There are some cases in which customers do not need to fill out the form e.g. special insurance types, multilateral organisms, retirement fund managers and deposit accounts with a simplified process.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence is required for PEPs. In Colombia, this includes not only politically related people but also publicly recognised people. This also includes due diligence of deposit accounts which will be used by political parties and during political campaigns.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	There are regulatory requirements in relation to PEPs. In Colombia, a PEP is defined as a publicly relevant person (not only politicians). Each time a PEP is identified, additional due diligence has to be performed, especially when the client manages public resources.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	For correspondent banking relationships, every international transaction should be reported to the authorities. Each report requires information on the origin of the money i.e. client, address, telephone number, activity and reason for sending the wire and beneficiary.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	No.
Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	Entities must define special procedures in order to perform KYC for non-face-to-face interviews. They must also implement follow up procedures for clients' transactions.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	UIAF of Colombia: (www.uiaf.gov.co)
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on SARs is not available for 2015, please see below the most recent data available. Volume of SARs: 2013 – 6,993 SARs (Source: UIAF). GDP (in current prices): 2013 – USD380,063m (Source: data.worldbank.org). This results in a ratio of 1 SAR for every USD54m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, institutions should report individual cash transactions above USD5,000 and total monthly cash transactions above USD25,000. They should also report: a) suspicious transactions b) transactions of remittances and buy and sell of foreign exchange; c) transactions with international credits cards; d) products offered; and e) information about campaigns and parties political.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	See A20.
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Special requirements and an investigation from the regulator shall be performed at an institution that does not report the required periodical AML information.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No, each entity is free to develop or use their specific methodology to perform transaction monitoring according to their KYC policies.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No, each entity shall define if a suspicious transaction shall be continued or not, although it has to be reported to the UIAF.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Entities monitor all transactions regardless of the entity's jurisdiction.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes, the financial Colombian regulation defines that the external auditor must perform audits of the AML risk management system quarterly. Additionally, the internal auditor must perform an audit annually.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) the external auditor performs an audit quarterly; b) the results are reported to the board of directors; and c) the final opinion is part of the financial statement audit.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	The external and internal auditors must evaluate that the risk management system is operating according to all requirements of the regulation. The audit is performed in accordance with the auditor judgement who designs the tests necessary to assure that the entity is complying with the regulation.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	In Colombia, the regulation for personal data protection stipulates that all individuals have the right to know about and update personal information that has been gathered about them by public or private entities and prohibits the processing of any individual's sensitive information without the prior, explicit, and informed consent of that individual. Sensitive data is expressly protected. The law has a reinforced protection for so-called sensitive data, which is information that deserves special protection because of the high risk posed by its processing to citizen's rights and freedoms. The incorrect use of this sensitive data might cause discrimination. Sensitive data includes people's racial and ethnic origins; colour and sexuality; their political, religious, philosophical, or other beliefs; their participation in a given association; or their membership in a trade union, among others.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	In Colombian legislation, banking secrecy and the right to privacy are not considered valid arguments to reject banking information requests issued by judges of the Republic of Colombia or Colombian AML authorities, within the limits established by article 15 of the Constitution and 2 of Law 1121 of 2006, also known as Organic Statute of the Financial ("EOSF"). Banking secrecy includes the financial and personal information in custody of the financial entities. Information relating to criminal records (those that are part of ongoing investigations without final decision of competent authority) and medical histories are considered sensitive and require prior, explicit and written authorization of the owner to be transferred.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Refer to A30. Habeas Data law expressly prohibits the transfer of information to another country without the prior, express and written permission of the owner of the information and further states that the other country must have an equal or higher standard of protection of information and guarantees for the owner of the information.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Refer to A30.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Dominican Republic

Key contact: Omar del Orbe
Email: omar.delorbe@do.pwc.com
Tel: +829 642 7712

Postal address: Lope de Vega ave, #29, Novo Centro Bldg.
PwC Floor, P.O. Box 1286
Santo Domingo – República Dominicana

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	AML Law in the Dominican Republic (Law No. 72-02 and modifications on Anti-Money Laundering from Illicit Traffic of Drugs and Controlled Substances and other Serious Violations) was enacted on 4 Jun 2002. Subsequently in 2003, the implementation guideline No. 20-03 was issued.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	As a result of local AML Law No. 72-02, the National Committee Against Money Laundering was created and composed of: a) Superintendence of Banks ("SIB"); b) Ministry of Treasury; c) Attorney General of the Dominican Republic; d) President of the National Drugs Council; and e) President of the National Directorate for Drug Control. This Committee is comprised of a Unit of Financial Analysis ("UAF") to which the different organizations against money laundering in the Dominican Republic report to. The unit covers the banking sector, other financial services, and non-financial sectors. a) Superintendence of Banks of the Dominican Republic ("SIB"): (http://sib.gov.do/); b) General Directorate of Internal Revenue: (http://www.dgii.gov.do/); c) Superintendence of Securities of the Dominican Republic: (http://www.siv.gov.do/); d) Superintendence of Pensions of the Dominican Republic: (http://www.sipen.gov.do/); e) General Directorate of Customs: (https://www.aduanas.gob.do/); f) Specialized Attorney for the Persecution of Administrative Corruption: (http://dpca.pgr.gob.do/); g) Central Directorate of Criminal Investigations: (http://www.dicrim.gob.do/); h) Anti-money laundering unit of the Attorney General's office of the Dominican Republic: (http://pgr.gob.do/); and i) Financial Investigation department of the National Directorate for Drug Control: (http://www.dncd.gob.do/). Central Bank of the Dominican Republic ("CBDR") has its own internal regulation based on Law No. 72-02: http://www.bancentral.gov.do/normativa/normas_vigentes/normas_preencion_lavado_activos.pdf

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The Law and the implementation guideline Law have definitions of suspicious or unusual transactions that could be associated to money laundering. However, there are no other practical guidelines.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, the regulators promote a proactive approach that is based on risk. According to the Newsletter No. 014-12 issued by the SIB in Oct 2012, the Framework Supervision of Financial Entities based on risk was finally adopted.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The last assessment was in 2006 and a follow-up report was released in 2015: http://www.fatf-gafi.org/countries/#Dominican Republic and https://www.cfatf-gafic.org/index.php/member-countries/d-m/dominican-republic

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No, according to the Newsletter No. 03-10 issued by the SIB, the due diligence process should be applied to all customers that carry out significant transactions (refer to the guide "Know your customer (KYC)" issued by the SIB (http://www.sib.gob.do/pdf/lavado/TERCERA-EDICION-Instructivo-Conozca-Su-Cliente-Ready.pdf)).

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: a) name and surname; b) date and place of birth; c) identification number; d) marital status; e) address and telephone number; f) main activity or occupation; and g) income (salary and other savings). Legal entities: a) company name; b) date of incorporation; c) address and telephone number; d) tax identification number; e) bylaws and other information; f) main activity; g) revenue volume; and h) shareholders and ultimate beneficial owners;
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Legal entities accepting the identification documentation should be sure that the copies of such documentation correspond to the originals, i.e. either a contractor's internal verification or external authentication (notary, apostille) will be needed. Each institution also has its own policies and procedures to verify the documents and its copies.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Financial institutions must implement procedures to identify the ultimate beneficial owner of each transaction, review of records of the Company's institution, obtain personal and bank references on each of the major shareholders and directors, verify their identity and register their names.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced/simplified due diligence arrangements are available to 'occasional customers'. The SIB regulation defines 'occasional customers' as those who do not demand transactions on a permanent basis and whose total amount of transactions with the institution is less than USD10,000.
Q13.	In what circumstances are enhanced customers due diligence measures required?
A13.	A Corresponding Bank Customer who receives a substantial portion of their income from their businesses activity with high risk clients may present greater risks. A Corresponding Bank Customer who presents greater risks, PEPS and NGOs or foundations should be subject to a higher level of due diligence. See A15 and A14.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Financial institutions should apply additional due diligence procedures in the case of PEPs, their relatives and their associates. Financial institutions should: a) verify their reputation with public sources; b) investigate the source of the applicant's funds before opening an account; c) anticipate the account's activity; d) execute more continuous monitoring of the trade relationship, for a PEP to be accepted as a client; and e) if a PEP has control or directive functions in a correspondent bank, the entity should have knowledge of that person's role in said entity. Banks issue a form of politically exposed persons twice per year (PEP01).
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	According Article 8, section D of the instructive "Know your customer ("KYC")" issued by the SIB, the due diligence process of a corresponding banking that involves greater risks will include: a) for all control units, verify the source of wealth of the proprietors, including their reputation/credibility in the market, as well as recent changes in ownership; and b) investigate the experience and competency of each member of executive commission, as well as recent changes in the structure of the Directorate.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Article 18 of local regulations for foreign investments and opening of border institutions issued in 2004 by the Monetary Board, prohibits banks from operations with shell banks.
Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	Although this is not explicitly stated in AML Law 72-02, KYC establishes procedures to identify physical or legal persons who receive or transfer funds to clients. In addition, financial institutions have alerts for non-face-to-face transactions.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Reports are made to the Financial Analysis Unit (UAF). Please refer to A3: http://www.uaf.gov.do/
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes: a) cash transactions exceeding USD10,000 (IF01 form); b) electronic transfers up to USD1,000 (FD03-B form); c) daily report of remittance (FD03-A form); and d) transport of cash and bearer securities exceeding USD10,000 (FD04 form).
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Yes, please refer to A20 above. However, all suspicious transactions should be reported in according to the paragraph 5 of Art. 41 of the Law 72-02.
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Yes, Article 22 of AML Law 72-02 establishes imprisonment of 2-5 years and a fine of 50-100 minimum wage salaries.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No requirements from a legal or regulatory standpoint exist for the use of automated suspicious transactions.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	After a certain time, if there is no a response from UAF regarding the reported transaction, the institution should determine if it is appropriate to proceed or not with the transaction in question.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	According to Art. 61 and 62 of AML Law 72-02, the competent authority may submit and request assistance from the competent authorities of other States.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organization to report on the bank's AML systems and controls?
A26.	There is no legal requirement for a bank's external auditor or other external organization to report on the bank's AML systems and controls.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A. See A26 above.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A. See A26 above.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How it defined and what is are the additional protections?
A29.	In the Dominican Republic there is a specific data protection law (Law 172-13). a) the definition of personal Data Protection does not cover any direct information about KYC. KYC is a guide issued by the Superintendence of Banks; b) according to the Art. 4 of this law, the protection regime of personal data does not apply to data processing of corporations; and c) sensitive data: personal data revealing political opinions, religious, philosophical or moral beliefs, trade union membership and data concerning health or sex life. This law aims at comprehensive protection of personal data in files, public records, data banks or other technical means of processing of data intended to give information, whether public or private, and to ensure the right to honor and protect individual's privacy.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Additional prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes) is not considered in AML Law 72-02, however financial entities and other users are available to use credit bureaus and criminal records.

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Law 172-13 of Personal Data Protection regulates the Personal Data Transfer; however according to Art. 89 of this law, in relation to any international agreement to which the Dominican Republic is a signatory (such as information exchange treaty between the Dominican Republic and USA, and the information exchange dispositions included in the treaties to avoid double taxation- currently signed with Canada and Spain- shall be governed by its dispositions.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Article 56, Paragraph b) of the Monetary and Financial Law No. 183-02 establishes the legal obligation of banking secrecy and confidentiality.



'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Ecuador

Key contact: Esteban Valencia / Roberto Tugendhat
 Email: esteban.valencia@ec.pwc.com /
Roberto.tugendhat@ec.pwc.com
 Tel: +(593)2 382 9350 Ext. 334 /+ (593) 4 370 0220 Ext. 201

Postal address: Av. Francisco de Orellana E4-430 y Av.
 Amazonas, Piso 4,
 Quito, Ecuador

Last updated:
 January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2005. Regulation to Prevent, Detect and Eradicate Money Laundering and Financing of Crimes (hereinafter Law to Prevent Money Laundering - LPML) which should be complied by entities pertaining to the financial system and insurance sector to report financial transactions above the established thresholds. In 2007 the Superintendence of Banks of Ecuador issued resolutions that govern the activities to prevent money laundering, terrorism financing and other crimes on a risk oriented approach. 2010 The LPLM regulation added other controlled entities to the list included in the LMPL that must adhere when reporting to the Regulator. In Jul 2014, the Superintendence of Companies, Securities and Insurance issued standards to prevent money laundering and terrorism financing, which are managed through the National Entity for Money Laundering Prevention. In addition to the Regulation to Prevent, Detect and Eradicate Money Laundering and Financing of Crimes, there are currently two set of laws that regulate two groups of companies: i. Stock exchanges, brokerage houses, and fund managers and trusts; and ii. Credit unions, foundations and NGO's; retailing of vehicles, crafts, ships, and aircrafts; security transportation services, postal packages services, parallel postal services; travel agencies and tourism companies; real estate intermediaries and construction services, casinos and betting houses, slot machines and racetracks; pawnbrokers; pawn shops, jewelry dealers, precious gems; traders of antique and art pieces; notaries and property registrants.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The primary characteristics of the LPML request the implementation of KYC procedures to oversight transactions, follow up unusual transactions and report to correspondent authorities in case of arising any suspicious transactions.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) companies comprising the financial sector are regulated by the "Superintendencia de Bancos del Ecuador", SBE (http://www.sbs.gob.ec), and the other companies by the "Superintendencia de Compañías, Securities and Insurance del Ecuador" (http://www.supercias.gob.ec); b) the primary regulator for financial institutions and the non-financial sector is denominated "Unidad de Análisis Financiero" ("UAF") (http://www.uaf.gob.ec/); and c) the main regulator for AML controls is UAF which uses the SISLAFT system to prevent asset laundering and terrorism financing ("SISLAFT") (https://sislaft.uaf.gob.ec/sislaft).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes. Please refer to the legislation mentioned in A1.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, the new regulation is risk based oriented in connection to AML.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Ecuador is a member of the Financial Action Task Force on Money Laundering in South America ("GAFISUD"). The last mutual evaluation was carried out in 2011: http://www.gafilat.org/UserFiles/documentos/es/evaluaciones_mutuas/Ecuador_3era_Ronda_2011.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	According to requirements of the Superintendence of Banks, customers who carry out transactions above USD5,000 must fill in a questionnaire regarding the legal origin of funds for deposits made for individuals; and, in case of any stockholder bearing more than 6% of shares of a financial institution, such individual must file a statement on the legal origin of resources used for such transaction. It should be mentioned that for transactions amounting USD10,000 or more within a 30-day period on behalf of the same customer, control mechanisms should be enabled. While the groups of companies under the controller of the Superintendence of Banks, Securities, and Insurance (detailed on A1.) are regulated by different policies and thresholds by type of activity.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Among the information and documentation requirements to identify customers are the following: a) name of the entity – individual; b) Ecuadorian sole commercial registry number (RUC as in Spanish); c) individual's profession or degree / entity economic activities; d) invoice number; e) address in Ecuador or in country of origin / residency; and f) e-mail and phone number.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Institutions of the financial sector should apply appropriate procedures to ensure that data supplied by customers is actual and accurate; otherwise, no commercial relationship may be entered to a report of suspicious operation should be submitted to UAF. Likewise, the Superintendence of Banks, Securities, and Insurance establishes required documentation related to customers and suppliers.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	A copy of annual tax return or income certificate is required from customers as a proof of their income source. In case of variations in their customers' income or property, these instances should be monitored by entities, on the basis of available data.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Minimum requirements established by the regulations should be fulfilled by entities. There is no reduced/simplified due diligence; local regulations set forth minimum KYC requirements for CDD.
Q13.	In what circumstances are enhanced customers due diligence measures required?
A13.	Due diligence and KYC procedures are mandatory on: a) individuals and members included in the UN sanctions list; b) PEP's (approval should be performed at Management level); c) electronics transfers (transferor's information); and d) non-cooperative counties/jurisdictions/territories and tax heavens (transactions back and forth must be reviewed and communicated to UAF).
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	When PEP's are involved, institutions of the financial sector should implement the following due diligence procedures: a) set forth risk management systems to establish whether or not a prospective customer, a customer or an ultimate beneficiary is a PEP; b) senior management approval is mandatory prior to initiating relationships with a PEP; c) appropriate measures should be implemented to establish the customer's income and funds source and ultimate beneficiaries of wealth if they have been identified as PEP's; and d) continuous due diligence measures and procedures should be implemented upon existing relationships with a PEP.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Institutions comprising the financial system should implement policies and carry out procedures to prevent or detect unusual and suspicious operations performed among domestic and/or international legal entities. A report of all international transactions must be filed at correspondent authorities upon necessary characteristic of the transactions.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	In accordance with Resolution No JB-2012-2146 no correspondent relationships may be entered into between local institutions and shell banks.

Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	Entities should set forth certain procedures to carry out KYC for non-face-to-face transactions, also these customers' transactions must be followed up/traced.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	UAF of Ecuador: http://www.uaf.gob.ec/

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Transactions performed within the financial system according to the amounts mentioned in A8 must be reported, as well as transactions considered suspicious and unusual.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Refer to A20.

Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Yes. An infraction arises from the lack of compliance on reporting in accordance with UAF requirements, and sanctions may be imposed on individuals and entities involved.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No. Entities are entitled to develop or use their own technological resources to keep up monitoring in accordance with KYC policies.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	In the case of a transaction is performed, involved entity must report the correspondent customer's data and operation.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No specific mention about this subject is included in AML regulation.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	The appropriate operation of the risk management system should be reviewed by the external auditor and its report should be submitted to the correspondent authority.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) The external auditor conducts an annual review; b) The results are submitted to the Board of Directors; and c) The final opinion is part of the financial statements audit.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	The assessment that risk management system meets all requirements established in the regulation is performed by the external auditor, who applies its judgment to design necessary tests to assure an entity's compliance with the regulation.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How it defined and what is are the additional protections?
A29.	a) according to the Constitution on Freedom Rights chapter, the right to the protection of personal data, which includes the access and decision on this type of data, as well as its correspondent protection. The gathering, filing, processing, distribution or publishing of this data or information will require the owner's authorization or a legal request; b) The Coding of the Superintendence of Banks on right to protection establishes in its Art.14 that the user will be entitled to receive protection and demand the adoption of effective measures to guarantee the security of financial operation, customer's advocate from the Superintendence of Banks and Insurance and other pertinent administrative or legal acts; and c) according to the Constitution Art 11. The right to maintain the reserve about his convictions. Nobody may be obliged to declare on them. In no case will it be required or used without the owner's or its actual representatives authorization, any personal or third party's data on their religious believes, political affiliation or opinion; or their health status and sexual life, unless for medical attention purposes.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	According to Art. 11 of the Constitution: In no case will it be required or used without the owner's or its actual representatives authorization, any personal or third party's data on their religious believes, political affiliation or opinion; or their health status and sexual life, unless for medical attention purposes.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Please refer to A30 above.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Please refer to A30 above.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Honduras

Key contact: Milton Rivera / Ramón Morales
 Email: milton.rivera@hn.pwc.com /
ramon.morales@hn.pwc.com
 Tel: (504) 2553-3060 / (504) 2553-3060

Postal address: Entrada Principal Col. Orquídea Blanca,
 14 Avenida Circunvalación
 Noroeste, 10 Calle, San Pedro Sula

Last updated:
 January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Anti-Money Laundering Law Decree 45-2002, 05 Mar 2002 (Abolished); Special Law on Abandonment of Automotive vehicles Decree 245-2002, 17 Jul 2002 (Abolished); Law on Anti-Terrorism financing Decree 241-2010, 18 Nov 2010 (In force); and Anti-Money Laundering Special Law Decree 144-2014, 30 Apr 2015 (In force).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	Specific AML regulations were in force in effect as you may see in previous answer.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	National Commission on Banking and Insurance (Comisión Nacional de Bancos y Seguros - CNBS) by means of Interagency Commission for the Prevention of Money Laundering and Terrorist Financing (Comisión Interinstitucional para la Prevención del Lavado de Activos y Financiamiento del Terrorismo – CIPLAFT).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The links "Educación Financiera" and "Prevención del Lavado de Activos", provide helpful guidance regarding AML (http://www.cnbs.gob.hn/).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	No, however individuals and entities must develop internal policies and procedures for risk-based due diligence.

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, link not available.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The requirements are: a) identify the client and verify identity by way of reliable documentation; b) identify the final beneficiary and entities, so that individuals and entities may understand companies structures; c) understand and obtain information about the commercial relationship; d) perform due diligence on the client; and e) if there is doubt about the ongoing commercial relationship between individuals and legal entities, they must verify in situ. When information provided by the client is doubtful or inconsistent with the compiled information, the individual and entity must end the business relationship and consider reporting it to the UIF.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	N/A

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	N/A

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	N/A

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customers due diligence measures required?
A13.	N/A

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	Regulations are applicable to the general population, there are no specific requirements for PEPs.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	There is no specific regulation.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	For example, telephone or internet banking transactions do not have a specific regulation, however the new AML Law Decree 144-2014, published on 30 Apr 2015, states the general due diligence requirements. Please see A9 for reference.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Financial Intelligence Unit (Unidad de Inteligencia Financiera – UIF), an anonymous virtual platform for individuals and entities. Yet to be launched.

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, SARs (Reporte de actividades sospechosas – ROS), when any suspicious or unusual activity is detected the Financial Intelligence Unit (Unidad de Inteligencia Financiera – UIF) must be notified.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No, but any suspicious or unusual activity regarding conditions, place, entity and / or transaction amount must be reported.

Q22.	Are there any penalties for noncompliance with reporting requirements e.g. tipping off?
A22.	Imprisonment or a penalty (approx. HNL8,8112 or USD3,950).

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	N/A

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Interagency Commission for the Prevention of Money Laundering and Terrorist Financing (Comisión Interinstitucional para la Prevención del Lavado de Activos y Financiamiento del Terrorismo – CIPLAFT) works in harmony with the resolutions or directions emitted by ONU and OEA, adopted by the Honduran government; however cases are managed within the local authorities.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of “personal data” cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of “sensitive data”? How it defined and what is are the additional protections?
A29.	No, however authorities are working on the draft law: a) N/A; b) N/A; and c) N/A.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	N/A

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	According to article 47 of Anti-Money Laundering Special Law, safeguarding fundamental rights of individuals and entities, banking, tax or professional secrecy cannot be invoked. However, certain information that has been required by an authority or received by the authority, cannot be shared by individuals and/or entities to any other individual or entity, especially if they're an interested party.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Jamaica

Key contact: Peta-Gaye Bartley
Email: peta-gaye.s.bartley@jm.pwc.com
Tel: +1 (0) 876 922 6230

Postal address: Scotiabank Centre,
Duke Street, P.O. Box 372,
Kingston, Jamaica

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Money Laundering Act 1996 which was subsequently repealed by The Proceeds of Crime Act 2007 which came into effect in May 2007, the Proceeds of Crime (Money Laundering Prevention) Regulations 2007, and the Proceeds of Crime Regulations 2007.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	2013 saw the passage of considerable amendments to existing money laundering legislation including the Financial Investigations Division (Amendment) Act which was passed in Jul 2013, the Proceeds of Crime (Amendment) Act 2013 which includes amendments to the Proceeds of Crime (Money Laundering) Regulations and the Terrorism Prevention (Amendment) Act 2013.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) Bank of Jamaica is responsible for supervising commercial banks, merchant banks, building societies and credit unions (www.boj.org.jm); b) Foreign exchange traders, bureaux de change and remittance companies are supervised by the Bank of Jamaica (www.boj.org.jm) and the Financial Services Commission is responsible for supervising firms and individuals in the securities and insurance industry: (www.fscjamaica.org); and c) The Minister of National Security has designated attorneys, accountants, real estate dealers, casinos and gaming lounges as designated non-financial businesses and professions ("DNFBPs") and therefore subject to the framework of supervision contained in section 91A of the Proceeds of Crime (Amendment) Act 2013. The changes will take effect for those categories from 01 Apr 2014 and for attorneys from 01 Jun 2014. Trust and company service providers and dealers in precious metals and stones have not been designated as DNFBPs.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The Bank of Jamaica published AML/CFT policy which was most recently revised in Sep 2010 and can be accessed here: (http://www.boj.org.jm/pdf/BOJ%20AML%20POLICY%20Final.pdf) and Guidance Notes on the Prevention and Detection of Money Laundering and Terrorist Financing Activities for commercial banks, merchant banks, building societies, credit unions, cambios, bureau de change and money transfer and remittance agents and agencies which was most recently revised in Mar 2009 and can be accessed here: (http://www.boj.org.jm/pdf/AMLCFT%20GN%20Mar%2009%20published.pdf) The Financial Services Commission provides guidance on AML (revised 20 Mar 2014): (http://www.fscjamaica.org/general-guidelines-and-bulletins/content-1221.html)
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Paragraph 46 of the Bank of Jamaica's AML/CFT Guidance Notes provides that where no comprehensive review has been conducted of existing client identification records since the coming into effect of the Money Laundering Act, Regulations and the Bank of Jamaica's Guidance Notes then the institution should immediately implement a retrospective review of all pre-existing accounts/customers to ensure that full KYC identification details are on file.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Paragraph 75 of the Bank of Jamaica's Guidance Notes encourages the adoption of a risk based approach to the obtaining of KYC information.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The last Caribbean FATF Mutual Evaluation Report on Jamaica was published in Oct 2005. It found Jamaica to be partially or non-compliant with 18 recommendations. The 11th Follow-Up Report on Jamaica was published on 03 Dec 2014 and can be accessed here (https://www.cfatf-gafic.org/index.php?option=com_docman&task=cat_view&gid=309&Itemid=417&lang=en). The 9th Follow Up-Report dated 03 Jan 2014 recommended that Jamaica be taken out of enhanced and placed in regular (expedited) follow up. The last Financial System Stability Assessment done by the IMF on Jamaica was in Apr 2012: https://www.cfatf-gafic.org/index.php?option=com_docman&task=cat_view&gid=309&Itemid=417&lang=en

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Article 8 of the Proceeds of Crime (Money Laundering Prevention) Regulations 2007 provides for de minimis amounts which do not require the application of client due diligence. In the case of transactions of a value of USD250 or less in either USD or any other currency, unless the nature of the transaction is suspicious. The exemption however does not apply to a money transfer and remittance agent or agency.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: True name and names used, correct permanent address including postal address (if different from permanent address), date and place of birth, nationality, contact numbers, date and place of birth, taxpayer registration number, at least two referees, and source of funds and wealth where considered appropriate. Identification should be verified from documents issued by reputable sources which includes a valid driver's licence bearing a photograph, current valid passport, current valid voter's identification card with a photograph, signed employer identity card bearing a photograph and signature or taxpayer registration number in addition to any one of the other identification documents listed. Legal persons: Entity's full name, description of the business conducted by the entity, country or jurisdiction of incorporation or establishment, taxpayer registration number, registered office or place of business, date on which the entity began to hold and ceased to hold the account, full name, date of birth, most recent and previous addresses of any person who is a signatory to the account. The following documentation should be obtained: Certificate of incorporation or registration, articles of incorporation or partnership deed, director's resolution authorising company's management to engage in transactions, financial institutions mandate, signed application form or an account opening authority containing specimen signatures, a financial statement of the business (audited except in the case of companies incorporated and in operation for less than 18 months), a description of the company's principal line of business and suppliers (if applicable) list of names, addresses and nationalities of principal owners, directors, beneficiaries and management officers including directors, beneficiaries and management officers including evidence of the identity of natural persons, Group/Corporate structure where applicable, tax compliance certificate and a copy of the licence to operate where the principal line of business is one that falls under a regulatory/supervisory body and determine and document the source of funds and wealth.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	The name and permanent address and employment details of a customer should be verified by an independent source, other than those provided by the customer, such as by requesting sight of a current utility bill for the customer's place of residence, checking a local telephone directory, checking the voters list, home visits, confirming the customer's place of employment independently, cross checking KYC details provided with other affiliated companies or other financial institutions.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	There is no specific information in local guidance which deals specifically with beneficial ownership. However, firms should carry out verification in respect of the parties operating the account. Where there are underlying principals, the true nature of the relationship between the principals and the account signatories must also be established. Appropriate enquiries should be performed on the principals, especially if the signatories are accustomed to acting on their instructions. In this context "principals" should be understood in its widest sense to include, for example, beneficial owners, settlers, controlling shareholders, directors, major beneficiaries etc.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Verification of the institution is not needed for five types of eligible institutions, including a licensed bank, a financial institution licensed under the Financial Institutions Act, a building society registered under the Building Societies Act, a society registered under the Co-operative Societies Act and an insurance company registered under the Insurance Act. Paragraph 50 of the Bank of Jamaica's Guidance Notes provides that KYC due diligence requirements for corporate customers can be satisfied if the corporate customer has established that it is listed on the Jamaica Stock Exchange's public listing of companies and is of good standing. The Credit Reporting Act 2010 came into effect 01 Oct 2010. It establishes the framework for credit reporting regime in Jamaica to ensure that this is done through reasonable procedures that meet the needs of commerce for credit information in a manner that is fair and equitable to the consumer. The Credit Reporting Regulations were approved by Parliament on 04 Jan 2011. Only entities licensed under the Act can offer credit bureau services and credit information can only be sourced and used from specific credit information providers.
Q13.	In what circumstances are enhanced customers due diligence measures required?
A13.	a) institutions offering private banking services for high net worth individuals must ensure that enhanced due diligence policies and procedures are developed and documented. Senior management should ensure that the personal circumstances, income sources and wealth of private banking clients are known and verified as far as possible and must provide approval for such relationships; b) where accounts are transferred from another financial institution, enhanced KYC standards should be applied especially if the licensee has any reason to believe that the account holder has been refused banking facilities by the other financial institutions; c) PEPs; d) non face-to-face customers; and e) correspondent banking.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Financial institutions are required to implement enhanced due diligence for business relationships involving foreign and domestic PEPs as follows: a) investigation and determination of the income sources prior to opening an account. Reference to income sources includes source of funds, source of wealth and asset holdings, confirmation of the general salary and entitlements for public positions; b) senior management approval of the decision to open an account for a PEP; c) ongoing monitoring of PEP accounts; and d) regular reviews to ensure KYC information remains up to date.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The following enhanced due diligence should be performed by correspondent banks: a) obtaining authenticated/certified copies of certificates of incorporation and articles of association; b) obtaining authenticated/certified copies of banking licenses or similar authorisation documents, as well as any additional licences in respect of foreign exchange; c) determining the supervisory authority which has oversight responsibility for the respondent bank; d) determining the ownership of the financial institution; e) obtaining details of the respondent bank's board and management composition; f) determining the location and major activities of the financial institution; g) obtaining details regarding the group structure within which the respondent bank operates, as well as any subsidiaries it may have; h) obtaining proof off its years of operation, along with access to its audited financial statements; i) information as to its external auditors; j) ascertaining whether the bank has established and implemented sound CDD, AML/CFT policies and strategies and appointed a Compliance Officer; k) ascertaining whether the respondent bank has been the subject or is currently the subject of any regulatory action or investigation; l) establishing the purpose of the account; m) documenting the respective responsibilities of each institution in the operation of the account; n) identifying any third party that may have access to the account; and o) ensuring senior management approval is obtained.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Financial institutions are encouraged to avoid the practice of opening new accounts for non face-to-face customers unless higher standards of scrutiny are applied. This requires more rigorous identification and verification standards including independent verification by a reputable third party.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The Financial Investigations Division. In Jamaica, such reports are referred to as suspicious transaction reports ("STRs"). See: http://www.mof.gov.jm/financial-investigations/units-sections.html

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, cash transactions over a certain threshold should be reported to the Financial Investigations Division. Article 3 of the Proceeds of Crime (Money Laundering Prevention) Regulations 2007 provides that the following cash transactions must be reported: a) a money transfer and remittance agent or agency of USD5,000 or more; b) cambios and bureau de change of USD8,000 or more; and c) any other financial institution USD15,000 or more. Transactions conducted by the Central Bank of Jamaica, a ministry, department or agency of government, a statutory body or authority, a company registered in which the Government or an agency of the government is in a position to influence the policy of the company, any embassy, high commission or consular office is exempt from the requirement. The duty to report extends beyond transactions being conducted with customers to transactions that another person has engaged in which may constitute money laundering. Section 101 of the Proceeds of Crime Act 2007 requires banks to make a report where cash, which includes negotiable instruments, exceeds USD10,000 or the equivalent amount in any currency being taken in or out of Jamaica. Paragraph 102 of the Bank of Jamaica's AML/CFT Guidance Notes indicates that STRs should be filed in cases where the suspicion is that funds are being diverted to avoid the payment of taxes or to otherwise deprive the government of revenues.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No, all suspicious transactions should be reported.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Section 94 of the Proceeds of Crime Act 2007 criminalises the failure to make the requisite disclosure within the stipulated timeframe of 15 days. Failure to file suspicious transaction reports with the designated authority will attract up to one year imprisonment jail or JMD1m (approx. USD8,000) (Resident Magistrate, RM Court). Failure to file a threshold transaction report attracts a fine of up to JMD400,000 (approx. USD3,000) (RM Court). In respect to tipping off a company can be fined up to JMD600,000 (approx. USD5,000) (RM Court). Section 97 of the Proceeds of Crime Act 2007 criminalises tipping off.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes, those making reports are required to adhere to the 'appropriate consent' procedure contained in section 91 and 99 of the Proceeds of Crime Act 2007.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of “personal data” cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of “sensitive data”? How it defined and what is are the additional protections?
A29.	Jamaica is in the process of amending its data protection laws.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	N/A, see A29.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	N/A, see A29.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	N/A, see A29.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Mexico

Key contacts: Martin Montealegre / Moisés Navarrete
Email: martin.montealegre@mx.pwc.com /
moises.navarrete@mx.pwc.com
Tel: +52 (55) 5263 5775 / +52 (55) 5263 6602

Postal address: Mariano Escobedo No. 573
Col. Rincón del Bosque
CP 11580, México D.F., México

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	In 2004 the Financial Intelligence Unit ("FIU") was established to prevent and combat Anti-money Laundering / Terrorist Financing ("AML/TF"). There are different laws that apply to the financial sector and the issue dates of each General Regulation (or General Provisions) vary: a) in 2004 – General Regulation for Retirement Fund Management and Investment Companies; b) in 2006 – General Regulation for Savings and Popular Credit Institutions; c) in 2009 – General Regulation for Commercial Banks and Foreign Exchange Houses; d) in 2010 – General Regulation for Brokerage Houses; e) in 2011 – General Regulation for Microfinance institutions (SOFOL – Limited Purpose Financial Societies and SOFOM – Multiple Purpose Financial Societies), General Deposit Warehouses, Financial Leasing Companies, and Financial Factoring Companies; f) in 2012 – General Regulation for Foreign Exchange Centers, Money Transmitters, Insurance and Surety Companies, and Credit Unions; and g) in 2012 - AML/TF law designated to non-Financial Sector Businesses and Professions. Most of these General Regulations undergo amendments over time.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	There are different standards for each type of financial institution. Some AML regulations became effective in the last two years, mainly to regulate the activity of the Societies for Saving and Loans, Investment Funds, Investment advisers and Entity of Saving and Popular Credits. The main change was the strengthening of KYC and the obligation of the annual audit.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	In Mexico, various organisations regulate AML controls, depending on the type of financial institution. The principal is Secretaría de Hacienda y Crédito Público ("SHCP", Secretary of Finance and Public Credit (http://www.hacienda.gob.mx/LASHCP/MarcoJuridico/InteligenciaFinanciera/Paginas/leyes_reglamento.aspx) and receives the report of all the financial institutions through the next regulators: Regulator 1: Comisión Nacional Bancaria y de Valores ("CNBV", National Banking and Securities Commission (http://www.cnbv.gob.mx/PrevencionDeLavadoDeDinero/Paginas/default.aspx) regulates: a) commercial banks; b) development banking institutions; c) Limited Purpose Financial Society ("SOFOL"); d) brokerage houses; e) societies managing mutual funds (Sociedades Operadoras de Sociedades de Inversión); f) distribution societies of mutual fund shares; g) financial lessor; h) financial factoring companies; i) general deposit warehouses; j) credit unions; k) societies for saving and loans; l) foreign exchange houses; m) Multiple Purpose Financial Society ("SOFOM"); n) entity of saving and popular credits; o) foreign exchange centers; and p) money transmitters. Regulator 2: Comisión Nacional de Seguros y Fianzas ("CNSF", National Insurance and Surety Institution (http://www.cnsf.gob.mx/Paginas/Home.aspx) regulates: a) insurance institutions; and b) surety institutions. Regulator 3: Comisión Nacional de Sistemas de Ahorro para el Retiro ("CONSAR", National Retirement Savings System Commission (http://www.consar.gob.mx/) regulates: a) retirement fund managers. Regulator 4: Servicio de Atención Tributaria ("SAT", Tax Customer Service (https://sppld.sat.gob.mx/pld/index.html) regulates Actividades vulnerables (Vulnerable Activities – regulation designated to non-Financial Businesses and Professions): a) contests, sweepstakes or gambling games; b) issuance and marketing of service cards, credit or prepaid cards and travellers checks; c) granting loans; d) buying and selling of precious metals and stones, jewellery, watches, and art; e) sale or lease of aircraft, marine or terrestrial vehicles; f) transfer or custody of money or securities; g) armour-plating services; h) professional service, in an independent manner, when preparing and performing on behalf of a third person any of the following operations; i) purchaser or seller of real estate; j) management of securities or assets; k) management of bank accounts, savings or assets; and l) constitution, de-merge, merge, operation and management of corporations: a. public notaries; b. forwarding agent; c. non Profit Organizations; and d. Leasing of real estate.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The SHCP, via the Official Journal of the Federation, publishes practical guidance to firms regarding AML requirements and best practices for AML prevention. The SHCP has a section of FAQs aimed at fomenting a culture of AML prevention in financial institutions as well as non-financial institutions: http://www.shcp.gob.mx/INTELIGENCIA_FINANCIERA/Paginas/Preguntas_Frecuentes.aspx Taking into account that the prevention of crime starts with educating and diffusing a culture of prevention, the CNBV created the present section with the purpose of educating the public in a practical way, about different aspects related to AML/CFT: http://www.cnbv.gob.mx/PrevencionDelLavadoDeDinero/Paginas/Cultura-PLDFT.aspx In collaboration with the Financial Crimes Enforcement Network ("Fincen"), the CNBV established a guide of best practices for credit institutions seeking to open accounts or contracts with credit institutions established abroad, including those involving operations with US dollars in cash: https://www.fincen.gov/pdf/CNBV_Best_Practices_Spanish.pdf
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	The financial sector has historically applied KYC policies, but under an internal controls approach rather than for the purpose of anti-money laundering prevention.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	There is no official risk approach model established by the authority, but the general provisions require the entity to integrate a model based on parameters which classifies their clients depending on the risk they represent, establishing at least two levels of risk: low and high risk customers.
Q7.	Has the country been the subject of a FATF (of FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Mexico was initially evaluated by the Grupo de Accion Financiera ("GAFI") in 2008 (http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Mexico%20ful.pdf), since then GAFI and Grupo de Accion Financiera de Sudamerica ("GAFISUD") have issued Interim follow up reports in 2009, 2010, 2011, 2012 and 2014, including: a) Mutual Evaluation Report of Mexico by GAFI: a. 2008; and b. in February 2014, the FATF recognized that Mexico had made significant progress in addressing the deficiencies identified in its 2008 mutual evaluation report and could be removed from the regular follow-up process. b) interim follow up reports by GAFI: a. October 2010; b. October 2011; and c. October 2012. c) monitoring reports by GAFISUD: a. June 2009; b. December 2009; c. June 2010; d. December 2010; e. June 2011; f. December 2011; and g. June 2012. d) IMF Assessment: a. November 2013.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Each of the different entities that are subject to AML general provisions as mentioned in A3 consider different transaction thresholds, depending on the type of products and services that they each provide.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Requirements for customer identification information may vary according to financial entities, but in general they include: Individuals: a) full name; b) gender; c) federal entity of birth; d) date of birth; e) country of birth; f) nationality; g) employment information; h) address; i) telephone number; j) e-mail; k) Code of Taxpayer Registration (“RFC”); and l) serial number of Advanced Electronic Signature. Corporations: a) corporate name; b) economic activity or social activity; c) nationality; d) Code of Taxpayer Registration (“RFC”); e) serial number of Advanced Electronic Signature; f) address; g) telephone number; h) e-mail; i) date of constitution; and j) full name of the person empowered to enter into contracts. Also copies of customer identification documents may vary according to financial entities, but in general they include: Individuals: a) personal identification; b) Proof of the Single Key Population Registration (Constancia de la Clave Única de Registro de Población, “CURP”), document attesting the assignment of the tax identification number and / or equivalent issued by competent authority and Advanced Electronic Signature; c) proof of address; d) signed declaration stating that the person acting for this purpose in the name and for its own account or on behalf of a third part; and e) Power of Attorney if the individual acts as a proxy for someone. Corporations: a) testimony or certified copy of a public document proving their legal existence; b) document attesting the assignment of the tax identification number and / or equivalent issued by competent authority and Advanced Electronic Signature c) proof of address; and d) testimony or certified the instrument containing the powers of the legal representative and the personal identification of each of those representatives.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Copies of identification documentation are provided at the initial stage of the commercial relationship at the time the client file is created. There is no legal requirement regarding the authentication of identification documents. However, for the verification of documents, the regulation states that the staff of the entity must ensure that copies of the documents obtained are legible and compare them against the original document. Also, some institutions are implementing measures authenticity, some of which include black lights and special training for the detection of false identification.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Requirements for the identification of the beneficiary may vary depending on the type of client and the institution that requires them, but in general they include: a) full name; b) date of birth; c) proof of address; d) same documents required by client; and e) if a document presents scraps or has been repaired the entity should ask for this other information: two bank references or commercial references that contain the aforementioned data.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	When the client is a company, department or entity regulated by the National Banking and Securities Commission and is considered as a low risk client.
Q13.	In what circumstances are enhanced-customer due diligence measures required?
A13.	Enhanced due diligence should be carried out when the customer is rated as a high risk. To determine the risk rating and whether they should be considered PEPs, each one of the entities must consider the background of the customer, their profession, activity or course of business, source and destination of the funds, customer residence and other circumstances determined by the institution.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	When the PEP has been rated as high risk or is foreign.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The regulation stipulates that for the provision of services to correspondent counterparts abroad, institutions must approve, at management level, the relationship that allows up such provision. They must obtain the following from its foreign counterparts: a) a certification by an independent auditor on anti lavada de dinero ("ALD", Anti-money laundering); and b) information that allows the institution to: a. know the business to which these counterparties are engaged; b. evaluate the controls at their disposal, on ALD; c. determine whether these counterparties are supervised by a competent authority in the field of ALD; and d. determine whether they have good reputation.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, according to AML General Provisions.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Depending on the value of the transaction, some institutions require additional information to support that transaction.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Reports are sent to the SHCP via the respective regulatory bodies of each entity (see A3).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 113,925 SARs (Source: UIF) GDP (in current prices): 2014 – USD1,294,689.7m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD11.4m of GDP.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	According to the regulation entities must submit the following reports : a) relevant transactions: cash transactions are made by a customer for more than the amount equivalent to USD10,000; b) unusual transactions: activities, conduct or behaviour of a customer who does not agree with history or activities known to the bank; and c) troubling internal operations: the activity, conduct or behaviour of any of the directors, officers, employees and agents of the entity that, by their nature, may contravene, violate or evade the application of the provisions of the regulation. Also, for some financial entities, there are thresholds for cash transactions, international fund transfers and US dollar transactions above which a suspicious activity report must be filed
Q21.	Are there any minimum thresholds below which transactions do not need to be reported?
A21.	In most financial entities, there are thresholds for relevant operations, cash transaction, international fund transfers, and USD transactions, below which a suspicious activity report does not need to be filed.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, according to AML General Provisions. There are different penalties depending on each case.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Entities must have automated systems which must have the following functions: a) maintain and update data to allow consultation of the records; b) generate, encode, encrypt and securely transmit to the secretary, through the commission, information on significant transactions reports, unusual operations, and international transfers; c) classify types of operations or financial products offered by entities to their customers or users; d) detect and monitor the operations performed by a client or by the same user from those indicated; e) run warning systems that contribute to the detection and monitoring of suspicious activity analysis; f) group on a consolidated basis of the different contracts to the same client; g) maintain historical records of possible worrisome internal operations and unusual operations; h) serve as a means for the agency staff so they can report to internal areas that they determine, in a safe, confidential and auditable way; i) maintain security schemes of information processed; and j) run an alert system on operations that intend to carry out with people linked to terrorism or its financing, or other illegal activities.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes, according to AML General Provisions.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes, according to AML General Provisions.
Q27.	If an external report on the bank's AML systems and controls is required: a) How frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) auditors need to submit an annual report; b) auditors need to submit the report to the National Banking and Securities Commission; and c) no.
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) yes, a sample of KYC files is required according to AML General Provisions; b) yes, a sample test of SAR reports is required according to AML General Provisions; and c) yes, an examination of the risk assessment is required according to AML General Provisions.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	a) yes; b) a notice of privacy is signed by the customer to let the corporation use their personal data; and c) yes, some data is considered sensitive personal data such as that which can reveal aspects such as the origin racial or ethnic, health present and future, genetic information, religious, philosophical and moral beliefs, union membership, political opinions, and sexual preference.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	There is no prohibition for data transfer as long as it is not specified in the notice of privacy.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	The Personal Data Protection Law is the only law that regulates the Personal data transfer; however other federal laws can impact to this law indirectly.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	The "Financial Institution Law" (under article 117th that regulates the bank secrecy) protects the following data: a) bank deposits; b) bank operations; c) bank services; and d) loans.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Paraguay

Key contact: Rubén Taboada / Gastón Scotover /
Soledad Aguero
Email: ruben.taboada@py.pwc.com /
gaston.scotover@py.pwc.com / soledad.aguero@py.pwc.com
Tel: +595 21 418 8000

Postal address: General Díaz Nro. 521
Edificio Internacional Faro – Piso 6,
Asunción

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1997 and 2011.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	Secretaría de Prevención de Lavado de Dinero ("SEPRELAD") (The Ministry for Anti Money Laundering): www.seprelad.gov.py/
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Resolution N° 349/2013 and N°411/2013.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last 3 years? If yes, please find a link to a relevant report (if publicly available).
A7.	During the year 2014, Paraguay received a visit from the International Monetary Fund ("IMF") (El Fondo Monetario Internacional ("FMI")) and the Inter-American Development Bank ("IDB") (Banco Interamericano de Desarrollo ("BID")) in order to evaluate the implementation of the Strategic Plan of SEPRELAD that was launched in 2013.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes. Due diligence procedures are not required on transactions below USD10,000.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The law and its procedures define minimum requirements to identify the following customers: Individuals: birth date; nationality; National Identification number (cédula de identidad) or passport number; Registro Unico de Contribuyente ("RUC") if applicable, which is the Taxpayers Identification Number; marital status and spouse's name (if applicable); home and business address; telephone number; profession; occupation; and commercial references. Legal entities: entity name; activity; Registro Unico de Contribuyente ("RUC"), which is the Taxpayers Identification Number; business address; telephone number; shareholders list; executives list; commercial references; and entity constitutive documents.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	According to law, financial institutions should always verify original identification documents. However, for legal entities, there are some documents that can be provided as copies, if those copies are certified by a notary public officer.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The following three situations require financial institutions to collect additional information about beneficial ownership: a) when the client informs the institution that the final beneficiary is another person or entity; b) when the financial institution has doubts about the final beneficiary; or c) when the customer engages in commercial, financial or industrial transactions in a location where they have no operations. No requirements are established around verification of this data.

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	No specific procedures or guidance exists for this situation, only that documents are not required for operations below USD10,000.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence arrangements are required for transactions above the USD10,000 threshold.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	There are specific requirements to classify the customer as high risk. Its operations must be approved by the highest authority of institutions to establish due diligence procedures to apply, including spouses, relatives and relatives up to fourth degree of consanguinity or second degree of affinity. Non-profit organisations are also included.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The correspondent must be approved by the highest authority of the institution; he/she must know the nature of the activities of the correspondent, and evaluate the policies and procedures to prevent money laundering and terrorist financing implemented by the correspondent. On account transfers through correspondents, have evidence that preventative measures have been implemented and due diligence procedures performed on transfers.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	No.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	The entity must develop policies and procedures relating to prevention to avoid the use of technological devices to perform operations related to Money Laundering and Terrorist Financing (“ML/TF”), as well as keeping up to date computer platforms.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The Secretaría de Prevención de Lavado de Dinero (“SEPRELAD”) (The Ministry for Anti-Money Laundering): www.seprelad.gov.py

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Institutions must also report suspicious transactions, fund transfer operations to and from other countries (transfers, exchanges, cash, cheques or any other payment method), as well as physical remittance of money.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Yes. Anything below USD10,000.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Yes.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes. Resolution N° 349/2013.
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) once a year; b) SEPRELAD and the Central Bank of Paraguay; and c) no.
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	The test involves checking the process followed by the bank regarding how it complies with the regulations, based on Know Your Customer/Client requirements. It is equivalent to the process performed in Uruguay.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, Law N° 1682/01. a) the law does not forbid the sharing of information for AML purposes, however the customer must give authorisation for the financial institution to report personal information; b) as per a) above; and c) no.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Refer to A29.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Refer to A29.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. Law N° 861/96, for Banks, Financial Institutions, and other Governmental Entities.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Peru

Key contact: Nancy Yong / Guillermo Zapata
Email: nancy.yong@pe.pwc.com / guillermo.zapata@pe.pwc.com
Tel: +(511) 211 6500 Ext. 2029 / +(511) 211 6500 Ext. 8043

Postal address: Av. Santo Toribio 143,
Piso 2, San Isidro, Lima 27,
Perú

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	AML legislation was included in the Peruvian Criminal Code, article 293 B, by Legislative Decree 736 in 1991. However, in 2002 the following regulations became effective: a) The Law 27765, Anti-Money Laundering Criminal Law, which replaced the AML regulation on Peruvian Criminal Law. This law was not enforced until Apr 2012; and b) The Law 27693, Law that creates the Peruvian Financial Intelligence Unit (AML supervisor, its acronym in Spanish is 'UIF-Peru'). This law has subsequently been modified by Law 28009 and 28306. The Supreme Decree 163-2002-EF, Rules of the UIF-Peru, which was modified by Supreme Decree 018-2006-JUS in 2006. In 2008, Peru issued SBS Resolution 838-2008 which established complementary regulation to entities under the scope of the Superintendencia de Banca y Seguros ("SBS"). Note that in Apr 2012, Peru enforced the Legislative Decree 1106, Law against Money Laundering, Illegal Mining and Organized Crime. In the same way, on Oct 2014, Peru enforced the SBS Resolution 6729-2014 that expands the list of the parties legally bound to report to the UIF-Peru. adding: a) individual or legal entities engaged in sale or rental of machinery and equipment; b) legal entities that distribute, transport, and / or sell chemical inputs that can be used in illegal mining; and c) laboratories and companies that produce and / or sell chemical inputs and have their assets audited. In 2015 Peru enforced SBS Resolution N° 2660-2015 which repeals SBS Resolution 838-2008. This new Resolution implements the integral risk management system (under COSO methodology) for enterprises under the supervision of the SBS. Please note that this Resolution is applicable to all banking and financial institutions under the scope of the SBS. Note: We are quoting Peru's most relevant anti-money laundering legislation.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The previous AML regime only considered a Money Laundering Crime where the money was obtained by drug trafficking, terrorism, abduction or human trafficking.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	All banking and financial services are supervised by the Superintendencia de Banca y Seguros. The UIF is in charge of supervising the non-financial sector. Please note that depending on the particular sector of a company, a ministry might be in charge of supervising its activities. The link of the regulator is the following one: http://www.sbs.gob.pe/
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	SBS Training: http://www.sbs.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=2&JER=464
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Legislative Decree 1106 includes additional control mechanisms related to criminal law. The requirement is to verify the identity of customers who are regulated on Supreme Decree 018-2006-JUS. Before the new AML regime was introduced, SBS Resolution 838-2008 established a series of requirements that entities subject to supervision by the SBS should fulfil upon identifying a customer, being the customer a natural person or a legal entity. The Resolution also established a series of private and public documents that were to be requested before the establishment of a commercial relationship. The requested documentation was to be kept up to date. Similar measures were imposed to companies outside the financial and banking system. For more information, please visit: http://www.sbs.gob.pe/repositorioaps/0/2/jer/nac1_seguntiponormasnaciresoluciones/resoluciones/Resoluci%C3%B3n%20SBS%20N%C2%BA%20838-2008.pdf
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. As stated in A1, SBS Resolution N° 2660-2015, Rulebook for asset laundering and terrorism financing risk management was issued by the SBS. The aforementioned Rulebook establishes a series of procedures to identify, prevent, evaluate and manage risks related to asset laundering and terrorism financing in business subject to supervision by the local authorities. This Rulebook stipulates that supervised entities should have specific manuals, offer training and implement procedures related to risk management of asset laundering and terrorism financing.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Last Mutual Report FATF/GAFI was executed in Jul 2005: http://www.fatf-gafi.org/countries/n-r/peru/

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	SBS Resolution N° 2660-2015 states that supervised entities within the scope of the SBS shall register the following operations: a) customers' operations worth at least USD10,000 and above (or its equivalent in PEN); b) fund transfers worth at least USD2,500 and above (or its equivalent in PEN). Transfers linked to private pension funds do not need to be reported; c) customers' operations in not-authorized credit and savings cooperatives worth at least USD5,000 and above (or its equivalent in PEN); d) in case of insurance policy: i) Life insurance with an annual premium worth USD1,000 and above (or its equivalent in PEN); life insurance single with a single premium worth USD2,500 and above (or its equivalent in PEN), ii) Other kind of insurance with and annual premium worth USD10,000 (or its equivalent in PEN) and above; and e) credit warrants worth USD2,500 and above (or its equivalent in PEN). Foreign currency exchange worth USD5,000 and above (or its equivalent in PEN). SBS Resolution N° 486-2008 states that supervised entities that are not subject to supervision by a public body should keep a registry of customers who make single transactions worth USD10,000 or more and those who make multiple transactions worth USD50,000 or more within a month. This Resolution is applicable to all entities outside the scope of the SBS. The most relevant regulation for financial and non-financial services are the following. For more information visit: http://www.sbs.gob.pe/
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Complete name and surname, birth date, identification document, profession or occupation and domicile. Legal entities: Name, taxpayer registration number, purpose and legal representative information (complete name and surname, birth date, identification document, profession or occupation and domicile). SBS Resolution N° 2660-2015 states that supervised companies should request and record the following information from their individual customers: a) first and middle names, surname and mother's maiden name; b) identification document number and type; c) nationality and residence; d) address; e) phone number and email address; f) purpose of the relationship to be established with the enterprise; g) occupation or profession and workplace; h) in case of a politically exposed person (PEP), name of the institution, public body or international organization and post; and i) identity of legal representatives and holders of power of attorney. The information should include that requested in the previous points. An identification document is also required. The aforementioned Resolution states that supervised companies should request and record the following information from their institutional customers: a) name; b) taxpayer number; c) corporate objective; d) identity of shareholders and associates who own more than 25 percent of the company's capital, providing all the information requested from customers who are legal entities; e) purpose of the relationship to be established with the enterprise; f) legal persons linked to the customer and to its economical group; and g) main office address and phone number.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	According to article 30.5 of SBS Resolution 2660-2015, supervised companies must execute information verification procedures, such as home inspections, personal interviews, and internal procedures approved by supervised companies. The verification should state the location, date and procedures employed by the company. This verification should be registered in the natural person or legal entity's personal file. Note: Non-financial or banking institutions have similar verification duties imposed by legislation.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	They are the same high level requirements mentioned in A10.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	SBS Resolution N° 2660-2015 establishes that companies will be allowed to employ reduced due diligence arrangements when its LA/FT risk level allows it in accordance to the Superintendence's regulations. Minimal information to be obtained from natural person customers is as follows: a) first and middle names, surname and mother's maiden name; b) identification document number and type; and c) address. The following information should be required from legal entities: a) name; b) taxpayer number; c) identity of legal representatives (whole names and surnames); and d) main office address and phone number. In order to identify a customer, an identification document should be provided in case of natural persons. Legal entities will provide public documentation that confirms their existence and contain their names, having to provide at least their constitutive documents. Note: For non-financial or banking institutions the due diligence arrangements are not as detailed as those mentioned above. Regulation let's each company establish its own verification methods.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customers due diligence measures required?
A13.	SBS Resolution N° 2660-2015 establishes that companies will have to employ enhanced due diligence procedures to identify their customers when the following conditions apply to a customer: a) non-resident nationals or foreigners; b) legal entities from overseas; c) trust funds; d) non-profit organizations. A non-profit organization is that which collect and use funds with charitable, religious, cultural, educational, social or fraternal purposes; e) politically exposed people ("PEP"). Companies should reinforce their customer identification procedures when one of their customers becomes a PEP after commercial relations have been established; f) people identified as: a. PEP relatives up to the second degree of consanguinity and second degree of affinity; and b. PEP's spouse or partner. g) legal entity in which a PEP owns 25 percent or more of its shares; h) associates, shareholders or similar and managers of a legal entity in which a PEP owns 25 percent or more of its shares; i) natural persons or legal entities who receive money transfers from countries that do not cooperate with the International Financial Action Group – GAFI, countries with risks related to LA/FT, countries with minimal banking supervision or countries subject to sanctions from the Office of Foreign Assets Control – OFAC; j) natural persons or legal entities under investigation by competent authorities for asset laundering, previous offenses and/or terrorism financing; k) those linked to natural persons or legal entities under investigation or on trial for asset laundering, previous offenses and/or terrorism financing l) dedicated to correspondence services with foreign companies constituted in countries with minimal or no taxation in accordance to the tax office's dispositions, or countries with no banking regulation or supervision; and m) other cases identified by companies. Note: For non-financial or banking institutions the regulation and due diligence arrangements are not as detailed as those mentioned before. The regulation lets each company establish its own verification methods.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	SBS Resolution N° 2660-2015 states that being a PEP is reason enough to require special information from them. It should be requested from PEPs the names of their relatives up to the second degree of consanguinity and second degree of affinity and it should be requested the legal entities' names in which they own 25 percent or more of its shares or capital. Note: For non-financial or banking institutions the regulation the due diligence arrangements are not as detailed as those mentioned before. The regulation let's each company establish its own verification methods.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	SBS Resolution 2660-2015 does not enforce enhanced due diligence upon relationships with cross-border banking and similar operations. However, it requires banks from overseas to comply with Peruvian LA/FT regulation, granting them a thirty day period starting the day legislation was issued in the country where the bank was constituted to issue a report to the Superintendence regarding: a) existing limitations; and b) measures to adopt to manage LA/FT-related risks.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	See A15. There are no prohibitions or restrictions to relationships with shell banks.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	There are no additional due diligence requirements for non face-to-face transactions and/or relationships. All transactions are subject to the same controls and assessments regardless of their nature.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	UIF-Peru of the SBS: http://www.sbs.gob.pe

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: Jan to Sept of 2015 - 5,024 SARs (Source: http://www.sbs.gob.pe/repositorioaps/0/2/er/esta_transparenciaoperativa/20151029_BolEst_Septiembre2015.pdf) Comparative GDP data is not available for this specific period.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Article 9 of Law 27693 stipulates the operations to be reported according to the amounts mentioned in A8. Moreover, article 11 of Law 27693, defines unusual and suspicious transactions.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Yes. Please refer to A8 for a complete list of thresholds to be taken into account when evaluating financial transactions. Nevertheless, in case the transaction is assessed as a suspicious or unusual one by the company's Compliance Officer, it must be reported regardless of the transaction's worth.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Penalties for not complying with Law 29038 requirements are detailed on SBS Resolution 8930-2012, SBS Resolution 7314-2013 and SBS Resolution 5389-2013

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Article 1 of SBS Resolution 9810-2011, stipulates that regulated entities are requested to use automated Suspicious Transaction Monitoring Technology (its acronym in Spanish is "ROSEL") to report suspicious transactions.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	There are no limitations related to this aspect. Once the transaction is executed, the supervised entity must report the operation and the customers' information.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	There is no local regulation related to this matter. However, due to several international agreements, the UIF can share information with its foreign counterparts.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	According to SBS Resolution 17026 -2010, article 9 and 12, the external report on the bank's AML must comply with the following: a) the auditors shall submit the conclusions of report on the bank's AML systems directly to the SBS, it may request a copy of the report from the audit firm or the Bank; and b) the report shall be made by a different auditing firm or a completely different team from that issued the opinion on the fairness of the financial statements.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) a report should be issued on a yearly basis, as it is mentioned in article 24 of SBS Resolution N° 17026 -2010; b) the report is submitted to the bank and the conclusions of the report are presented to the SBS, as it is required by article 9 of SBS Resolution N° 17026 -2010; and c) no, please see A26.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) yes. Article 25 (c) and (d) of SBS Resolution N° 17026 -2010; b) yes. Article 25 (e) and (f) of SBS Resolution N° 17026 -2010; and c) there is no local regulation related to this matter.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of “personal data” cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of “sensitive data”? How is it defined and what are the additional protections?
A29.	a) yes. In order to perform such evaluation, it is necessary to make use of personal data which is regulated by Law 29733, Personal Data Protection Law; b) personal Data Protection Law applies only to personal information of individuals. Corporate data is regulated according to stock market legislation for listed companies. In that sense corporate data is classified information. Besides there is regulation regarding intellectual property (patents, trademarks and others) that protect corporate data; and c) according to Article 3 of Law 29733, Personal Data Protection Law, “sensitive data” has a separate definition to “personal data”. Sensitive data is defined as personal data consisting of biometric data, data concerning racial and ethnic origin; political, religious, philosophical or moral opinions or convictions, personal habits, union membership, and information related to health or sexual life. Article 2 of Law 29733. In order to obtain sensitive data from individuals, their consent must be obtained through written means which guarantees an unequivocal consent. Sensitive data require higher security measures such as data encryption, special storage, limited access for authorized users of the companies and secure destruction such as the use of paper shredders.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	In general, according to Law 29733 (Art.3) and its Regulation (Art.19), there is no prohibition for the transfer of personal data. To transfer data into or out of the country requires the individual's consent and the non-binding opinion of the local authority of Personal Data Protection.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	The following is the legislation related to information transfer: a) Political Constitution of Peru 1993, article 2. 6; b) Personal Data Protection Act, Law 29733; c) Rules of Personal Data Protection Act, Supreme Decree 003-2013-JUS; and d) Law of Transparency and Access to Public Information, Law 27806. These legal regulations don't establish any barriers to information transfer.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	The General Law of the Financial and Insurance Systems and Organic Law, Ley 26702, article 140, which regulates banking secrecy, forbids financial companies and their directors and employees to provide any information on debit transactions with their customers. Also, Peruvian law requires other data referred to confidential information, such as: a) Reserve Tax. Article 85 of the Peruvian Tax Code, Supreme Decree 133-2013-EF; and b) Market Reserve. Article 45 of the Peruvian Securities Market Act, Supreme Decree 093-2002-EF. Please be advised that every professional association such as that of lawyers, engineers and doctors establish within their code of conduct a requirement of confidentiality regarding the services executed by the members of each association.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Uruguay

Key contact: Dannys Correa
Email: dannys.correa@uy.pwc.com
Tel: +598 29160463 ext. 1377/1373

Postal address: Cerrito 461, 2nd Floor,
Montevideo 11000,
Uruguay

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	a) 2009 – Law No. 18.494 – introduced several modifications to Law 17.835; b) 2004 – Law No. 17.835 – system controls and prevention of money laundering and financing of terrorism; and c) 1998 – Law No. 17.016 – standards with regard to the misuse of public power (corruption). Previously, Uruguayan AML Laws focused on the illicit traffic of narcotic drugs but have been gradually extended to other crimes.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	Uruguayan Central Bank ("UCB"): http://www.bcu.gub.uy/ Internal Audit of the Nation: http://www.ain.gub.uy/
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, the Unit of Financial Information and Analysis ("UIAF") of the UCB has issued guidance with regard to suspicious or unusual transactions in order to assist the parties required to report these transactions in the detection of unusual or suspicious patterns in customer behaviour. Although the published guidelines are not exhaustive, they constitute a collection of types or patterns of transactions that could be linked to money laundering operations from criminal activities or terrorist financing: http://www.bcu.gub.uy/
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, the UCB, supervisor of the financial system, established the requirement to periodically update information on existing clients, especially in the case of high risk customers.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, the UCB has established that the supervision process must be proactive and integrity orientated, focused on risks and performed on a consolidated basis. The Corporate Governance and Internal Control System Regulations which are in force (UCB Circular 1987) establish that institutions must have a risk framework according to the nature, size and complexity of their transactions. An AML framework is specifically required.

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The country has not been subject to review in the last three years. The UIAF participate in Grupo de Acción Financiera de Sudamérica (“GAFISUD”) and in the Egmont Group.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, customer due diligence is not required on transactions below USD3,000 with occasional customers.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The institutions must identify their customers in compliance with the UCB requirements when they open accounts or when they process transactions, with the exception of transactions with occasional customers below USD3,000. The UCB regulations establish the minimum identification requirements for individuals and legal entities. Individuals: a) name and surname; b) date and place of birth; c) identification document; d) marital status; e) address and telephone number; f) main activity or occupation; and g) volume of income (salary and other earnings). It should be ascertained whether the customer is acting on their own or on behalf of a third party. In the latter case, the ultimate beneficiary should be identified. The same information should be obtained on all owners, agents, representatives and those authorised to operate on behalf of individual clients. It should be ascertained whether the information on level of incomes of these customers constitutes the source of income of the account. Legal Entities: a) company name; b) established date; c) address and telephone number; d) tax identification number; e) bylaws and other information on the entity as registry number etc.; f) main activity; g) volume of income (on financial statements); and h) shareholders and ultimate beneficial owners. The above mentioned data required for individuals must be obtained for those listed as corporate managers and representatives, agents and those authorised to act on the company's behalf. It should be ascertained whether the information on level of incomes of these customers constitutes the source of income of the account.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Notary certification and signature verification are required to certify the validity of the documents provided. Each institution also has its own policies and procedures to verify the documents and its copies.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Financial institutions must implement procedures in order to identify the ultimate beneficial owner of each transaction, verify their identity and register their names.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced/simplified due diligence arrangements are available to 'occasional customers'. The UCB regulation defines 'occasional customers' as those who do not demand transactions on a permanent basis and whose total amount of transactions with the institution is less than USD30,000 on an annual basis.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence measures are required for 'permanent customers'. Institutions must analyse each customer and classify them according to their activity, residence and risk profile. Institutions must obtain, evaluate and register additional information about the financial situation, in order to justify the customer's transactions and the origin of funds for those customers classified as high risk and those with transactions over a certain limit.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Financial institutions should apply additional due diligence procedures in the case of PEPs, their relatives and their associates. Financial institutions should: a) rely on procedures that allow them to determine whether a client is a PEP; b) get senior management approval upon establishing a new relationship with this type of client; c) take reasonable measures in order to determine the origin of the funds; and d) carry out a special and permanent assessment of the customer's transactions.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	For correspondent banking relationships, local institutions must obtain the following information in relation to foreign institutions: a) the nature of their business; b) management details; c) reputation; d) principal activities and location of the premises; e) account purpose; f) regulation and supervision in their country; g) political context; and h) procedures applied in order to prevent being used for laundering of assets or financing of terrorism.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, it is not permitted to perform any type of business with financial institutions established in jurisdictions that do not require physical presence. It is also not permitted to establish a relationship with foreign institutions which allow shell banks to open accounts.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Financial institutions must implement special procedures to verify the relevant identity and to control non face-to-face transactions such as non-resident or e-banking transactions.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Reports are made to the UIAF, which was established by Resolution of the Board of Uruguayan Central Bank: http://www.bcu.gub.uy/
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 – 275 SARs (Uruguayan Central Bank) GDP (in current prices): 2013 – USD55,700m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD202,59m of GDP
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	By the above mentioned Circular No. 1722 of UCB dated 21 Dec 2000, transactions considered suspicious can be conducted on a periodic basis or isolated, and that according to the customs of the activity concerned, are unusual, with no apparent economic or legal justification, or of unusual or unjustified complexity. Subjects required to report must immediately inform the UIAF regarding transactions covered by this where there is evidence or suspicion of involvement in the legitimisation of assets derived from criminal activities. In addition, financial intermediation institutions must notify the UCB and provide information regarding physical or legal persons carrying out the following transactions: - operations consisting of coins, currency conversion, foreign cheques, precious metals, bank deposits, shares or other securities which are easy to redeem, for amounts in excess of USD10,000 or its equivalent in other currencies; - receiving and sending of money orders and transfers (including international transfers) for amounts in excess of USD1,000 or its equivalent in other currencies, regardless of the mode of operation used for execution. Transfers and money orders are exempted from the obligation to be reported if they are made between bank accounts in cases where both the account of origin and destination are based in local financial intermediaries; and - purchase or sale, exchange or arbitration of foreign currency or precious metals for an amount over USD10,000 or its equivalent in other currencies, where the counterpart is made in cash.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	See A20 above.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, fines and penalties from Uruguayan Central Bank and National Internal Audit Office.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Yes.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	After a certain time, if there is no response from UCB regarding the reported transaction, the institution should consider if it is appropriate to proceed with the transaction with the customer.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	The Communication 2010/254 issued by the CBU on 21 Dec 2010 defined that banks must have an audit report referring to the consideration of reasonable assurance regarding the design and operations of policies, procedures and monitoring mechanisms adopted to prevent the bank from being used for money laundering and terrorist financing.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) annually; b) directors and shareholders of the Bank; and c) no.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) yes; b) yes; and c) yes. The procedures to be performed include: a) inquiry corroborating the description of policies, procedures and control mechanisms established by the Bank; and b) verification that the policies, procedures and control mechanisms are in accordance with the provisions of the regulation and its effective implementation by the auditor's judgment samples.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	In Uruguay there is a specific data protection Law (No. 18331). The definition of "personal data" is included in it. The Law is applicable to corporate data as well. The country has a separate definition of "sensitive data", defined as: the data and personal information referring to origin, ethnic, politic, religion, health and sexual life and preference.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	The response is affirmative; there are credit reports, banking information, and criminal information (only local Authorities and Interpol) that are prohibited from being transferred. Medical information is protected by secrecy.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes, the international transfer of data is regulated by Law and limited upon requirements (e.g. consent, adequate protection, International law regulation, etc.) and it is controlled by the public authorities.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	In Uruguay there are secrecy regulation laws, such as banking secrecy, professional secrecy, court data, and other specific regulations.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

United States of America

Key contact: Jeff Lavine
Email: jeff.lavine@pwc.com
Tel: +1 (703) 918-1379

Postal address: 1800 Tysons Boulevard McLean,
VA 22102-4261,
USA

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	In 1970 the United States Congress passed the Currency and Foreign Transactions Reporting Act, commonly known as the Bank Secrecy Act ("BSA"). The BSA established specific requirements for record keeping and reporting by private individuals, banks and other financial institutions. Since the passing of the BSA, several other laws have enhanced and amended the BSA to provide additional tools to combat money laundering. The key laws are: a) Money Laundering Control Act (1986); b) Anti-Drug Abuse Act of 1988; c) Annunzio-Wylie Anti-Money Laundering Act (1992); d) Money Laundering Suppression Act (1994); e) Money Laundering and Financial Crimes Strategy Act (1998); f) Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act); g) Intelligence Reform & Terrorism Prevention Act of 2004; h) Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 ("CISADA"); and i) Iran Threat Reduction and Syria Human Rights Act of 2012. The USA PATRIOT Act of 2001 is the most significant of the enhancements and amendments to the BSA. Section 312 of the USA PATRIOT Act (formerly known as special due diligence for correspondent accounts and private banking accounts) in particular, requires US financial institutions to obtain beneficial ownership/enhanced due diligence ("EDD") information in certain situations as delineated under §312 for US correspondent accounts held by certain foreign financial institutions, and private banking accounts held by foreign persons (including politically exposed persons).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The BSA laws and regulations have not changed dramatically within the past two years. Recently, however there has been a change related to sanctions. The Joint Comprehensive Plan of Action ("JCPOA"), an international agreement, is arguably the most recent significant event to impact the US sanctions environment. It should be noted, however, that the economic landscape for US companies and their foreign subsidiaries or affiliates will experience little to no change as a result of the JCPOA terms. The vast majority of US sanction relief provided by the JCPOA is only applicable to non-US companies and financial institutions, and specified foreign governments. Sanctions relief provided by the JCPOA will only target specified key industries / areas. Additionally on 25 Aug 2015 the Financial Crimes Enforcement Network ("FinCEN") published a notice of proposed rulemaking ("NPRM") to impose AML programs and additional reporting requirements on investment advisers registered with the US Securities and Exchange Commission ("SEC"). If adopted, the proposal would require registered investment advisers to: a) develop and maintain written AML programs reasonably designed to prevent money laundering and terrorist financing and to achieve compliance with the BSA; b) include registered investment advisers within the meaning of "financial institutions" for purposes of the BSA's implementing regulations and impose specific reporting requirements; c) require that registered Investment Advisers monitor for suspicious activity and file SARs with FinCEN; and d) delegate examination authority for compliance to the SEC (http://www.gpo.gov/fdsys/pkg/FR-2015-09-01/pdf/2015-21318.pdf).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q3.	Who is the regulator for AML controls for: (a) banking; (b) other financial Services; (c) non financial sector (e.g. casinos, high value goods etc.)? Please include link to the regulator(s) website.
A3.	Authority to assess penalties for violations of US AML rules and regulations rests with the Secretary of the Treasury, primarily delegated to the FinCEN: (http://www.fincen.gov). Further reliance is placed on US Federal Regulators and Self-Regulatory Organizations ("SROs"), largely used in the US securities industry. Additionally, the Department of Justice ("DoJ") can bring criminal, civil and forfeiture actions: (http://www.justice.gov). Lastly, individual states can choose to have their own regulatory bodies with jurisdiction to enforce state banking laws and levy civil penalties (e.g., New York Department of Financial Services ("NYDFS"): (http://www.dfs.ny.gov)) a) banking: depending upon the type of banking charter an institution has, and its membership in the Federal Reserve System, a bank's federal regulator will be one of the following: a. Board of Governors of the Federal Reserve System ("FRB") (http://www.federalreserve.gov); b. Office of the Comptroller of the Currency ("OCC") (http://www.occ.gov); and c. Federal Deposit Insurance Corporation ("FDIC") (http://www.fdic.gov) b) other financial services: a. credit unions: National Credit Union Administration ("NCUA") (http://www.ncua.gov/Pages/default.aspx); b. broker dealers: US Securities and Exchange Commission ("SEC") (http://www.sec.gov); Financial Industry Regulatory Authority ("FINRA") (http://www.finra.org); and New York Stock Exchange ("NYSE"), which is a SRO for exchange members (http://www.nyse.com); c. registered mutual funds: SEC (http://www.sec.gov); d. commodity and futures firms: US Commodities Futures Trading Commission ("CFTC") (http://www.cftc.gov/index.htm) and the National Futures Association ("NFA") (http://www.nfa.futures.org); e. Money Services Businesses ("MSB"): FinCEN (http://www.fincen.gov) and the Internal Revenue Service ("IRS") (http://www.irs.gov); f. insurance companies: FinCEN and IRS; g. non-bank residential mortgage lenders and originators as loan or finance companies: IRS (http://www.irs.gov); and h. consumer protection for financial products and services: Consumer Financial Protection Bureau ("CFPB") (http://www.consumerfinance.gov) c) non-financial sector: FinCEN and/or IRS also cover the following sectors: casinos; mortgage companies and brokers; and precious metals/jewellery.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	a) banking: Federal Financial Institutions Examination Council ("FFIEC") (http://www.ffiec.gov/bsa_aml_infobase/default.htm); FRB's Supervision and Regulation Letters ("SR Letters"): (http://www.federalreserve.gov/bankinforeg/srletters/srletters.htm); and the FFIEC's information technology examination handbook (IT handbook) (http://ithandbook.ffiec.gov/it-booklets.aspx) (note: The FFIEC manual was updated on 17 Nov 2014 for the first time since 2010 – which indicates that 2015 regulatory exams in the US will follow the updated BSA/AML requirements delineated in the new FFIEC guidance manual); b) MSBs: FinCEN's BSA/AML Examination Manual for Money Services Businesses (http://www.fincen.gov/news_room/rp/files/MSB_Exam_Manual.pdf); c) broker dealers: SEC's AML source tool for broker-dealers (http://www.sec.gov/about/offices/ocie/amlsourcetool.htm) and http://www.finra.org/Industry/Issues/AML); d) registered mutual funds: SEC's AML source tool for mutual funds (http://www.sec.gov/about/offices/ocie/amlmsourcetool.htm); and e) commodity and futures firms (http://www.cftc.gov/IndustryOversight/AntiMoneyLaundering/index.htm) and (http://www.nfa.futures.org/NFA-compliance/NFA-futures-commission-merchants/anti-money-laundering.HTML).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Section 326 of the USA Patriot Act requires banks, savings associations, credit unions and certain non-federally regulated banks ("banks") to have a Customer Identification Program ("CIP"). Broker-dealers in securities are subject to similar regulations. In January 2004, FinCEN published Guidance on the CIP regulations that clarify that the CIP rule applies for customers that establish new accounts after 1 Oct 2003 and do not apply retrospectively unless the bank establishing a new relationship does not have a reasonable belief that it knows the true identity of the customer: http://www.fincen.gov/statutes_regs/guidance/pdf/finalciprule.pdf

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. A risk based approach to AML is expected by U.S. regulators. BSA/AML U.S. regulatory guidance is provided in the FFIEC BSA/AML Examination Manual (December 2014): http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014.pdf
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	FATF announced the start of the 4th round of peer reviews / mutual evaluations of each member country's AML / CTF regime to determine compliance with FATF Recommendations (2012) and the methodology for assessing compliance with the FATF Recommendations and the Effectiveness of AML / CFT Systems (2013). The 4th Round of Mutual Evaluations for the US is tentatively scheduled to take place in February / March 2016 with possible plenary discussions in October 2016: http://www.fatf-gafi.org/countries/u-z/unitedstates and http://www.fatf-gafi.org/media/fatf/documents/assessments/Global-assessment-calendar.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No. Basic CIP information and customer due diligence ("CDD") is required for all accounts / customers regardless of activity level or transaction amounts. Specific CDD and EDD requirements can vary based on an institution's unique risks and internal policy requirements.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Section 326 of the USA PATRIOT Act requires any financial institution engaged in financial activities to establish a written, board approved CIP to collect and verify identifying information about each prospective customer. The CIP must include risk-based procedures to verify the identity of each prospective customer to the extent reasonable and practicable. The information must be sufficient to enable the institution to form a reasonable belief that it knows the true identity of each customer. At a minimum, the following must be obtained and verified: Individuals: a) name; b) date of birth; c) residential or business address (an army or fleet post office box number or residential address of next of kin may be substituted); and d) identification number (can be determined by the institution, but should typically be a Taxpayer Identification Number ("TIN") for both individuals and entities (e.g., social security number or employer identification number). Entities (non-individual): a) name; b) principal place of business; office location; or other physical location of operations / presence; and c) identification number. There are two noteworthy exceptions to the CIP rule as related to the information above: a) an institution's CIP policy may account for customers who have applied, but not yet received, a TIN. In these cases, policy may call for the confirmation of the TIN application being submitted before account opening and require the TIN information be obtained and updated within a reasonable period of time after the account is established; and b) allows credit card issuers to obtain the identifying information from third-party sources prior to extending credit to a customer (31 C.F.R. §103.121(b)(2)(i)(a)). Refer to the FAQs; Final CIP Rule (http://www.fincen.gov/statutes_refs/guidance/pdf/finalciprule.pdf).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	While US regulations do not go into depth on specific verification or authentication requirements, the rules around CIP set forth the following minimum requirements: Verification through documents: An institution must ensure its CIP includes procedures that set forth the documents that can be used as part of the verification process. These documents may include: a) for an individual, unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and b) for non-individuals (e.g. corporation, partnership, or trust), documents showing the existence of the entity which can include certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument. Verification through non-documentary methods: An institution must ensure its CIP includes procedures that describe the non-documentary methods that can be used as part of the verification process. It should also cover circumstances in which the institution is unable to verify the true identity of a customer through the documents presented / available (31 C.F.R. §103.121).
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Financial institutions do not currently have explicit regulatory requirements to obtain and retain information on the beneficial owners of a customer entity except as required by Section 312 of the USA PATRIOT Act, where identification of beneficial owners of certain high risk correspondent accounts is mandated as part of the EDD requirements associated with correspondent accounts. Currently U.S. financial institutions have adopted risk-based approaches to CDD and the collection of beneficial ownership information. The level of ownership in a customer entity that triggers beneficial owner identification and due diligence should be determined by the AML risk rating of the customer. It is generally considered that at a minimum, any beneficial owner holding greater than 25% interest in the customer entity should be subject to due diligence, and many institutions collect beneficial ownership information at 10% for high risk entities. As a matter of good practice, the percentage of ownership that triggers due diligence should be lower as the AML risk of the customer / account increases. Note: FinCEN issued a Notice of Proposed Rulemaking ("NPRM") on CDD requirements for banks, broker dealers in securities, mutual funds, futures commission merchants and introducing brokers in commodities on 4 Aug 2014 (http://www.fincen.gov/statutes_regs/files/CDD-NPRM-Final.pdf). This followed the issuance of an Advance Notice of Proposed Rulemaking ("ANPRM") related to CDD and beneficial owner requirements in February 2012. Final comments from industry on the NPRM were due on 3 Oct 2014. The proposed rule would come under the BSA to clarify and strengthen CDD requirements for: (i) banks; (ii) brokers or dealers in securities; (iii) mutual funds; and (iv) futures commission merchants and introducing brokers in commodities. The proposed rule would contain explicit CDD requirements and would include a new requirement to identify beneficial owners of legal entity customers, subject to certain exemptions. FinCEN has stated that, <i>"proposing clear CDD requirements is the most effective way of clarifying, consolidating, and harmonising expectations and practices across all covered financial institutions."</i> As of November 2015, a final rule has not yet been promulgated.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	In the U.S. the Know your Customer ("KYC") process consists of CIP, CDD, and EDD. Regulators require customer due diligence to be conducted commensurate with the AML risk posed by the customer. All customers are subject to CIP, with certain limited exceptions that are defined by regulation. The level of CDD, and whether or not EDD is required, will depend on the customer's AML risk rating. The concept of simplified due diligence does not exist under the U.S. regulatory framework, and has not been promoted by U.S. regulators. The US regulatory regime is founded on the risk-based approach, which applied to KYC would mean that a tiered-approach to CDD and EDD should take place for every customer.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Section 312 of the USA PATRIOT Act requires financial institutions to conduct enhanced due diligence when establishing private banking accounts in the U.S. for a non U.S. person and for certain high risk foreign correspondent accounts.. Typically, customers classified as high risk based on an institution's customer risk rating methodology are also subject to EDD. Factors that would be considered in determining a customer's risk rating would include, at a minimum: geography, nature of business / employment, products / services / channels utilised and potentially legal entity structure among other factors. The FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual also provide guidance on products, services, customers and entities that pose inherent higher risks and thus may require EDD that include but are not limited to: a) Politically Exposed Persons ("PEPs"); b) third party payment processors; c) embassy, foreign consulate and foreign mission accounts; d) Money Services Businesses ("MSBs"); e) professional services providers; f) non-governmental organizations and charities; and g) cash intensive businesses. The KYC program should also include periodic risk-based monitoring of the customer information to determine if there are any substantive changes to the original customer information. High risk customer relationships are generally reviewed annually.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Section 312 of the USA PATRIOT Act requires financial institutions in the U.S. providing private banking services to non-U.S. persons to identify those accounts associated or linked to PEPs and conduct EDD to reasonably ensure the funds in the account are not derived from corruption or other illegality. Institutions are expected to take similar steps as part of risk management to identify PEPs in other areas of the institution. This should include collecting sufficient information from each customer to allow for the determination of PEP status (including relatives and close associates).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Section 312 of the USA PATRIOT ACT directs covered US financial institutions to establish a due diligence program for correspondent banking that at a minimum: a) determines whether the account is subject to enhanced due diligence under section 312; b) assesses the money laundering risk posed, based on a consideration of relevant risk factors; and c) applies risk-based policies, procedures, and controls to each correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the correspondent account activity. The rule itself provides guidance in assessing the risks posed by a correspondent relationship. Section 312 contains a provision requiring U.S. financial institutions to apply EDD when establishing or maintaining a correspondent account for a foreign bank that is operating: a) under an offshore banking license; b) in a jurisdiction found to be non-cooperative with international anti-money laundering principles; or c) in a jurisdiction found to be of primary money laundering concern under §311 of the USA PATRIOT Act. In cases where EDD is required, the institution is required to take reasonable steps to: a) conduct appropriate enhanced scrutiny; b) determine whether the foreign bank itself offers correspondent accounts to other foreign banks (i.e., nested accounts) and, as appropriate, identify such foreign bank customers and conduct additional due diligence on them; and c) identify the owners of such foreign bank, if its shares are not publicly traded (most institutions have a list of approved stock exchanges) (http://www.fincen.gov/news_room/rp/rulings/html/312factsheet.html). Generally, enhanced scrutiny of the transactions associated with any correspondent accounts should be performed to guard against the increased risk of money laundering, in order to identify and report any suspicious transactions / activity as required by US regulations and law.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes. Note that a foreign shell bank does not include an entity defined as a regulated affiliate, i.e. the law defines this term to be an entity with an offshore banking license that is: a) an affiliate of a depository institutions that maintains a physical presence in the U.S. or a country other than the U.S.; and b) is subject to supervision by a banking authority in the country regulating the affiliated depository institution.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In circumstances where a financial institution establishes a relationship with a customer remotely, the institution will need to employ non-documentary methods to verify the identity of the client since it will not be able to use a document to compare the customer to the photo identification, or it will need to establish appropriate reliance agreements in order to rely on a third party who will conduct CIP on behalf of the institution. As part of its CIP, a financial institution should define whether it will accept remote account opening, and if so, what documentary and non-documentary methods will be used to verify customer identity. As a general rule, U.S. regulators encourage the use of more than one method to verify identity.
Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	U.S. financial institutions that are subject to SAR reporting, are required to submit SARs electronically to FinCEN - Department of the Treasury: http://www.fincen.gov/forms/bsa_forms/index.html#SAR

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: January 2014 to June 30, 2015 – 2,643,680 SARs (Source: FinCEN "SAR Stats" report dated October 2015 (https://www.fincen.gov/news_room/rp/files/SAR02/SAR_Stats_2_FINAL.pdf)) Comparative GDP data is not available for this specific period. The data reflected below is based on SARs with filing dates between January 1, 2014 – December 31, 2014 ('subject period'): a) depository institutions filed 886,927 SARs during the subject period; b) MSBs filed 720,985 SARs during the subject period; c) securities and futures firms filed 22,448 during the subject period; d) insurance companies filed 3,183 SARs during the subject period; e) casino and card clubs filed 46,575 SARs during the subject period; f) other types of financial institutions filed 46,899 SARs during the subject period; g) loan or finance companies filed 84 SARs during the subject period; and h) housing government sponsored entities filed 160 SARs during the subject period.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes. Additional reporting includes: a) Currency Transactions Reports ("CTR"); b) report of international transportation of Currency or Monetary Instruments ("CMIR") (http://www.fincen.gov/forms/files/fin105_cmir.pdf) c) Foreign Bank Account Report ("FBAR") (http://www.fincen.gov/forms/files/f9022-1_fbar.pdf), and d) record keeping for certain funds transfers and funds transfer transparency (the Travel Rule).
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Yes, depending upon the type of transaction for various reporting: a) SARs transactions aggregating below USD5,000 (Cf. the requirement to file with FinCEN based on suspicious activity alone with no monetary loss or value attached to the filing (e.g. employee malfeasance or suspicious circumstances involving an attempted account opening); b) CTRs transactions aggregating USD10,000 or less; c) CMIRs transactions aggregating USD10,000 or less; d) FBARs when the aggregate value of the foreign financial accounts are USD10,000 or less during the calendar year; and e) record keeping for transmittal orders for funds transfers (the travel rule) below USD3,000.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes. Penalties for non-compliance are noted in the BSA (http://www.fincen.gov/statutes_regs/bsa). Also see the relevant regulations of FinCEN (http://www.fincen.gov). Generally, Institutions must ensure that all employees know and understand the rules surrounding SAR confidentiality, safe harbour and whistle blower protections (http://www.fincen.gov/statutes_regs/guidance/html/FIN-2012-A002.html).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No. While there are no explicit legal or regulatory requirements to use an automated monitoring system per se, regulators and independent monitors have placed a tremendous amount of scrutiny on the effectiveness of these systems and the data that are feeding into them. Each institution is expected to tailor and tune their automated transaction monitoring systems based on its own risk profile and business strategy. Furthermore, regulators view automated transaction monitoring systems as models, and require independent validation of these systems.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes, but the financial institution should determine which transactions can be monitored outside its jurisdiction on a risk adjusted basis.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes. To comply with the USA PATRIOT Act, a financial institution must implement an AML program that includes, at a minimum: a) the development of internal policies, procedures, and controls (e.g. to determine what is unusual or suspicious activity and what steps to take once an unusual activity is identified); b) the designation of a compliance officer; c) an ongoing employee training program; and d) an independent audit function to test the programs. In the US, this independent review can be conducted internally (e.g. by the financial institution's internal audit function), externally or be co-sourced.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) generally BSA/AML audits are conducted every 12 – 18 months. The audit frequency and scope is set by the institution; b) AML audit reports are generally submitted to the Audit Committee of the Board of Directors, as well as to the Business Unit and Compliance Head for the business that is the subject of the audit. BSA/AML Audit reports are reviewed by the relevant regulatory agency when examiners come in to examine the institution or as part of ongoing supervision as part of an enforcement action; and c) no.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) yes; b) yes; and c) yes. The independent review requires review and testing of a bank's entire AML program, as well as its sanctions program. This will include review and testing all policies, procedures, controls and processes, whether manual or automated, of the AML and sanctions program. The review will cover the program's design and effectiveness, noting any gaps or findings to regulatory requirements and expectations, as well as to bank documented policies and procedures.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	In contrast to the EU, the US does not have any comprehensive personal data protection or privacy laws that apply across all industries. Rather, the US has taken a sectoral approach, in which laws are generally targeted at specific industries or specific types of data. In addition, certain industries are subject only to self-regulation and voluntary guidelines. In the banking industry, the significant data privacy laws are encompassed in the Graham Leach Bliley Act ("GLBA") in the section known as "Regulation P" [12 CFR 1016]. This section calls out numerous specific policies, procedures and actions a financial institution must have in place with respect to consumer privacy notices, choice management and other privacy related matters. In addition, there are financial privacy requirements in the Fair Credit Reporting Act ("FCRA") [Regulation V, 15 USC 1681] with respect to choice management as well as dispute resolution. The Telephone Consumer Protection Act ("TCPA") [47 CFR Part 64] as well as the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act of 2003") have privacy related impacts to financial institutions. The key non-bank secrecy privacy laws are the following: a) Electronic Communications Privacy Act of 1986; b) Health Insurance Portability and Accountability Act of 1996; c) Fair Credit Reporting Act of 1970, which was amended by the Fair and Accurate Credit Transactions Act of 2003; and d) The Children's Online Privacy Protection Act of 1998. In 2000, the Department of Commerce entered into a 'Safe Harbour' framework with the European Union to enable American companies voluntarily to adopt the European Union's Data Protection Directive and voluntarily submit to US enforcement action by the Federal Trade Commission ("FTC") in case of violation of their voluntary privacy commitments. To participate in the program, a US company self-certifies to the US Department of Commerce that it will follow the Safe Harbour Privacy Principles which mirror the core requirements of the EU Data Protection Directive. With limited exception, US based financial firms are generally not eligible to participate in the Safe Harbour program for client or customer data and must make use of binding or contractual methods to comply with EEA data movement regulations. For those firms which GLBA applies, "sensitive customer information means a customer's name, address, or telephone number in conjunction with the customer's social security number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number."

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	On 23 Nov 2010, FinCEN issued guidance, effective 1 Mar 2011, interpreting binding regulations regarding the sharing of SARs by US banks. The guidance provides that a US bank may share a SAR or any information that would reveal the existence of a SAR, with a domestic affiliate, provided the affiliate is subject to a SAR regulation. The guidance defines 'affiliate' of a bank to mean any company under common control with, or controlled by, that depository institution. The guidance also provides that a US bank that has filed a SAR may not share the SAR, or any information that would reveal the existence of a SAR, with its foreign branches. Banks and securities and futures industries may, however, share SARs with its head/parent office irrespective of the head / parent office's location.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Any firm contemplating the transfer of data from a non-US jurisdiction into the US may contemplate that financial records within the US are subject to examination by a wide array of US regulatory and law enforcement bodies.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	GLBA generally prohibits a bank from disclosing non-public client data to a non-affiliated third party unless it: a) provides the client with a notice of its policies and procedures regarding its disclosure of and protection of non-public personal client data; and b) provides the client with an opportunity to prevent a bank from sharing his or her non-public client data with non-affiliated third parties. Thus, in contrast to EU banks secrecy laws, most of GLBA's restrictions on the transfer of personal data do not apply unless a client chooses to have them apply. In addition, GLBA does not restrict a bank's ability to share non-public personal client data. Each of the regulators charged with implementing GLBA has issued regulations. The regulations issued by the OCC are at 12 CFR 30 App. B and 12 CFR 40. The Right to Financial Privacy Act (1978) does not apply to cross-border transfers of data. The Fair Credit Reporting Act (1970) does not apply to cross-border transfers of data. The Bank Secrecy Act of 1970 ("BSA") - Despite the name, this law governs the detection and protection of money laundering rather than the protection of client data. Please note that these laws are the primary federal laws. State laws may also apply. Due to a change made to the pre-emption standard applicable to national banks by the Dodd-Frank Wall Street Reform and Consumer Protection Act, signed into law 21 Jul 2010, national banks may soon be subject to additional state privacy laws. See Public Law No: 111-203 § 1044 ('State Law Pre-emption Standards for National Banks and Subsidiaries Clarified').

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Austria

Key contact: Christoph Polly / Christoph Obermair /
Roland Schoebel
Email: christoph.polly@at.pwc.com /
christoph.obermair@at.pwc.com / roland.schoebel@at.pwc.com
Tel: +43 1 501 88-1167 / +43-1-501 88-3629 /
+43-1-501 88-1170

Postal address: Erdbergstrasse 200;
1030 Vienna;
Austria

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1994. Current AML / CFT relevant amendments: a) Austrian Banking Act and Austrian Insurance Supervision Act last amended on 15 Aug 2015; b) Austrian Criminal Code (§§ 165 following StGB) last amended on 14 Sep 2010; and c) Austrian Finance Criminal Code (§ 38a and § 39 FinStrG) last amended on 31 Aug 2015.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A - The Austrian AML laws and regulations are now based on the Third EU Money Laundering Directive.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) Austrian Financial Markets Authority (FMA) (https://www.fma.gv.at/en/homepage.html); b) Austrian Financial Markets Authority (FMA) (https://www.fma.gv.at/en/homepage.html); and c) Casinos: Ministry of Finance (https://english.bmf.gv.at/); and other: Relevant economic chamber (https://www.wko.at/Content.Node/wir/Austrian_Economic_Chambers_Home.html).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	There are six different circulars in place regarding AML / CFT regulations for the banking industry, other financial services and insurance companies, issued by the Austrian Financial Markets Authority, last amended on 24 Apr 2012 (https://www.fma.gv.at/en/legal-framework/circulars/money-laundering-terrorism-financing.html).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, every active customer has to be identified as well as every client whose account has been closed since 1994.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, a "circular on the risk-based approach" was published by the Austrian Financial Markets Authority on 23 Dec 2009, updated on 01 Dec 2011 (https://www.fma.gv.at/typo3conf/ext/dam_download/secure.php?u=0&file=5972&t=1452004668&hash=28158d2a5884e4fde4493625502a91dd).
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, FATF Mutual Evaluation Report Austria as of 26 Jun 2009 (http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Austria%20full.pdf) and Mutual Evaluation of Austria: 3rd Follow-up Report as of 14 Feb 2014 (http://www.fatf-gafi.org/media/fatf/documents/reports/mer/FUR%20Austria.pdf). The next evaluation is scheduled for 2016/2017.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, one-off transactions below EUR15,000 if there is no AML or CFT suspicion.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Identification and verification is performed using official ID e.g. passport. Customers have to inform the institution if they act on their own account, or on a principal's account. If someone acts on behalf of another person (as a trustee), the identity of that person (the trustor) must also be clarified. The customer has to disclose the ultimate beneficial owner. The institution has to recheck the identity of the ultimate beneficial owner using a risk based approach. Individuals: the following has to be obtained: a) full name; b) date and place of birth; c) nationality; d) address; and e) signature. As part of the verification process, the identity of the customer has to be verified by an independent source (documents of identification), e.g. a passport, identity card or an Austrian driving licence. The name of the state authority which issued the document and the date of issuance also have to be recorded. Legal entities: the following has to be obtained: a) registered name and domicile of the entity; and b) full name of the legal representatives of the entity. This data has to be verified by 'appropriate documentation' e.g. an excerpt of the company register.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	The requirements are defined and are to be seen as a way to rely on the authenticity of the document; if there are any doubts then the identity of a person should be verified by other measures. In this case, a suspicious activity report has to be considered.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The Austrian banking and insurance laws require the verification of the identity of beneficial owners holding more than 25% of the shares or voting rights of an entity or holding 25% or more of a trust or foundation. Where a principal owner is another corporate entity or trust, the institution has to take measures to establish the identity of the ultimate beneficial owners (who can only be natural persons) and/or, if applicable, the trustees. In case of a trust or foundation, the identity of the founder and the beneficiaries designated to receive 25% or more of the trust/foundation have to be disclosed by the client. Credit institutions, financial institutions and insurance companies must call upon the customer to reveal the identity of the customer's beneficial owner(s). The customer must comply with this request, and credit institutions, financial institutions and insurance companies must take risk-based and appropriate measures to verify the beneficial owner's identity so that the credit institution, financial institution or insurance company is satisfied that it knows who the beneficial owner is. In the case of legal persons or trusts, this also includes taking risk-based and appropriate measures in order to understand the ownership and control structure of the customer.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced due diligence arrangements are available for the following, but only if the AML/CFT risk is considered low: a) domestic public authorities and public authorities of the European Union ("EU"); b) listed companies; c) credit and financial institutions situated in a third country which impose requirements equivalent to those defined in the third EU AML Directive and which are supervised in compliance with those requirements; and d) beneficial owners of pooled accounts held by notaries and other legal professionals from EU Member States.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	For customers where a higher risk of money laundering or terrorist financing applies, for example: a) if the customer has not been physically present for identification (distance business/non-face-to-face-relationships); b) for cross-frontier correspondent banking relationships with correspondent banks from other countries or from the European Economic Area ('EEA') (the latter only if the AML/CFT risk is considered heightened); and c) for Politically Exposed Persons ("PEPs") of other EU Member States and of third countries. Furthermore, if the client or an authorised signatory, a person, to whom the client has a significant business relationship, or the trustee or the beneficial owner has his/her domicile or residence in one of the following states (see below), or the transaction is made via an account at a bank in one of the following states: a) Iran; b) Democratic People's Republic of Korea ("DPRK"); c) Bolivia; d) Cuba; e) Ethiopia; f) Indonesia; g) Kenya; h) Myanmar; i) Nigeria; j) Pakistan; k) Sao Tome and Principe; l) Sri Lanka; m) Syria; n) Tanzania; o) Thailand; p) Turkey; q) Vietnam; and r) Yemen.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	In any transaction or business relationship with a PEP of another EU Member State (except Austria) or another country.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Enhanced due diligence procedures to be performed for cross-border correspondent banking relationships with correspondent banks from third countries or from the EEA (the latter only if the AML/CFT risk is considered heightened) as follows: a) credit institutions and financial institutions must gather sufficient information about a correspondent bank to fully understand the nature of its business and be able to ascertain the reputation of the institution and the quality of supervision on the basis of publicly available information; b) credit institutions and financial institutions must satisfy themselves of the correspondent bank's anti-money laundering and anti-terrorist financing controls; c) credit institutions and financial institutions must obtain approval from senior management before establishing new correspondent banking relationships; d) credit institutions and financial institutions must document the respective responsibilities of each institution; and with respect to payable-through accounts, credit institutions and financial institutions must be satisfied that the correspondent bank has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent, and that it is able to provide relevant customer due diligence data to the correspondent bank upon request.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, credit institutions are prohibited from entering into or continuing a correspondent banking relationship with a shell bank. Credit institutions have to take appropriate measures to ensure that they do not engage in or continue correspondent banking relationships with a bank that is known for permitting its accounts to be used by a shell bank.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Non face-to-face relationships and transactions are considered heightened AML/CFT risk by the relevant Austrian AML laws and regulations. For this reason, additional due diligence is always required for non face-to-face relationships and transactions. Trustees must always be identified personally (obligation of personal presence) - non face-to-face relationships are not sufficient for purposes of identification of trustees. Furthermore, additional due diligence is always required (whether face-to-face or non-face-to-face) in the case of any doubts, indication or suspicion of money laundering or terrorist financing. In these cases, suspicious activity reports have to be considered.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Suspicious activity reports are to be reported to the Austrian Financial Intelligence Unit ("A-FIU"), so called "Geldwäschemeldestelle" (http://www.bmi.gv.at/cms/BK/meldestellen/geldwaesche/start.aspx).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 1,673 SARs GDP (in current prices): 2014 – USD436,300m (Source: data.worldbank.org) This results in a ratio of 1 SAR for every USD260.7m of GDP.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Suspicious activities regarding money laundering and terrorist financing as well as the suspicion that a client might not properly have disclosed a trusteeship have to be reported.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No, every suspicion described in A20 has to be reported, regardless of the amount.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	No specific penalties prevail for non compliance with reporting requirements, but there are penalties for non compliance with AML and CFT regulations (e.g. § 99 (2) BWG, Austrian Banking Act). Non compliance with reporting requirements can be seen as non compliance with AML and CFT regulations.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No, there is no legal or regulatory requirement to use specific AML/CFT IT systems, but in practice, larger institutions will not be able to apply the risk based approach without any IT monitoring technology.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	In the course of suspicious activity reporting, the institution should ask the A-FIU, whether it can proceed with the transaction or not. The A-FIU has the right to stop ongoing transactions or to forbid future transactions, if there is a suspicion.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	There is no clear rule in place, but there is the legal requirement that Austrian institutions have to apply the same AML/CFT standards as in Austria to jurisdictions outside Austria where they conduct their business (e.g. in CEE (Central and Eastern Europe) and SEE (South Eastern Europe) countries where banks with headquarters in Austria also conduct business).

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes.
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) once a year; b) the report is submitted to the audit client who forwards it to the financial market authority and the Austrian national bank; and c) no, it is a separate audit of compliance with several regulatory requirements.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	It requires testing the internal control system of the bank regarding regulatory requirements which also includes AML. No sample testing is required.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Austria has established a data protection act. It has been in force since 1 Jan 2000 (https://www.dsb.gv.at/DocView.axd?CobId=41936): a) see the definition in Section 4 Data Protection Act: "Data" ("Personal Data") [Daten] ("personenbezogene Daten"): Information relating to data subjects (sub-para. 3) who are identified or identifiable; Data are "only indirectly personal" for a controller (sub-para. 4), a processor (subpara.5) or recipient of a transmission (sub-para. 12) when the Data relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means; "Data Subject" ["Betroffener"]: any natural or legal person or group of natural persons not identical with the controller, whose data are processed (sub-para. 8); b) see above (data subject); and c) see the definition in Section 4 Data Protection Act: "Sensitive Data" ("Data deserving special protection") ["sensible Daten" ("besonders schutzwürdige Daten")]: Data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health or sex life; The use of sensitive data does not infringe interests in secrecy deserving only and exclusively in the special cases as set out in § 9 data protection act.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Some general remarks: All data applications [Datenanwendungen] are subject to notification, unless an exception applies (see below). A data application [Datenanwendung] encompasses all categories of data [Datenarten] (e.g. name, address, salary) processed about certain categories of data subjects [Betroffenenkreise] (e.g. employees, customers). The notification has to state the categories of recipients [Empfängerkreise] - including possible recipient states abroad - as well as the legal basis for the transmission. Data concerning health life are considered to be sensitive data (see the definition above). For information on Criminal Records [Strafregister], the special regulations of the Criminal Records Act 1968 [Strafregistergesetz 1968] shall apply. See: https://www.dsb.gv.at/DocView.axd?CobId=41936
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Austrian Banking Act.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes, Credit institutions, their members, members of their governing bodies, their employees as well as any other persons acting on behalf of credit institutions must not divulge or exploit secrets which are revealed or made accessible to them exclusively on the basis of business relations with customers.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Belgium

Key contact: Rudy Hoskens
Email: rudy.hoskens@be.pwc.com
Tel: +32 2 710 4307

Postal address: Woluwe Garden,
Woluwe 18, B-1932 Sint-Stevens-
Woluwe- Belgium

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The local law became effective in 1993. However, to incorporate the third AML Directive, it has been amended by the law of 18 Jan 2010. All articles referred to below, are the articles mentioned in this law: http://www.ctif-cfi.be/website/images/NL/law_be/loi937042015.pdf
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	Since April 2011, the supervision of the Belgian financial sector has been organised according to the "Twin Peaks" model, with two autonomous supervisors, namely the National Bank of Belgium ('NBB') and the Financial Services and Markets Authority ('FSMA'), both of which are competent (depending on the licence, NBB or FSMA is competent) in the field of AML related matters to the financial sector. Within the "Twin Peaks" model the micro-prudential and systemic control, as well as the macro-prudential supervision is entrusted to the NBB. The supervision of the compliance with good conduct rules to which financial intermediaries are subject to are entrusted to the FSMA. For more information please see http://www.nbb.be and http://www.fsma.be .
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	There is specific guidance per sector on the website of the Belgian Financial Intelligence Processing Unit ('CTIF-CFI') for a risk-based approach: http://www.ctif-cfi.be/website/index.php?option=com_content&view=article&id=71&Itemid=99&lang=en
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No - however, the local law requires identification data to be updated in cases where there are doubts about the veracity or accuracy of previously obtained identification data, or where the risk sensitivity of the client requires this (Art. 7, §3 and Art. 8, §2).
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Companies are required to apply fitting measurements on a risk based approach when verifying the identity of the final beneficiary or beneficiary of the client (Art. 8, §1, art. 8, §2 and art. 12, §2).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	After the adoption of their Mutual Evaluation Report ('MER'), FATF member countries are required to provide information on the measures that have been implemented to deal with the deficiencies identified in the report. Belgium is subject to this process of providing a biennial update (i.e. every two years) to the FATF Plenary on any of the 40 Recommendations that are rated PC (Partially Compliant) or NC (Non-Compliant). The fourth update was provided to the Plenary on 26 Feb 2015 and is available on the website of CTIF-CFI (http://www.ctif-cfi.be/website/images/NL/eval_fatf/mer2015.pdf). In May 2013, the IMF Country Report N° 13/133 was published: Belgium: Detailed Assessment of Compliance with the Basel Core Principles for Effective Banking Supervision (http://www.imf.org/external/pubs/ft/scr/2013/cr13133.pdf).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, when the customer wishes to carry out a transaction outside the context of a business relationship: - for an amount below EUR10,000 (art. 7, §1, 2°, a); and - consisting in a transfer of funds to a payee's account within Belgium for an amount less than or equal to EUR1,000 on condition that (art. 7, §1, 2°, b) these transfers are not considered to fall under the Regulation on information on the payer accompanying transfers of funds (No. 1781/2006): - the transfer is a payment within the terms of an agreement for the provision of goods or services, concluded between the payer and the payee; - the payee's account was opened to enable the payment for the provision of goods or services; - the payment service provider of the payee is subject to the obligations set out in the Law of 11 Jan 1993; and - this payment service provider is able, by means of a unique identifier, to trace the transaction via the payee back to the payer. If customers wish to carry out a financial transaction related to gaming for an amount less than or equal to EUR1,000) (art.9). Companies are not obliged to carry out the identification and identity verification of the following persons (art. 11, §1): - a credit or financial institution, as referred to in Article 2 of Directive 2005/60/EC, situated in Belgium or in another country of the European Economic Area; - a listed company whose securities are admitted to trading on a regulated market within the meaning of Directive 2004/39/EC in a country of the European Economic Area; - the beneficial owners of pooled accounts held by notaries and other independent legal professionals established in Belgium, in another country of the European Economic Area; - a customer or beneficial owner that is a Belgian public authority; and - customers that are European public authorities or institutions. Companies are not obliged to carry out the identification and identity verification of the following products or transactions (art. 11, §2): - life insurance policies where the annual premium is no more than EUR1,000 or the single premium is no more than EUR2,500; - insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; and - a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest. The above exceptions cannot apply where there is a suspicion of money laundering or terrorist financing or when there are doubts about the veracity or accuracy of previously obtained identification data regarding a customer who has already been identified.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals and institutions must identify clients and their agents. Identification of natural persons: surname, first name, date and place of birth and, whenever possible, relevant information on the address of the identified person (art. 7, §1, paragraph 3). Identification for legal persons, trusts, fiduciaries and similar legal arrangements: corporate name, registered office and directors, and note must be taken of the provisions regarding the power to commit the legal person, trust, fiduciary or similar legal arrangement (art. 7, §1, paragraph 4). The identification must be verified by means of a supporting document, of which a copy is made on paper or by electronic means. For natural persons, a copy of their identity card or passport is required and for legal person, a copy of their coordinated statutes (art. 7, §2). Together with the identification, information must be collected regarding the purpose and intended nature of the business relationship (art. 7, §1, paragraph 5).
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Clients must be identified by means of a supporting document, of which a copy is made on paper or by electronic means (art. 7, §2). Such documents need to be probative documents, admissible as evidence. There is no information about certification by external third parties in local legislation.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	For the beneficial owner, the identification must cover the surname, first name and, whenever possible, the date and place of birth. In addition, whenever possible, relevant information must be collected with regard to address details. Furthermore, appropriate risk based measures must be taken to verify these data sources (art. 8, §1, paragraph 4).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	The local regulation does foresee this possibility where (art. 11, §1): a) the customer or beneficial owner is a credit or financial institution as defined in art. 2 of the third AML Directive, established in Belgium or another country within the EEA, or an equivalent institution established in a third country that has foreseen requirements and controls similar to those in the third AML Directive and of which a specific list is to be drawn in a Royal Decree; b) the customer or beneficial owner is a listed company whose securities are admitted to trading on the regulated market within the meaning of Directive 2004/39/EC in a country of the EEA, or is a listed company from a third country, designated in a Royal Decree, and which is subject to disclosure requirements consistent with community legislation; c) the beneficial owner of a pooled account held by notaries and other independent legal professionals established in Belgium or another country within the EEA or from third countries, designated in a Royal Decree, provided that they are subject to requirements to combat money laundering or terrorist financing consistent with international standards and are supervised for compliance with those requirements and provided that the information on the identity of the beneficial owner is available, on request, to the institutions that act as depository institutions for the pooled accounts. If the client would be bound by professional secrecy, and thus unable to provide the information on the identity of the beneficial owner, the client needs to confirm in writing or by electronic means to the depository institution that the beneficial owners of the pooled accounts involved are solely clients with whom the relationship consists in ascertaining their legal position or performing their task of defending or representing those clients in, or concerning judicial proceedings including giving advice on instituting or avoiding proceedings. The client or beneficial owner is a Belgian public authority; d) the client is a European public authority or institution, included on a list to be drawn in a Royal Decree; and e) the client is a person or institution indicated in a specific list yet to be drawn in a Royal Decree. In addition, by way of derogation, it is allowed not to apply customer or beneficial owner due diligence in respect of (art. 11, §2): a) life insurance policies where the annual premium is no more than EUR1,000 or the single premium is no more than EUR2,500; b) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme; d) electronic money as defined in article 3, §1, 7° of the law of 22 Mar 1993 regarding the pursuit of and prudential supervision of credit institutions, where, if the device cannot be recharged, the maximum amount stored in the device is no more than EUR150, or where, if the device can be recharged, a limit of EUR2,500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR1,000 or more is redeemed in the same calendar year by the bearer as referred to in article 5 of the law of 22 Mar 1993; and e) in respect of any other product or transaction representing a low risk of money laundering or terrorist financing which meets the criteria to be established in a royal decree. If customers wish to carry out a financial transaction related to gaming for an amount less than or equal to EUR1,000 (art. 9).
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Local regulation foresees enhanced customer due diligence measures on a risk sensitive basis in situations which by their nature can represent a higher risk of money laundering or terrorist financing, and at least in the following situations (art. 12, §1): a) establishing a business relationship with or carrying out a transaction for a customer that was not physically present for identification purposes (non face-to-face contact) (art. 12, §2); b) establishing a business relationship or carrying out a transaction with or for a PEP (art. 12, §3) (see A14 below); and c) engaging in cross-border correspondent banking relationships with respondent institutions from third countries (art. 12, §4) (see A15 below).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Belgium has instituted a comprehensive set of measures applicable to PEPs. These measures include (art. 12, §3, paragraph 4): a) applying appropriate risk based procedures to determine whether the customer or his beneficial owner is a PEP; b) obtaining approval from a sufficiently senior level of management before establishing business relations with such customers; c) taking appropriate risk-based measures to establish the source of wealth and funds that are involved in the business relationship or transaction; and d) conducting enhanced ongoing monitoring of the business relationship.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Belgium is in full compliance with the FATF recommendations regarding issues of correspondent banking. It is obliged to (art. 12, §4, paragraph 1): a) gather sufficient information about the respondent institution in question to understand fully the nature of its business and to determine from publicly available information its reputation and the quality of the supervision to which it is subject; b) assess the respondent institution's anti-money laundering and anti-terrorist financing controls; c) obtain approval from a sufficiently senior level of management before establishing new relationships; d) document in writing the respective responsibilities of each institution; and e) with respect to payable-through accounts, be satisfied that the respondent institution has verified the identity of and has performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes (art. 12, §4, paragraph 2).
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	When entering into a business relationship with a client that is not physically present, specific and adequate measures need to be taken to deal with the increased risk of money laundering and terrorism financing that exist in such circumstances (art. 12, §2).

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The Belgian Financial Intelligence Processing Unit (CTIF-CFI), established by the Law of 11 Jan 1993, is a central part of the Belgian AML/CFT system. CTIF-CFI is an independent administrative authority with legal personality and is supervised by the Ministers of Justice and Finance. CTIF-CFI is in charge of processing suspicious financial facts and transactions linked to money laundering and terrorism financing and which are reported by institutions and individuals specified in the law (http://www.ctif-cfi.be/). In accordance with the Law of 11 Jan 1993 on preventing use of the financial system for purposes of money laundering and terrorist financing, CTIF-CFI received a total of 27,767 disclosures in 2014, which is approximately an 33% increase compared to 2012.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 27,767 SARs GDP (in current prices): 2014 – USD533.4m (Source: data.worldbank.org[*]) This results in a ratio of 1 SAR for every USD19.2m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	The institutions and persons as referred to in the law, shall carefully examine any transaction or action they consider particularly likely, by its nature or its unusual character in view of the customer's activities, by the circumstantial elements or by the capacity of the persons involved, to be related to money laundering or terrorist financing (art. 14, §1, paragraph 2). The following institutions and persons should report the following transactions: a) the sales price of real property may only be paid by means of a bank transfer or cheque. The agreement and deed of sale must specify the number of the financial account from which the amount was or will be debited (art. 20); b) in case of doubt about the veracity or accuracy of previously obtained identification data about a customer who has already been identified (discretionary) (art. 7, §1, 4°); c) in case of a suspicion of money-laundering or terrorism financing (art. 23 – 26); d) in case of international transactions and facts involving natural or legal persons domiciled, registered or situated in a country or territory whose legislation is considered insufficient by a competent international consultative and coordinating authority or whose practices are deemed by this authority to impede the fight against money laundering and terrorist financing (art. 27); e) in case of the suspicion of serious and organised fiscal fraud (art. 28).
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	The price of a sale by a merchant of one or more products, as well as the price of one or more provision of services supplied by a service provider, for an amount of EUR3,000 or more may not be paid in cash, unless the amount does not exceed 10% of the sale price and as long as this amount does not exceed EUR3,000 regardless of whether the sale or service takes place in a single or in several apparently related transactions. The price of a purchase by a merchant in precious metals of one or more products, for an amount of EUR3,000 or more may not be paid in cash, unless the amount does not exceed 10% of the purchase price and as long as this amount does not exceed EUR3,000 regardless of whether the purchase takes place in a single or in several apparently related transactions (art. 21).
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	According to article 40 of the AML law of 1993, non-compliance with reporting requirements towards CTIF-CFI can result in the following sanctions imposed by the competent authority: a) publish, in accordance with terms it determines, the decisions and measures it shall adopt; b) impose an administrative fine of not less than EUR250 and not more than EUR1.25m after hearing the defence of the institutions and persons or at least after having duly summoned them.

^{*} GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Monitoring should be carried out on a continuous basis or triggered by specific transactions. It need not require electronic systems, although for some types of banking activity, where large volumes of transactions occur on a regular basis, automated systems may be the only realistic method of monitoring transactions. However, where automated systems are used, banks should understand their operating rules, verify their integrity on a regular basis and check that they address the identified ML/TF risks (FATF – Guidance for a Risk Based Approach, paragraph 67 – applicable in Belgium) (http://www.ctif-cfi.be/website/images/EN/rba/rbabankingsector.pdf).

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	According to article 23 of the law, the CTIF-CFI may, should it deem such action necessary due to the seriousness or urgency of the matter, oppose execution of any suspected transaction of which it has been informed. The CTIF-CFI shall determine to which transactions and to which accounts the opposition shall apply and shall inform the institutions and persons referred to in article 2, §1 immediately. This opposition shall halt the execution of the transaction for a maximum of two working days starting from the time of notification. If the CTIF-CFI thinks the measure should be extended, it shall refer the matter to the Public Prosecutor, who will take the necessary decisions. In the absence of a decision within the abovementioned two days after notification, the said institutions and persons are free to execute the transaction.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	There is no specific restriction to monitor the transactions in another jurisdiction but the responsibility remains within the entity in Belgium. In particular, transactions of some branches of foreign banks are monitored by the parent company.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, if you are processing personal data in Belgium, you are subject to the Belgian Privacy Act of 08 Aug 1992: a) yes. Personal data is defined as any information relating to an identified or identifiable natural person, hereinafter the 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Article 1 §1 Privacy Act.). Personal data covers any information relating to an identified or identifiable natural person, e.g. name, address bank account, education, images, GPS data, IP address, etc.; b) as mentioned, the scope of protection of this Act only covers natural persons (private individuals) not legal persons. Corporate data is therefore not protected under privacy law in Belgium, unless it relates to private individuals (e.g. HR data); c) yes. By principle, the processing of sensitive data is forbidden (exceptions exist). Sensitive data relate to race, political opinions, religious or philosophical beliefs, trade-union membership, health, sex life, prosecutions or criminal or administrative convictions (art. 6 Privacy Act).
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	From a privacy perspective, transfer of credit reports fall under the general requirements of personal data processing, to the extent these qualify as personal data.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	There exists specific privacy legislation for certain sectors e.g. public sector, telecom sector which apply in addition to the Privacy Act mentioned above.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	There is no bank professional secrecy in Belgium (as regards section 458 of Penal Code) but only a discretion obligation policy for income taxation. With respect to the taxpayer himself, section 318 of the Belgian Income Tax Code ("BITC") provides that tax authorities are not authorised to gather information from the accounts, books and documents of a bank, exchange, credit and savings institutions established in Belgium with a view to taxing its clients. However, if in the course of an inquiry related to the institution's own tax situation, the tax authorities discover relevant information leading to a suspicion that a mechanism of tax fraud exists or is being prepared, then the tax authorities are allowed to examine the institution's records in order to determine the client's tax liability. With respect to third parties, section 322 BITC provides that tax authorities may, for a given taxpayer, gather written evidence, hear third persons, proceed to inquiries and require from natural persons or corporate bodies as well as companies and associations not having legal personality, to produce any information which it may deem necessary for the purpose of assuring the fair collection of tax. As regards to banks, the second paragraph of section 322 provides the tax authorities the possibility to obtain information from clients of the bank provided they first requested information from the taxpayer himself who refused to communicate information, and provided indications of tax fraud or greater wealth exist. Finally, note that a Central Point of Contact has recently been created towards which the banks are deemed to communicate names and accounts of their clients which could later be used by the tax authorities in case of indications of fraud. In case of indication of fraud, an exchange of information may also take place between Belgium and other countries (Member States of the EU, and countries with which Belgium has concluded a double taxation treaty or a treaty relating to an exchange of information). Please refer to following legislation for more details: a) Art. 55-57 Law of 14 Apr 2011 (Dutch: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2011041406 and French: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2011041406&table_name=loi); and b) Royal Decree of 03 Feb 2014 (https://www.nbb.be/doc/cr/cap/ar_kb_2014_02_03_autorisant_bnb_et_declarants_a_acceder_au_mpp.pdf (Dutch and French)).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Bosnia & Herzegovina

Key contact: Jock Nunan / Nermina Hadziosmanovic
 Email: jock.nunan@rs.pwc.com /
nermina.hadziosmanovic@ba.pwc.com
 Tel: +38733295234 / +381113302100

Postal address: Fra Anđela Zvizdovića 1,
 Tower B 13th Floor,
 71000, Sarajevo

Last updated:
 January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The new law on the prevention of money laundering and financing of terrorist activities became effective on 01 July 2014.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	Previous law on the prevention of money laundering and financing of terrorist activities defined measures and responsibilities of the Financial intelligence department of the State Investigation and Protection Agency, persons liable under this Law, other state authorities and legal entities with public authorisations for detection and prevention and investigation of money laundering and financing of terrorist activities. It also prescribed measures and responsibilities of the Financial intelligence department for international cooperation for the prevention of money laundering and financing terrorist activities.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	State Investigation and Protection Agency (http://www.sipa.gov.ba/en) Financial Intelligence Department ("FID").
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes. See http://sipa.gov.ba/assets/files/secondary-legislation/eticki-kodeks-bs.pdf .
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	For customers who existed before the current AML legislation was introduced, companies are obliged to collect missing documentation and data.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last 3 years? If yes, please find a link to a relevant report (if publicly available).
A7.	The latest evaluation was in 2009 (http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round3/MONEYVAL(2009)42Rep_BIH3_en.pdf). In April 2015, Moneyval issued a statement on Bosnia and Herzegovina and noted that amendments to the financing of terrorism offence in the Criminal Code were adopted and entered into force on 24 March 2015. However, other necessary amendments to the Criminal Code have still not been adopted (http://www.coe.int/t/dghl/monitoring/moneyval/Publications/4th%20Public%20Statement.pdf).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Transactions less than approximately EUR15,339 are not reported to the Financial Reporting Organisation.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Identification of the customer based on documents, data and information obtained from relevant and objective sources (originals or verified copies of ID cards, excerpt from court registers, etc.) in order to: a) determine the beneficial owner; b) obtain information on the purpose and nature of the business relationship or transaction; and c) perform continuous monitoring of business activities of the customer.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Copies of identification documents must be verified.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Identity of the beneficial owner of the legal entity is verified through the original or verified copy of the excerpt from court register or other public register. If this is not possible the controller shall gather all relevant information from the original or verified documentation and business records submitted by the agent of the person authorised by the beneficial owner, or by obtaining a written statement from an agent or another person authorised by the beneficial owner.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced / simplified due diligence arrangements are available if customers are institutions with public authority (authorities of Bosnia and Herzegovina, Federation Bosnia and Herzegovina, Republic of Srpska or Brcko District), banks, insurance companies and other physical person or legal entity which is acting as agent in the sale of insurance policies, investment and retirement funds regardless of the legal form which have headquarters in Bosnia & Herzegovina, or in the territory of the European Union, or in the countries which fulfil internationally accepted standards for the prevention of money laundering and financing of terrorist activities, based on the information obtained from Financial Reporting organisations, international organisations or other authorised international authorities, and which are approved by Ministers, and customers which are characterised as low risk clients by controllers.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence, apart from usual identification requirements, include additional measures which are prescribed by the Law: a) when entering into a relationship with the bank or any other credit institution which is headquartered in a country which is not on the list of countries that apply internationally accepted standards for the prevention of money laundering and financing of terrorist activities. Additional data which are required for enhanced procedures are: data on date of issuing and period for which licence for performing financial services is valid, name and address of the authority that issued licence, description of the internal procedures for prevention of money laundering and financing of terrorist activities, description of the relevant legislation for prevention of money laundering which are applied in the country where the bank or credit institution is registered, a written statement that the bank or credit institution does not have business relationship with shell banks, a written statement that the bank or credit institution does not have established or that it is not entering into a business relationship with shall banks, a written statement that bank or credit institution is subject to administrative supervision in the country where it has headquarters, and that it is obliged to adjust its business with laws for preventing money laundering and financing of terrorist activities; b) when entering into a relationship with Politically Exposed Person ("PEP"). When the client and/or owner of the client that enters into a business relationship or executes a transaction, or when the client and/or owner of the client on whose behalf is entered into a business relationship or performed the transaction is a PEP, additional measures for identification of the client must be performed: gather information on source of income and assets which is or shall be subject to a business relationship or transaction for documentation that is presented by the client (when this information cannot be obtained in the prescribed manner, the client must provide written statements), persons liable for carrying out measures for money laundering detection and the prevention of money laundering shall obtain written approval from the top management before entering into a business relationship with the PEP, after entering into a business relationship with the PEP. Persons liable for carrying out measures for money laundering detection and the prevention of money laundering shall monitor transactions and other business activities of PEPs; c) in the event a client was not physically present when identification was performed. Persons liable for carrying out measures for money laundering detection and the prevention of money laundering shall gather additional documentation, information and data based on which identification can be checked. Additionally check or confirm submitted documentation, identification documents by the credit or financial institution, apply measures that the first payment in the business relationship is performed via an account opened in the name of the client in the other credit institution; and d) in any other cases, for new or existing clients, when due to the business relationship, specifics of the transaction, business profile of the client, or any other circumstances which are related to the client, when the risk of money laundering and financing of terrorist activities exists.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Enhanced customer procedures are required for foreign and domestic PEPs and for every physical person who has or used to have an exposed public function, their close family members and close associates. PEPs include president of the state, premiers, ministers, deputies of ministers, assistants of ministers, representatives of the legislators, judges of the supreme court, constitutional court or other courts, members of the audit department and board of governors of the Central Bank, ambassadors and officers of the military forces and members of the management or supervisory boards of companies which are mainly owned by the state.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Enhanced customer due diligence procedures are prescribed for banks and other financial institutions which have headquarters abroad. Apart from identification and monitoring procedures, the company is obliged to: a) gather information on whether a customer has license, and if yes, for which period the license is granted for providing banking services, name and headquarters of the authority which issued the license; description of the internal procedures which relate to identification and prevention of money laundering and financing of terrorist activities; description of the internal procedures for identification of the beneficial owner of the customer, which relate to reports on suspicious transactions to the relevant authorities; description of the internal procedures for keeping the reports, description of the internal controls and other procedures adopted by the bank for the detection and prevention of the money laundering or financing terrorist activities; b) obtain a description of the relevant legislation in the field of detection and prevention of money laundering and financing terrorist activities in the state where the bank or similar financial institution is established or registered; c) obtain a written statement that the bank or other similar financial institution does not have any business relations with shell banks; d) obtain a written statement that the bank or other similar financial institution does not have a legal relationship with shell banks; e) obtain a written statement that the bank or other similar financial institution is not under administrative supervision in the residence state and that, in accordance with legislation in the residence state, has an obligation to adjust its business activities to be in line with legislation which relates to the detection and prevention of money laundering and financing of terrorist activities; and f) ensure an employee of the controller shall not enter into business relationship with a foreign bank prior obtaining approval from his superior.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	The following identification procedures are required for customers not physically present during the identification process: a) gather additional identification documents, data and information based on which the identity of the customer can be checked; b) perform additional checks of the identification documents submitted and obtain confirmation for those documents from another loan or financial institution; and c) apply measures by which the first payment is performed via an account opened in the name of the customer in another financial institution.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	SARs are made to the State Investigation and Protection Agency (http://www.sipa.gov.ba/en) (Financial Intelligence Department of the State Investigation and Protection Agency).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 - 166 SARs GDP (in current prices): 2014 – USD18,286m (Source: data.worldbank.org *) This results in a ratio of 1 SAR for every USD110.2m of GDP.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	There is an obligation to report any suspicious client or person.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Transactions below approximately EUR15,339.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	AML legislation prescribes financial penalties for non compliance with reporting requirements for the legal entity, controllers, responsible persons in the legal entity and independent entrepreneurs.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	A transaction which is identified as suspicious is temporarily suspended based on the warrant of the Financial Reporting Organisation up to a maximum of 5 days.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Local legislation allows the Financial Reporting Organisation to request documentation and information from other authorities which are responsible for prevention of money laundering.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) once a year; b) the Banking Agency; and c) no.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) yes; b) yes, c) yes.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes: a) yes; b) N/A; and c) no.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Personal data that are processed may be taken out of Bosnia and Herzegovina to another country or be given to an international organization that implements adequate safeguards for personal data. Adequacy of safeguards is estimated on the basis of specific circumstances in which the transfer of personal data is conducted, in which particularly the following shall be taken into account: a) types of personal data; b) the purpose and period of processing; c) the country in which data is transferred; d) statutory rules in force in the country in which data are transferred; and e) professional rules and security measures that must be respected in that country. Personal data that are processed may be taken out of Bosnia and Herzegovina to another country that does not provide adequate safeguards when: a) the disclosure of personal data is provided by special law or an international treaty binding for Bosnia and Herzegovina; b) the prior consent was obtained from the person whose data are transferred and the person was informed on the potential consequences of the data transfer; c) the disclosure of personal data is necessary to fulfil the contract between the data subject and the controller or the fulfilment of pre-contractual obligations undertaken at the request of the person whose data are processed; d) the disclosure of personal data is necessary to save the life of the person to whom the data pertains or when it is in his/her vital interests; e) the personal data are transferred from the files or records which are, in accordance with the law or other regulations, available to the public; f) the transfer of personal data is necessary for the public interest reasons; and g) the transfer of personal data is necessary for concluding or fulfilling a contract between the controller with a third party when the contract is in the interest of the person whose data are processed. Exceptionally, the Agency for data protection may approve the transfer of data from Bosnia and Herzegovina to another country which does not provide an appropriate level of protection as defined, when a controller in another country provides adequate safeguards for the protection of privacy and fundamental rights and freedoms of individuals or provision of similar rights arises from the provisions of a special agreement.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Croatia

Key contact: Dženet Garibović
Email: dzenet.garibovic@hr.pwc.com
Tel: +385 1 6328 888

Postal address: Ulica kneza Ljudevita
Posavskog 31
10000 Zagreb

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Anti- Money Laundering and Terrorist Financing Act (Official Gazette No. 87/2008), based on the Third EU AML Directive, became effective on 1 Jan 2009. It replaced the previous Croatian AML legislation from 1997. It was amended by the Act on Amendments to the Act on Anti-Money Laundering and Terrorist Financing Act (Official Gazette 25/2012), however these amendments were of linguistic nature and did not bring any changes to the AML/TF procedures established by the original AML/TF Act. The new Criminal Code (Official Gazette 125/2011) came into force in January 2013 introducing new definitions of money laundering as a criminal offence (Article 265), terrorist financing and other related criminal offences (Articles 97 -103).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) The Croatian National Bank supervises banks and other credit institutions (http://www.hnb.hr/novcan/pranje_novca_terorizam/e-pranje-novca-terorizam.htm); b) The Croatian Financial Services Supervisory Agency ("HANFA"), conducts supervision of other financial services capital markets participants, funds, insurance companies, leasing and factoring companies etc. (http://www.hanfa.hr/) and the Financial Inspectorate of the Ministry of Finance regulates and supervises non-banking financial institutions such as exchange offices, money transfer services, etc. (http://www.mfin.hr/en/financial-inspectorate); and c) The Financial Inspectorate of the Ministry of Finance supervises professional activities sector (lawyers, notaries public, accountants, auditors, tax advisers) (http://www.mfin.hr/en/financial-inspectorate) and the Tax Administration – organisers of games of chance and checking of domestic legal entities and individual's compliance with the prescribed limitation of cash payments in an amount exceeding HRK105,000, i.e. amount exceeding EUR15,000 in the arrangements with non-residents (http://www.porezna-uprava.hr/en/Pages/default.aspx).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, there are several guidelines available: The Croatian National Bank's Guidelines for the implementation of the Anti -Money Laundering and Terrorist Financing Act with respect to credit institutions, credit unions and electronic money institutions: http://www.hnb.hr/novcan/pranje_novca_terorizam/e-smjernice-zakon-spft-ki-en.pdf The Croatian Financial Services Supervisory Agency Guidelines for the implementation of the Anti- Money Laundering and Terrorism Financing Act for obligated persons who fall within the supervisory scope of the Croatian Financial Services Supervisory Agency (Croatian version only): http://www.hanfa.hr/ Ministry of Finance – Financial Inspectorate: a) general guidelines for the implementation of the Anti -Money Laundering and Terrorism Financing Act (http://www.mfin.hr/en/anti-money-laundering-office); b) guidelines for the implementation of the Anti-Money Laundering and Terrorism Financing Act for audit firms, independent auditors, natural and legal persons who provide accounting and tax counselling services (Croatian version only) (http://www.mfin.hr/adminmax/docs/Sektorske_smjernice_za_revizore_itd.pdf); c) guidelines for the implementation of the Anti-Money Laundering and Terrorism Financing Act for lawyers and public notaries (Croatian version only) (http://www.mfin.hr/adminmax/docs/Smjernice_ZSPNFT_odvjetnici_i_javni_bilježnici.pdf); d) guidelines of the Office for Money Laundering Prevention of the Ministry of Finance (Croatian version only) (http://www.mfin.hr/hr/zakoni-i-pravilnici); and e) latest general guidelines from Jul 2015: (http://www.mfin.hr/adminmax/docs/Opce%20smjernice%20FI_rev2015.pdf).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, the current AML/TF Act contains provision which required customer due diligence to be conducted in relation to all existing customers where risk assessment indicated that ML/TF risk existed within one year after the effective date of Act i.e. until 01 Jan 2010. Every active customer has to be identified and the identity verified in accordance with the Act and related regulations.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Croatia has not been the subject of a FATF Mutual Evaluation or IMF assessment exercise in the last three years, however the assessment of the implementation of anti-money laundering and counter-terrorist financing (AML/CFT) measures in Croatia was conducted by MONEYVAL. Please see Evaluation Report on Croatia (http://www.coe.int/t/dghl/monitoring/moneyval/evaluations/round3/MONEYVAL(2008)03Rep-HR3_en.pdf). Followed by the First Progress Report adopted on 18 Mar 2009 (http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/progress%20reports/MONEYVAL(2009)6ProgRep-HRV_en.pdf) and Second Progress report adopted on 13 Apr 2011(http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/Progress%20reports%202y/MONEYVAL(2011)4-ProgRep2HRV_en.pdf). The most recent MONEYVAL evaluation was conducted through an on-site visit from 17-23-NOV-2012 and the evaluation report on the 4th assessment visit to Croatia was adopted in Sep 2013: http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round4/CRO4-MERMONEYVAL(2013)15_en.pdf Link to mutual evaluation of Croatia, confirming Croatia is a member of MONEYVAL: http://www.fatf-gafi.org/countries/a-c/croatia/documents/mutualevaluationofcroatia.html

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, one-off transactions below HRK105,000 (approx. USD14,830) in total, whether carried out as a single operation or several linked transactions reaching the prescribed threshold. In addition, electronic money institutions from another Member State and branches of third-country electronic money institutions may be exempt from the obligation to carry out customer due diligence measures in the following cases: a) when issuing electronic money, if a single amount of a payment executed for the issuance of such money, on an electronic data carrier which may not be recharged, does not exceed the HRK equivalent of EUR150 (approx. USD160); and b) when issuing electronic money and dealing with electronic money, if the total amount of executed payments, stored on an electronic data carrier which may be recharged, does not exceed the HRK equivalent of EUR2,500 (approx. USD2,710) during a calendar year, except in the cases where the electronic money holder cashes the HRK equivalent of EUR1,000 (approx. USD1,090) or more during the same calendar year. Credit institutions may be exempt from the obligation to carry out the customer due diligence measures in the case of other products or transactions associated with them, which pose negligible ML/TF risks, provided they meet the conditions prescribed by an ordinance of the Minister of Finance. Insurance companies licensed for the performance of life insurance business, insurance companies from member-states with a business unit in Croatia or authorised to directly perform life insurance business in Croatia, pension companies, as well as legal entities and individuals performing business or activity of insurance representation or intermediation for entering into life insurance agreements may be allowed not to carry out customer due diligence in the following cases: a) contracting life insurance policies in which the individual premium instalment or several insurance premium instalments to be paid within one year does not exceed a total HRK equivalent amount of EUR1,000 (approx. USD1,090), or in cases when single premium payment does not exceed the HRK equivalent value of EUR2,500; and b) contracting pension insurances providing that types of insurance are being contracted whereby it is not possible to transfer the insurance policy to a third person or use it as collateral for a credit or loan, and a contract is entered into with a closed-end pension fund if the employer pays the contributions into the voluntary pension fund on behalf of the fund's members (no monetary threshold indicated). Institutions and persons may not be exempt from the obligation to carry out customer due diligence measures when there are grounds for suspicion of ML/TF with respect to a customer, product or transaction.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Identification and verification of an individual's identity is done through examination of the original customer's personal identification documents in the customer's presence (e.g. an ID Card for residents and a passport for non-residents). Individuals: a) full name and surname; b) permanent address; c) date of birth; d) place of birth; e) personal identification number; and f) name and number of the identification document, the name of the issuing authority. Legal entities: Verification of legal entities' information is done through examining documentation from court or other public register. The following data should be collected and verified: a) registered name; b) registered seat (street and number, place and country); c) business registration number; d) full name and surname, permanent address, date of birth place of birth, personal identification number, name and number of the identification document, the name of the issuing authority of a legal representative/person acting on behalf of a legal entity on the basis of Power of Attorney; and e) name and surname, permanent address, date of birth and place of birth of the beneficial owner. If there is any suspicion during the course of identifying the legal person and verifying the legal person's identity as to the veracity of data collected or credibility of the documents and other business documentation from which data was collected, the institution or person performing identification and verification shall ask the legal representative or the person authorised by power of attorney to give a written statement prior to establishing a business relationship or executing a transaction.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Identification and verification of an individual's identity is done through examination of the original customer's personal identification documents in the customer's presence. In case of legal entities, identification and verification is performed by examining an original or a notarised copy of documentation from court or other public register presented by the legal person's legal representative or person authorised by power of attorney. At the time of submission, the originals or the notarised copies of the required documentation must not be more than three months old. The legal entity's identity can be also identified and verified by gathering the required data through a direct examination of court or other public register. The copy of the excerpt from the register examined directly must be endorsed i.e., the examiner must put date, time, his/her name and surname. While verifying customer's identity, the institutions and persons performing identification and verification must first check the nature of a register from which data for the identity verification purposes are obtained. Identification and verification of the legal representatives of legal entities, persons who act on behalf of a legal entity on the basis of the Power of Attorney and representatives of the trust, foundations or NGOs is done thorough the examination of original personal identification documents of those persons in their presence. If the documents are insufficient to collect all prescribed data, the missing data are collected from other valid public document submitted by those persons i.e. from those persons directly. Beneficial owner's identification and verification is done by examining the originals or notarised copies of documents from a court or other public register not more than three months old at the time of their submission. If those documents are insufficient for collecting data on beneficial ownership, then examination of the original or notarised documents and other business documentation supplied by the legal representative or person authorised by power of attorney is performed or data is collected directly from a written statement given by the customer's legal representative or the person authorised by power of attorney.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The Croatian AML/FT Act defines beneficial owner as an individual who: a) ultimately owns or controls a legal entity through direct or indirect ownership or control of 25% plus one share of voting rights in that legal person, or otherwise exercises control over management of a legal person; b) with trust and foundations, a beneficial owner of 25% or more of the property rights of the legal transaction, or in whose main interest the transaction or legal person is set up or operates or who exercises control over 25% or more of the property rights of the legal transaction; or c) controls another natural person on whose behalf a transaction is being conducted or an activity performed. These individuals must be identified, and risk-based and adequate measures must be taken to verify their identities.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced/simplified due diligence arrangements are possible in respect of customers or products or transactions representing a low risk money laundering or terrorist financing risk except in instances when there are reasons for suspicion of money laundering or terrorist financing in relation to a customer or a transaction. This applies to relationships or transactions with the following: a) credit or financial institutions from the EU/EEA states or third countries considered as having equivalent AML/CFT systems to the EU (banks, savings bank, housing savings banks, Croatian Post, investment funds management companies, pension funds companies, financial instruments companies insurance companies who provide life insurance services); b) companies listed on a regulated market in the EU states or from the third countries which are subject to disclosure requirements consistent with the EU legislation; c) domestic public authorities and the public authorities of the EU; and d) persons who meet the conditions set forth by the Ordinance on the determination of conditions under which institutions and persons identify customers who pose a negligible risk in terms of money laundering or terrorist financing.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence measures and enhanced ongoing monitoring is required in any situation which due to the nature of the business relationship, the form and manner of transaction execution, business profile of the customer or other circumstances associated with the customer can present a greater risk of money laundering or terrorist financing. Three specific types of relationships where enhanced due diligence measures must be applied are: a) where the customer has not been physically present for identification and identity verification purposes; b) in respect of a correspondent banking relationship with respondents from non-EU/EEA states; or c) in respect of a business relationship with a PEP.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	In any transaction or business relationship with a PEP from a country other than Croatia ('a foreign PEP').

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Enhanced due diligence measures must be applied in respect to correspondent relationship with a bank or other credit institution from a third country (non-Member States of the EU/EEA) and the following additional data and documentation must be gathered in the process: a) the date of issuance and validity period of authorisation to provide banking services, and the name and seat of a competent third-country authority that issued the authorisation; b) a description of the implementation of internal procedures relating to ML/TF prevention and detection, particularly the procedures of customer identity verification, beneficial owner identification, reporting to the competent bodies on suspicious transactions and customers, record keeping, internal audit and other procedures that the bank or other credit institution adopted in relation to ML/TF prevention and detection; c) a description of systemic arrangements in the field of the ML/TF prevention and detection in effect in a third country in which the bank or other credit institution has its seat or in which it has been registered; d) a written statement confirming that the bank or other credit institution does not operate as a shell bank; e) a written statement confirming that the bank or other credit institution neither has business relationships with shell banks established, nor does it establish business relationships or conduct transactions with shell banks; and f) a written statement confirming that the bank or other credit institution falls under the scope of legal supervision in the country of its seat or registration, and that it is required to apply legal and other regulations in the field of the ML/TF prevention and detection in accordance with that country's effective laws. In order to establish new correspondent banking relationships, a prior written approval of a credit institution's senior management must be sought. In the context of enhanced due diligence, credit institutions must obtain the following additional documentation: a) a written statement that the correspondent bank or other credit institution has verified the identity of a customer and that it conducts ongoing due diligence of customers who have direct access to payable-through accounts, and b) a written statement that the correspondent bank or other credit institution can provide, upon request, relevant data obtained on the basis of due diligence of customers having direct access to payable-through accounts.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, they are specifically prohibited. Credit institutions are not allowed to establish or continue a correspondent relationship with a bank which operates or might operate as a shell bank or with another similar credit institution known to enter into agreements on opening and keeping accounts with shell banks.
Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	Non-face-to-face transactions and/or relationships are considered higher risk of ML/TF by the Croatian AML/TF Act and other relevant regulations. Where a customer has not been physically present for identification purposes, enhanced customer due diligence must always be performed. In such cases, institutions and persons covered by the Croatian AML/TF Act must apply one or more of the following supplementary enhanced due diligence measures: a) obtain additional documents, data or information on the basis of which the customer's identity shall be verified; b) additionally verify the submitted documents or additionally certify them by a foreign credit or financial institution; and/or c) apply a measure whereby the first payment within the business activity is carried out through an account opened in the customer's name with the given credit institution. Establishing a business relationship without physical presence of the customer is not permitted, unless a reporting entity applied those additional measures. Pursuant to the Croatian AML/TF Act credit and financial institutions are obliged to pay special attention to any ML and/or TF risk which may stem from new technologies enabling anonymity (Internet banking, ATM use, tele-banking, etc.) and put policies in place and take measures aimed at preventing the use of new technologies for the ML/or TF purposes. They must have policies and procedures in place for risks attached with a business relationship or transactions with non-face-to-face customers and to apply them at the establishment of a business relationship with a customer and during the course of conducting customer due diligence measures which include the supplementary measures described above.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	All suspicious activity reports should be sent to the Croatian Financial Intelligence Unit, Anti-Money Laundering Office: http://www.mfin.hr/en/anti-money-laundering-office
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 698 SARs GDP (in current prices): 2014 - USD 57,220 million (Source: data.worldbank.org[*]) This results in a ratio of 1 SAR for every USD81.97m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, besides an obligation to report suspicious transactions, there is an obligation to report to the Anti-Money Laundering Office on each transaction being conducted in cash totalling HRK200,000 (approx. EUR28,000 or USD30,430) and more immediately, and no later than within three days upon the execution of the transaction. The Act also mandates that a special attention is paid to all complex and unusually large transactions, as well as to each unusual transaction without an apparent economic or visible lawful purpose even when the reasons for suspicion of the ML/TF have not been detected. However if the reasons for suspicion are detected in relation to such transactions, they should be reported to the Office. In all instances when the customer seeks an advice from persons involved in the performance of professional activities on money laundering or terrorist financing, the persons involved in the performance of professional activities must immediately notify the Office thereof, and no later than within three business days from the date the customer sought for such an advice.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No, every suspicious transaction, irrespective of its value or execution manner must be reported.
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Yes, there are penalties prescribed by the AML/TF for failure to comply with reporting requirements ranging from HRK25,000 (approx. EUR4,000 or USD4,350) to HRK700,000 (approx. EUR100,000 or USD108,700) for legal entities. In addition, monetary fines ranging from HRK1,500 (approx. EUR200 or USD218) to HRK30,000 (approx. EUR4,000 or USD4,350) are envisaged for members of the management board or other legal persons responsible for non-compliance with reporting requirements.

^{*} GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No. Although the AML/TF Act imposes an obligation on the institutions and persons to establish an information system adequate to their respective organisational schemes, in order to provide the Anti-Money Laundering Office with prompt, timely and complete information as to whether or not they maintain or have maintained a business relationship with an individual or a legal entity, as well as to the nature of such a relationship, there is no requirement to use a specific AML/TF monitoring technology such as automated Suspicious Transaction monitoring technology.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes. The institutions or persons are required to refrain from conducting of a suspicious transaction and to notify the AML Office of such a transaction without any undue delay before executing the transaction, indicating the reasons for suspicion of money laundering or terrorist financing as well as the deadline within which the transaction is to be conducted. Only in exceptional circumstances the reporting entity can proceed with a current/ongoing transaction before notifying the Office, if the Office could not be notified due to the nature of the transaction or due to the fact that the transaction was not executed or for other justified reasons. Nevertheless, the reporting entity is obliged to report the Office subsequently, and no later than the next business day following the execution of such transaction.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	There are no provisions on monitoring transactions outside Croatia in the relevant AML/TF legislation.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No. Only a regular internal AML audit is required by the law.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Croatia has data protection laws in place. a) yes; b) no clear rules regarding corporate data; and c) yes; sensitive data is defined as information covering the racial or ethnic origin of the data subject, political opinions, religious or other beliefs of a similar nature membership of trade unions, physical or mental health or condition, sexual life and personal data regarding criminal and misdemeanour proceedings. In principle, such data cannot be processed, and derogation is tolerated under very specific circumstances. These circumstances include the data subject's explicit consent to process sensitive data, carrying out legal obligations to which personal data filing system controller is subject, or if the data subject discloses such data on his/her own. Such data has to be specifically labelled and protected. Therefore, any information assets (information systems, computers) that store or process sensitive data are also assigned a high level of protection. The additional protections of sensitive data are set forth in the Regulation on the manner of storing and special measures of technical protection of the special categories of personal data (Official Gazette, No. 139/04).
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	There is no specific reference in the law to the transfer of these reports for KYC purposes. However, any transfer of credit reports, criminal records and medical data should be done with strict observation of processing conditions set forth in the Personal Data Protection Act and other relevant data protection regulations e.g. credit reports transfer for credit risk analysis purposes to other credit institutions or to an institution established to collect and disseminate information on the creditworthiness of legal entities and individuals is not considered a violation of and secrecy obligations. Personal data contained in criminal records can only be processed under supervision of the competent authority. Medical record data must not be collected, processed or used without a prior written consent from a patient and can only be used for an in accordance with the purpose for which they were collected.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	EU case law on data protection (European Court of Justice cases) has applied to Croatia since 01 Jul 2013 (accession date) and may impact on the transfer of information.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes there is a bank secrecy section in the Credit Institutions Act and it is aimed at protecting the confidentiality of all information, facts and circumstances of which a credit institution becomes aware in the course of providing services to clients or in the course of business with individual clients. Banking secrecy obligations do not apply where confidential information is disclosed to the Anti-Money Laundering Office pursuant to the law governing the prevention of money laundering and terrorist financing.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Cyprus

Key contact: Chris Odysseos
Email: chris.odysseos@cy.pwc.com
Tel: +357 22 555 494

Postal address: PwC Central
43 Demostheni Severi Avenue,
CY-1080, Nicosia, Cyprus

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1996.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) Central Bank of Cyprus (www.centralbank.gov.cy); b) Cyprus Securities and Exchange Commission ("CySEC") (www.cysec.gov.cy); and c) Unit for Combating Money Laundering ("MOKAS") (http://www.law.gov.cy/law/mokas/mokas.nsf/index_en/index_en?OpenDocument).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The Institute of Certified Public Accountants of Cyprus ("ICPAC") has issued a Directive for the Prevention & Suppression of Money Laundering & Terrorist Financing Laws of 2007 and 2010 that serves as guidance to audit firms. The latest version was issued in Sep 2013.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last 3 years? If yes, please find a link to a relevant report (if publicly available).
A7.	Cyprus is being assessed by MoneyVal Council Of Europe. The latest report was released in September 2011 (http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round4/CYP4_Sum_MONEYVAL%282011%2902_en.pdf).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, occasional transactions under EUR15,000 whether the transaction is carried out in a single operation or in several operations which appear to be linked.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: should provide documentary evidence for their full name, date of birth, the address at which they can be located, their profession or occupation and specimen signature. An official document bearing a photograph of the person should be obtained. It is important that the current permanent address should be verified as it is an integral part of identity by requesting sight of a recent utility bill, local authority tax bill or bank or co-operative society statement, or making a credit reference agency search. Legal Entities: should provide documentary evidence of full name, registration address, a copy of the latest report and accounts, a copy of the certificate of incorporation/certificate of trade or equivalent, a copy of the company's Memorandum and Articles of Association and other certificates issued by the Registrar of Companies, a group structure to identify individuals who control over 10% of the entity's shares or voting rights, and the names of the directors. The identification of directors and beneficial shareholders is in line with the requirements for individual clients.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	The documents must be certified true copies of the originals.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Due diligence measures comprise identifying and verifying the identity of the beneficial owner owning or controlling more than 10% of the shares or voting rights of the client.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	According to paragraph 63-(1) of the Law: Simplified customer due diligence and identifications procedures can be used in respect of the following: a) credit of financial institution covered by the EU Directive or those who are situated in a country outside the European Economic Area which: a. in accordance with a decision of the Advisory Authority for Combating Money Laundering and Terrorist Financing, imposes requirements equivalent to those laid down by the EU Directive; and b. it is under supervision for compliance with those requirements; b) listed companies whose securities are admitted to trading on a regulated market in a country of the European Economic Area or in a third country which is subject to disclosure requirements consistent with community legislation; and c) Domestic Public Authorities of countries of the European Economic Area.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	According to paragraph 64-(1) of the Law: Enhanced due diligence measures should be in place in respect of the following customers: a) where the customer has not been physically present for identification purposes; b) in respect of cross-frontier correspondent banking relationships with current institutions to customers from third countries; and c) in respect of transactions or business relationships with politically exposed persons ('PEPs') residing in a country within the European Economic Area or a third country. According to paragraph 64-(2) of the Law: "Enhanced customer due diligence measures must be taken in all other instances which due to their nature entail a higher risk of money laundering or terrorist financing."
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	According to paragraph 5.61 of the Directive, if the prospective client is a PEP, the firm should obtain senior management approval for establishing business relationship. In addition, according to paragraph 4.55 of the Directive, the firm should establish the source of wealth and source of funds for PEPs and also conduct ongoing monitoring on the business relationship. Paragraph 5.62 of the Directive states that the firm should pay special attention when PEPs originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent to international standards. With regards to the issue of corruption, a useful source of information is the Transparency International Corruption Perceptions Index which ranks countries and territories based on how corrupt their public sector is perceived to be.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	According to 64 (b) of the Law, in respect of cross-frontier correspondent banking relationships with credit institutions to customers from third countries, it is required to: a) gather sufficient information about the credit institution customer to fully understand the nature of the business and the activities of the customer and to assess, from publicly available information, the reputation of the institution and the quality of its supervision; b) assess the systems and procedures applied by the credit institution customer for the prevention of money laundering and terrorist financing; c) obtain approval from senior management before entering into correspondent bank account relationships; d) document the respective responsibilities of the person engaged in financial or other business activities and of the credit institution customer; and e) with respect to payable-through accounts, it must be ensured that the credit institution-customer has verified the identity of its customers, and performed ongoing due diligence on the customers having direct access to the correspondent bank accounts and that it is able to provide relevant customers' due diligence data to the correspondent institution, upon request.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	If the client is a non-Cypriot resident who is not seen face-to-face, then a professional adviser in the client's home country could be used to confirm identity, or a copy of the passport authenticated by an attorney or consulate, or verification details covering true name, permanent address and verification of signature could be checked with a reputable credit or financial institution or professional advisor in the prospective client's home country.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	MOKAS: http://www.law.gov.cy/law/mokas/mokas.nsf/mokas02_en/mokas02_en?OpenDocument

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 – 828 SARs (Source: MOKAS) GDP (in current prices): 2013 – USD24,057.3m (Source: data.worldbank.org) This results in a ratio of 1 SAR for every USD29.1m of GDP.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	According to 6.05 of the Directive, any knowledge or suspicion of money laundering or terrorist financing should be promptly reported to MOKAS.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No, because according to paragraph 6.01 of the Directive for the Prevention & Suppression of Money Laundering & Terrorist Financing Laws of 2007 and 2010, the types of transactions which may be used by those exercising money laundering or terrorist financing are almost unlimited, it is difficult to define a suspicious transaction.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	According to the Law: "(27-(1)) A person who a) knows or reasonably suspects that another person is engaged in laundering or financing of terrorism offences; and b) the information on which that knowledge or reasonable suspicion is based, comes to his attention in the course of his trade, profession, business or employment shall commit an offence if he does not disclose the said information to the Unit as soon as is reasonably practicable after it comes to his attention. 27-(3) No criminal proceedings shall be brought against a person for the commission of the offences referred to in subsection (1), without the expressed approval of the Attorney General. 27-(4) An offence under this section shall be punishable by imprisonment not exceeding five years or by a pecuniary penalty not exceeding EUR5,000 or by both of these penalties."
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No. According to the Directive for the Prevention & Suppression of Money Laundering & Terrorist Financing Laws of 2007, paragraph 6.04, a firm might also consider monitoring the types of transactions and circumstances that have given rise to suspicious transaction reports by staff, with a view to updating internal instructions and guidelines from time to time. However there is no requirement to use automated Suspicious Transaction monitoring.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	According to paragraph 70 of the Law: "Persons engaged in financial and other business activities refrain from carrying out transactions which they know or suspect to be related with money laundering or terrorist financing before they inform the Unit of their suspicion. It is provided that, if it is impossible to refrain from carrying out the transaction or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the persons engaged in financial or other business activities, must inform the Unit immediately afterwards."
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Local legislation does not cover monitoring transactions outside Cyprus.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	In accordance with the Central Bank of Cyprus "Directive on a Framework of Principles of Operation and Criteria of Assessment of Banks' Organisational Structure, Internal Governance and Internal Control Systems of 2006 to 2012" ("the CBC Directive") banks should submit to the Central Bank of Cyprus a report prepared by external auditors/consultants every three years, on the assessment of the adequacy of the internal control System on an individual company as well as consolidated group basis. Under the CBC Directive, the external auditor/consultant assesses the internal control environment (including systems) with regard to the banks' management of the risk of money laundering and terrorism financing.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) the report must be provided every 3 years; b) the report is submitted by the external auditor/consultant to the Bank. The Bank is subsequently responsible for its submission to the Central Bank of Cyprus; c) under a financial statement audit, a bank's AML systems and controls are not explicitly reported on. During a financial audit, the procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, "the auditor considers internal controls that are relevant to the entity's preparation of financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control" (extract from the Independent Auditor's report as this has been approved by ICPAC).
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	Under the CBC Directive, it is not explicitly required for the external auditor/consultant to perform sample testing of KYC files and SAR reports, or to examine risk assessments. However, the external auditor/consultant may judge it necessary to perform such sample testing in the assessment of the Bank's internal control environment with regard to the management of the risk of money laundering and terrorism financing.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	a) yes, the Processing of Personal Data (Protection of the Individual) Law of 2001 as amended in 2003; b) the data protection law does not apply to corporate data as the definition of data subject does not include a company. Corporate data may be protected contractually by confidentiality agreements; and c) yes there is a separate definition of "sensitive data". Sensitive data means data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, participation in, association and trade union membership, health, sex life and sexual orientation, as well as on criminal charges or convictions. The collection and processing of sensitive data is prohibited. Any collection or processing of sensitive data requires the consent of the data subject, e.g. in order to go through with a contract with the consent of the data subject e.g. in employment contracts, insurance contracts etc.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	For KYC purposes the Law provides that the processor can process personal and sensitive data with the consent of the data subject. Personal data can be processed without the consent of the data subject in case that the processing is necessary in order for the processor to be in compliance with a law or regulation of the EU and in case the processing is necessary for the performance of a contract to which party is the data subject or to take steps at the request of the data subject prior to entering an agreement (s 5.) In addition, according to the Anti-Money Laundering Law in terms of processing of data: a) persons engaged in financial or other business must apply adequate and appropriate systems and procedures in relation to the identification and due diligence as to the customer in accordance with the provisions of this Law; and b) criminal records and medical data fall under the definition of sensitive data. As stated in question 29(c), the collections and processing of sensitive data is prohibited. However, under section 6(2), as mentioned above, there are some exceptions to this prohibition. Those exceptions include medical data and criminal records. Section (6)(2)(f) Medical data: processing of medical data is allowed when the processing of that data related to medical data and is executed by a person whose profession is to provide health services and who is subject to a duty of confidentiality or other related codes of conduct, provided that such processing is necessary for medical prevention, diagnosis, cure or management of health. Section 6(2)(g) Criminal data: processing of criminal records is allowed when such processing is concerned with the detection of offences, criminal convictions, security measures and investigation of mass destruction and is necessary to serve national need and national security, to serve the needs of forensic or correctional policy of the Republic or organisation or institution that is authorised for that purpose by the Republic.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Transfer of personal data within the EU is free. For a transfer to a third country, a license must be obtained from the Commissioner of Protection of Personal Data.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	The Data Protection Law applies here the same way as described above. The Banking Law 66(I)/1997 (as subsequently amended) allows a licensed credit institution to obtain information from their customers in order to open an account such as their identification i.e. name, identity number or passport number. All persons that work for the Central Bank and their representatives of the Central Bank auditors or experts are bound by the obligation of professional secrecy. The Central Bank may exchange information with the competent authorities of different Member States in accordance with this law and in accordance with other laws or instructions or regulation applicable to credit institutions by the EU like Article 31 and 35 of Regulation (EU) No 1093/2010.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Czech Republic

Key contact: Sirshar Qureshi
Email: sirshar.qureshi@cz.pwc.com
Tel: +420 2 5115 1235

Postal address: Hvězdova 1734/2c
140 00 Praha 4,
Czech Republic

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1996 (amended 2004, 2006 and 2008 - Act No. 253/2008 Coll. effective as of 1 September 2008) and last amended in Oct 2015 (http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/legislativa-aml-cft).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The key regulator for AML controls is: Ministry of Finance of the Czech Republic Financial Analytical Department ("FAU") (http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/stanoviska-financniho-analytickeho-utvar). Controls are also further performed also by (refer to Section 35 of the Act 253/2008 Coll.): a) Czech National Bank (www.cnb.cz) in accordance with Act No. 6/1993 Coll., on the Czech National Bank (http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/en/legislation/acts/download/act_on_cnb.pdf). The Czech National Bank is a supervisory authority of the financial market in the Czech Republic; and b) Czech Trade Inspectorate (www.coi.cz/en/) administrative authorities supervising lotteries and other similar games, and holders of licences to operate betting games.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, guidelines and methodical recommendations issued by the Ministry of Finance (http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/stanoviska-financniho-analytickeho-utvar). Guidelines also issued by Czech National Bank (http://www.cnb.cz/cs/dohled_financni_trh/legislativni_zakladna/legalizace_vynosu/metodiky_vyklady.html).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, the Czech National Bank stipulates in Decree No. 281/2008 Coll. (as amended by Decree No. 129/2014 (http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/en/legislation/decrees/decrees_281_2008.pdf)), that financial and credit institutions should implement the risk based approach when assessing the risk of legitimisation of proceeds of crime and financing of terrorism. The institutions should take into consideration the best practices applied in this area. Furthermore, the Czech National Bank issued its official ruling on 26/05/2009 in which it specifies the respective AML standards: http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/legislative/vestnik/2009/download/v_2009_08_21109560.pdf
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	MONEYVAL assessment Apr 2011: http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Czech_en.asp

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, any single transaction below EUR15,000 does not require any customer due diligence unless it is a: a) a suspicious transaction; b) an agreement to enter into a business relationship; c) an agreement to establish an account, to make a deposit into a deposit passbook or a deposit certificate, or to make any other type of deposit; d) an agreement to use a safety deposit box or an agreement on custody; e) a transaction with a PEP; and f) as part of the business relationship.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The following information is required: Individuals: Name, surname, birth identification number or date of birth, place of birth, sex, address and citizenship. These would normally be verified by an identity card or passport. Individuals who conduct business: In addition to the above, full name of the business, place of business and identification number needs to be noted. Legal entities: the full name, residency/seat, identification (or similar identification received from foreign offices) showing evidence of the company's existence (i.e. certificate of incorporation, trade register statement or other). The same principles for individuals apply for the identification of individuals in the company's statutory body. If the company's statutory body or the owner is another legal entity, identification documentation must also be collected for that entity.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	These should be certified by an appropriate person e.g. a notary, local authorities etc. Specific rules apply to credit and financial institutions, where certain employees are authorised to verify these when opening account, concluding contract etc.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The shareholders of a legal entity (with more than 25% holding) must be ascertained. Identification requirements are the same as for the relevant legal entity.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence is applicable for a transaction exceeding EUR1,000 unless it is a: a) suspicious transaction; b) an agreement to enter into a business relationship; c) an agreement to establish an account, to make a deposit into a deposit passbook or a deposit certificate, or to make any other type of deposit; d) an agreement to use a safety deposit box or an agreement on custody; e) a life insurance contract, should the customer have a right to pay extra premiums above the agreed limit of the one-off or regular premiums payments; f) a purchase or receipt of cultural heritage, items of cultural value, used goods or goods without a receipt of origin to further trade in such goods, or receipt of such items in pawn; or g) withdrawal of the final balance of a cancelled bearer passbook.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence is applicable for: a) a remote financial services agreement under the Civil Code; b) a transaction and business relationship with a PEP; and c) a correspondent bank relationship with a foreign credit or similar institution ("Correspondent Institution").

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Legislation requires financial institutions to: a) have sufficient procedures to determine whether the customer is a PEP who is a resident of another country; b) obtain approvals from senior management on a daily basis for establishing business relationships with such customers; c) take reasonable measures to gather information about the sources of income and funds that are involved in the business relationship or transaction; and d) continuously monitor the business relationship.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	All transactions with PEPs are subject to due diligence including the provision of information and supporting documentation relating to: a) the purpose and intended nature of the transactions or business relationship; b) the beneficial owner, if the client is a legal entity; c) the information required for continuous monitoring of the business relationship; and d) a review of the income source.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In the case of a remote financial services agreement under the Civil Code, the entity shall review the customer as follows: a) the first payment under this agreement shall be made via an account kept in the customer's name held at a credit institution or a foreign credit institution operating in the European Union ("EU") or the European Economic Area ("EEA"); and b) the customer shall submit to the entity a copy of a document verifying the existence of this account together with copies of the relevant parts of his identity card and at least one more identification document to validate the customer's identification data of this card i.e. the type, serial number, issuing country or institution and validity.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Ministry of Finance of the Czech Republic Financial analytical department ("FAU") (Guidance how SAR must be made: http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/oznameni-podezreleho-obchodu).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 3,192 SARs GDP (in current prices): 2014 – USD205,269.7m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD64.3m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Suspicious transactions are identified based on criteria such as unusual transactions, international wire transfers etc. However, no special report is required.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, penalties are described in detail in Section 43 to 53 of the Act No. 253/2008 Coll.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No, however, transaction monitoring should be performed by using adequate means which assumes use of some automated technology.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes, in general a transaction that is identified/reported as suspicious can be continued after 24 hours from the time when it has to be notified and received by the Ministry of Finance, unless the Ministry of Finance postpone the transaction.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No. However, if the external auditor during performance of the regular audit procedures finds out facts which indicate suspicion of committing economic crime, crime against property or crime of corruption, he is obliged to inform the FAU, statutory representatives and control body of the given bank thereof. The central bank is however authorised to ask the bank to appoint the auditor for review of their internal control system which might also include a review of the AML function if requested by the central bank.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	If such a request is made by the central bank, it covers a selected year of operations and the report is due by the end of Feb of the next year. The auditor provides this report to the bank and the bank delivers the report to the central bank. This review is done independent to the financial statement audit and may even be done by a different auditor.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	Such report is focused primarily on internal controls as defined by the Basel Committee on Banking Supervision best practice, however it would also include a compliance review with the key legal requirements. No sample testing or risk assessment examination is required.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes. Czech Act No. 101/2000 Coll. on Data Protection ("Data Protection Act") (https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107&p1=1107) governs the area of personal data protection: a) yes; b) corporate data, i.e. data that relate to legal entities, not the natural persons do not fall under the category "personal data" protected under the Data Protection Act; c) yes, the Data Protection Act stipulates a separately protected category of personal data. It is forbidden to process personal data on racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in political parties or political movements, trade union membership and data concerning health or sex life.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Generally, the consent regarding the transfer of data must comply with requirements in the Article 4 letter n) and Article 5 par. 4 of the Data Protection Act. Furthermore, the criminal records and medical data are also considered as the sensitive data according to the Article 4 letter b) of the Data Protection Act. The sensitive data may be transferred only with the consent or instruction of the subject of the data together with other requirements of the Article 9 letter a) of the Data Protection Act. For further details please see the above mentioned provisions of the Data Protection Act (https://www.uoou.cz/en/vismo/zobraz_dok.asp?id_ktg=1107&p1=1107).
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Transfers of personal data outside EEA and EU have been recently affected by the decision of No. C-362/14 Maximilian Schrems v. Data Protection Commissioner from 06 Oct 2015 of the Court of Justice of the European Union cancelling the Safe Harbor Regime. As a result, the Czech Office for Personal Data Protection recommends to use standard contractual clauses according to the Commission decision No. 2010/87/EU from 05 Feb 2010 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF) and/or Binding Corporate Rules (http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm) to govern the transfer of information to the US.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes, the general business secrecy is stipulated in the Act No. 89/2012 Coll., the Civil Code, and specific bank secrecy is stipulated in the Act No. 21/1992 Coll., on banks. Bank secrecy means keeping confidential all the information and documents on matters relating to the client of the bank that is not publicly accessible. In particular, information on transactions, account balances and deposit balances. The bank is obliged to keep this information confidential and protected from disclosure, misuse, damage, destruction, loss or theft. Information and documents on matters that are protected by bank secrecy cannot be disclosed to third parties without the prior written consent of the client. There are also other types of confidentiality prescribed by the relevant laws, such as attorney-client confidentiality, medical confidentiality, auditor confidentiality.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Denmark

Key contact: Sofus Emil Tengvad
Email: ste@pwc.dk
Tel: +45 3945 3619

Postal address: Strandvejen 44,
DK 2900 Hellerup,
Denmark

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1993 (significant amendments in 2006, 2008, 2009, 2010, 2012 and 2013).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) The Danish FSA (http://www.finanstilsynet.dk); b) The Danish FSA (http://www.finanstilsynet.dk); and c) Business Registry Authority (http://www.erst.dk/), Lawyer: The Danish Bar and Law Society (http://www.advokatsamfundet.dk).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	A Danish general guidance is issued by the Danish FSA (http://www.finanstilsynet.dk/da/Temaer/Hvidvask/Regler.aspx). Furthermore, the Danish Business Authority has issued guidance for specific sectors e.g. accountancy sector (https://www.retsinformation.dk/Forms/R0710.aspx?id=146481).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, all customers need to be verified according to the regulation, new customers as well as old customers.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	A risk based approach is allowed in accordance with law. However, the actual approach has to be approved as being consistent with the AML regulations.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The latest report of this nature is the follow up report to the Mutual Evaluation of Denmark dated Oct 2010 (http://www.fatf-gafi.org/countries/d-i/denmark/documents/follow-up-report-to-the-mutual-evaluation-of-denmark.html).

Customer due diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	As the main principle customer due diligence always applies. However, transactions below EUR6,700 may be exempted from part of the due diligence requirements pursuant to the current regulation and guidelines. A potential exemption from the customer due diligence requirement must be based upon a risk assessment and must comply with all statutory requirements.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: name, address and social security number. Accepted evidence includes: passport, driving license, birth certificate, tax returns and tax code (including social security number). In addition electronic public keys (NEM-ID) can function as a supporting document if it is presented together with one or more of the primary documents. Corporates: name, address and company number. Accepted evidence includes: registered information from the Danish Commerce and Companies Agency and Articles of Association.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	There are no mandatory requirements in the law, but it is stated in local guidance that copies of identification documentation are accepted. Copies of documentation can be certified by financial institutions according to the law.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The beneficial owners must be identified by identification information (primary documents for identification is accepted, ref. A.9). The group structure or ownership of a group has to be identified as well as shareholders who own more than 25% of a company.

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Customer due diligence is reduced in three main areas: a) payments for life insurance or under pension agreements under specific circumstances e.g. payments of EUR1,000 or less for recurring fees and a one-time fee of EUR2,500 or less; b) electronic money - if the device cannot be recharged and the maximum amount stored in the device is no more than EUR250, or where, if the device can be recharged, a limit of EUR2,500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR1,000 or more is redeemed in that same calendar year; and c) specific transactions and products as described by the Danish Financial Services Agency ("FSA") in order no. 712 of 2008.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Local guidance states four cases: a) customers who do not physically present themselves for identification purposes; b) cross-border correspondent banks; c) PEPs; and d) shell companies.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Legislation requires financial institutions to: a) have sufficient procedures to determine whether the customer is a PEP who is a resident of another country; b) obtain approvals from senior management on a daily basis for establishing business relationships with such customers; c) take reasonable measures to gather information about the sources of income and funds that are involved in the business relationship or transaction; and d) continuously monitor the business relationship.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	In cases of money transfers to or from a bank outside the European Union ('EU') where there is no official agreement of financial services with the EU, further proceedings have to be considered as stated in the local guidance. Before establishing new correspondent banking relationships, firms will be required to: a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine, from publicly available information, the reputation of the institution and the quality of supervision; b) assess the counterparty's AML and anti-terrorist-financing controls; and c) obtain daily approval from senior management.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In the case of a customer who has not been physically present for identification purposes, legislation requires the taking of 'further measures to ascertain the customer's identity'. It sets out an illustrative list of measures that can be taken to ascertain the customer's identity in these situations, such as: a) ensuring that the customer's identity is established by additional documentation; b) checking or verifying the documents supplied, or requiring a confirmatory certification by another financial institution; and c) requiring that the first payment in connection with the transactions is carried out through an account opened in the customer's name with a bank.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The Danish Money Laundering Secretariat hosted by the State Prosecutor for Serious Economic Crime (http://www.anklagemyndigheden.dk/Sider/hvidvask.aspx).
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 7,250 SARs GDP (in current prices): 2014 – USD342.0m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD47.2m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Any suspicion (that has not been disproved) of a potential violation of the regulation on money laundering and terrorist financing, has to be reported immediately to the relevant authorities.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	The de-minimis threshold for reporting is set to situations where suspicion relates to offenses punishable by imprisonment of less than a one year. The threshold referred to is not the possible sentencing in the particular case, but the maximum penalty for the accused criminal offense. In practice, the de-minimis threshold is of minor importance, and rarely applies (all suspicions related to offenses punishable by imprisonment of more than one year have to be reported).
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Any penalties will be handled by the State Prosecutor for Serious Economic Crime. In certain cases this can be up to six months imprisonment.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Companies must have administrative procedures in place. Financial companies are considered to be operating in a high risk sector and therefore automatic monitoring of transactions is required by the Danish FSA.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No. In certain situations however, the authorities can issue a temporary order to freeze transactions from being executed. In addition, the EU regulations applies to transactions involving sanctioned individuals.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes: a) yes, the definition of "personal data" will likely cover material held for KYC purposes (please see link below); b) the act on processing of personal data does not apply to corporate data (please see link below); and c) there are no specific definitions of "sensitive data" in the Danish act on processing of personal data. However, sections 6-8 defines three different categories of information: normal personal information (6), sensitive personal information on private matters (7) and other types of information on private matters (8) (please see link below). http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes, the information contained in such reports are subject to the protection of information in the Danish act on processing of personal data.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	This would have to be evaluated by a lawyer.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Estonia

Key contact: Viljar Kähari
Email: viljar.kahari@ee.pwclegal.com
Tel: +372 614 1858

Postal address: Advokaadibüroo
PricewaterhouseCoopers Legal OÜ
Pärnu mnt 15. Tallinn EE10141 Estonia

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2008 (initial legislation was adopted in 1999).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The Estonian Financial Intelligence Unit is the main supervision unit (https://www.politsei.ee/en/organisatsioon/rahapesu-andmeburoo/). The Estonian Financial Supervision Authority also regulates banks, management companies etc.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The Estonian Financial Intelligence Unit: https://www.politsei.ee/en/organisatsioon/rahapesu-andmeburoo/fius-advisory-guidelines/ The Estonian Financial Supervision Authority: http://www.fi.ee/index.php?id=3375
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, EC Moneyval expert committee 4th cycle of assessment, in which important FATF Recommendations have been re-assessed (not a full assessment against the FATF 40 Recommendations and 9 Special Recommendations but an update on major issues in the AML/CFT system). The evaluation report was published in November 2014: http://www.coe.int/t/dghl/monitoring/moneyval/

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Due diligence measures are always required upon establishment of a business relationship and upon suspicion of money laundering or terrorist financing (regardless of any limits provided by law). Otherwise, there is a EUR15,000 threshold for transactions (regardless of whether one or several related payments); EUR6,400 upon provision of currency exchange services; EUR2,000 for organisers of games of chance, regarding all persons who pay or receive more than that in a single transaction or several related transactions.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	An obligated person shall identify a natural person (face-to-face) and verify the person on the basis of an identity document. In addition to an identity document, the representative of a person participating in a transaction shall submit a document in the required format, certifying the right of representation. An obligated person shall identify a legal person and its passive legal capacity and verify the information obtained. Legal persons registered in Estonia and branches of foreign companies registered in Estonia shall be identified on the basis of an extract of a registry card of the relevant register. Foreign legal persons shall be identified on the basis of an extract of the relevant register or a transcript of the registration certificate or an equivalent document which has been issued by a competent authority or body not earlier than six months before submission thereof.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	A copy shall be made of the page of an identity document submitted for identification which contains the personal data and a photograph. In addition, upon identification and verification the following personal data shall be registered: a) the name and the representative's name; b) the personal identification code or, upon absence of a personal identification code, the date and place of birth; c) the name and number of the document used upon identification and verification of persons, and its date of issue and the name of the agency which issued the document; and d) the name of the document used upon identification and verification of the right of representation, and its date of issue and the name of the issuer. In certain cases the address of the place of residence and the profession or area of activity of the person shall be registered. A representative of a legal person of a foreign country shall, at the request of an obligated person, submit a document certifying his or her powers, which has been notarised or authenticated pursuant to an equal procedure and legalised or authenticated by a certificate substituting for legalisation (apostille), unless otherwise prescribed by an international agreement.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Identification of the beneficial owner is a part of due diligence measures, it includes gathering information about the ownership and control structure of a legal person, trust, civil law partnership or other contractual legal arrangement on the basis of information provided in pre-contractual negotiations or obtained from another reliable and independent source.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence measures can be undertaken if a person participating in a transaction entered into it in economic or professional activities or a person using a professional service or a customer is: a) a legal person governed by public law founded in Estonia; b) a governmental authority or another authority performing public functions in Estonia or a contracting state of the EEA; c) an authority of the European Community; d) a company of a contracting state of the EEA or a third country, which is subject to requirements equal to those provided for in Estonian legislation and whose securities are traded in a regulated securities market in one or several contracting state of the EEA; and e) a credit institution or a financial institution, a credit institution or a financial institution located in a contracting state of the EEA or in a third country, which in the country of location is subject to requirements equal to those provided for in Estonian legislation and the performance of which is subject to state supervision. An obligated person may apply the simplified due diligence measures with regard to the beneficial owners of an official account opened by a notary public or enforcement officer of a contracting state of the EEA or third country, provided that the official account is subject to due diligence measures which are in compliance with the international standards for prevention of money laundering and terrorist financing, state supervision is exercised over adherence to these requirements and the notary public or enforcement officer has and preserves information about the identity of the beneficial owner. An insurer or insurance broker may take simplified due diligence measures if: a) a life assurance contract is made whereby the annual assurance premium does not exceed EUR1,000 or a single premium does not exceed EUR2,500; b) a pension insurance contract is made which does not provide for the right of withdrawal or cancellation and which cannot be used as loan collateral; and c) a transaction is entered into in the framework of a superannuated pension scheme or another scheme allowing for such pension benefits whereby insurance premium is debited from wages and the terms and conditions of the pension scheme do not allow for assignment of the rights of a participant in the scheme. An electronic money institution may take simplified due diligence measures if an electronic money device does not allow for reloading and the amount saved in one electronic money device does not exceed EUR250. Credit and financial institutions supervised by Estonian Financial Supervision Authority may identify the client via electronic Estonian Identification Card if the value of the transaction(s) do not exceed EUR2,000 on a monthly basis. Simplified due diligence measures may also be applied in a transaction if all of the following conditions have been fulfilled: a) a written contract has been entered into with a customer for an indefinite period; b) a payment is made through the account of a customer or a person participating in a transaction, which has been opened in a credit institution or a branch of a foreign credit institution registered in the Estonian commercial register or in a credit institution which has been registered or has its place of business in a contracting state of the EEA or in a country where requirements equal to those provided for in Estonian legislation are in force; c) the obligated person has established by rules of internal procedure beforehand that the annual total value of performance of financial obligations arising from transactions of such type does not exceed the maximum limit of EUR15,000; and d) the obligated person registers at least the data specified in A10 with regard to a customer. Certain other criteria exist for applying simplified due diligence measures for public/state institutions (both local and foreign).

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	a) if the nature of a situation involves a high risk of money laundering or terrorist financing; b) if a person participating in a transaction, in a professional operation, or using a professional service; or a customer has been identified and verified without being present at the same place as the person or customer; c) if upon identification or verification of a person suspicion arises regarding the truthfulness of the data or authenticity of the documents submitted or regarding the identification of the beneficial owner or beneficial owners; and d) if a subject is a politically exposed person of a contracting state of the European Economic Area or a third country or their family member or close associate.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	Upon establishment of a business relationship with or entry into a transaction with or performance of a professional operation for or provision of professional services.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The regular due diligence measures shall be applied more frequently than usually. Additionally, the following requirements must be implemented: a) appropriate risk-based internal procedures for making a decision on establishment of a business relationship or entry into a transaction applied; b) the management board or a person or persons authorised by the management board shall decide on establishment of business relationships; and c) upon establishment of a business relationship and entry into a transaction, appropriate measures taken for identification of the origin of the money or other property used. Also at least one of the following enhanced due diligence measures shall be undertaken: a) identification and verification of a person on the basis of additional documents, data or information, which originates from a reliable and independent source or from a credit institution or a branch of a credit institution registered in the Estonian commercial register or from a credit institution which has been registered or has its place of business in a contracting state of the EEA or in a country where requirements equal to the Estonian legislation are in force, and if in such credit institution the person has been identified while being present at the same place as the person; b) application of additional measures for the purpose of verifying the authenticity of documents and the data contained therein, among other things, demanding that they be notarised or officially authenticated or confirmation of the correctness of the data by the credit institution which issued the document; and c) making the first payment relating to a transaction through an account opened in the name of a person or customer participating in the transaction in a credit institution which has its place of business in a contracting state of the EEA or in a country where requirements equal to those provided for in Estonian legislation are in force. Also enhanced due diligence measures shall be undertaken upon opening a correspondent account with a credit institution of a third country and during the period of validity of the respective contract, thereby regularly assessing the following: a) based on public information, the nature of the economic activities and the trustworthiness and reputation of the credit institution of the third country and the effectiveness of supervision exercised over the credit institution; and b) the control systems of the credit institution of the third country for prevention of money laundering and terrorist financing. The contract serving as the basis for opening a correspondent account or the rules of procedure of the credit institution shall contain the obligations of the parties: a) upon application of due diligence measures for prevention of money laundering and terrorist financing, including with regard to a customer having access to a payable-through account or another similar account; b) upon submission, on the basis of a query, of data gathered in the course of identification of customers and verification of submitted information; and c) upon preservation of data and upon performance of the notification obligation and application of other measures for prevention of money laundering and terrorist financing. Prior consent of the management board of the credit institution or financial institution or the person authorised by the management board is required for opening a correspondent account for a credit institution or a financial institution of a third country or for opening a correspondent account in a third country credit institution or financial institution or for signing the corresponding contract. Credit institutions and financial institutions are prohibited to open or hold a correspondent account in a credit institution, which meets at least one of the following conditions: a) the actual place of management or business of the credit institution is located outside its country of location and the credit institution is not part of the consolidation group or group of undertakings of a credit institution or financial institution that is subject to sufficient supervision; b) an account for a credit institution corresponding to the characteristics specified in clause 1) has been opened in the credit institution; and/or c) according to international standards or the circumstances provided for in this section, which are to be used as a basis for assessment, deficiencies become evident in the trustworthiness of the executives of the credit institution and in assessment of measures for prevention of money laundering and terrorist financing.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	No, Estonian law does not regulate such situations. However, every person must take all necessary steps to avoid money-laundering activities taking place.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Always, in the case of a person participating in a transaction, in a professional operation, or using a professional service; or a customer has been identified and verified without being present at the same place as the person or customer.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting	
Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	To the Estonian Financial Intelligence Unit: https://www.politsei.ee/en/organisatsioon/rahapesu-andmebuuro/
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 11,204 SARs (from which 252 cases were forwarded for further investigation and 20 criminal proceedings initiated) (Source: https://www.politsei.ee/dotAsset/448124.pdf) GDP (in current prices): 2014 - USD26,485m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD2.3m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	An obligated person, except a credit institution, shall immediately, but no later than within two working days of executing the transaction, notify the Financial Intelligence Unit of any transaction where a financial obligation exceeding EUR32,000 is performed in cash, regardless of whether the transaction made is a single payment or several related payments. A credit institution shall immediately, but no later than within two working days of executing the transaction, notify the Financial Intelligence Unit of any currency exchange transaction exceeding EUR32,000 in cash, unless the credit institution has a business relationship with the person participating in the transaction.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Both failure to report suspicion of money laundering or terrorist financing and submission of incorrect information as well as unlawful notification of information submitted to the Financial Intelligence Unit are offences punishable by a fine up to EUR1,200 or detention (for individuals) or up to EUR32,000 (for legal persons).
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	The obligated person has the right to refuse to enter into such a transaction, and they shall immediately, but no later than within two working days from identifying the act or circumstances, or from the rise of the suspicion, notify the Financial Intelligence Unit.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	Yes. External auditors must inform the Estonian Financial Supervision Authority if they find out that a credit institution materially violates Estonian law.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes: a) yes; b) corporate data is not protected under the data protection laws; and c) yes, sensitive personal data is: a. data revealing political opinions or religious or philosophical beliefs, except data relating to being a member of a legal person in private law registered pursuant to the procedure provided by law; b. data revealing ethnic or racial origin; c. data on the state of health or disability; d. data on genetic information; e. biometric data (above all fingerprints, palm prints, eye iris images and genetic data); f. information on sex life; g. information on trade union membership; and h. information concerning commission of an offence or falling victim to an offence before a public court hearing, or making of a decision in the matter of the offence or termination of the court proceeding in the matter. Additional protections for sensitive personal data ("SPD"): a) written explicit consent has to be obtained from data subject; b) a person responsible for protection of personal data needs to be appointed or the processing of sensitive personal data registered with the Data Protection Inspectorate; and c) processing SPD for communication to third persons for assessing the creditworthiness or other such purpose is not permitted.
Q30.	Are there any prohibitions on the (a) transfer of credit reports (for KYC and credit risk analysis purposes), (b) criminal records (for KYC and crime prevention purposes) and (c) medical data (for KYC and pension benefits purposes)?
A30.	There is a general principle that the processing of personal data is permitted only with the consent of the data subject unless otherwise provided by law. The consent shall clearly determine the data for the processing of which permission is given, the purpose of the processing of the data and the persons to whom communication of the data is permitted, the conditions for communicating the data to third persons and the rights of the data subject concerning further processing of his or her personal data. Silence or inactivity shall not be deemed to be consent. Consent may be partial and conditional: a) in such case the person communicating personal data has to establish the legitimate interest of the third person, verify the accuracy of the data to be communicated and register the data transmission; b) written consent of the data subject needs to be obtained; and c) written consent of the data subject needs to be obtained.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes, under Article 88 of the Credit Institution Act generally all data and assessments which are known to a credit institution concerning the clients of the credit institution or other credit institutions are deemed to be information subject to banking secrecy. However, the following data are not deemed to be information subject to banking secrecy: a) data which are public or available from other sources to persons with a legitimate interest; b) consolidated data on the basis of which data relating to a single client or the identities of persons included in the set of persons referred to in the consolidated data cannot be ascertained; c) a list of the founders and shareholders or members of a credit institution and data relating to the sizes of their holdings in the share capital of the credit institution, regardless of whether or not they are clients of the credit institution; and d) information relating to the correctness of the performance of a client's obligations to a credit institution.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Finland

Key contact: Ake Turunen
Email: ake.turunen@fi.pwc.com
Tel: +358 40 515 0804

Postal address: Itamerentori 2,
FIN-00180 Helsinki,
Finland

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2008 Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008) - last amended Jan 2016 (Original 1998, amended 2003). 2013 Act on Freezing of Assets to Combat Terrorism (325/2013). 1889 Criminal Code (39/1889) - last amended in 2015 on the part of Terrorist Financing.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	In general, previous AML laws followed previous European Union ("EU") directives.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) Financial Supervisory Authority (http://www.fin-fsa.fi); b) Financial Supervisory Authority (http://www.fin-fsa.fi); and c) Ministry of the Interior and Regional State Administrative agencies.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes. Guidance is provided by the Money Laundering Clearing House of Finland which operates within the National Bureau of Investigation ("NBI") (https://www.poliisi.fi/en/national_bureau_of_investigation).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, following a risk-based assessment.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The latest Mutual Evaluation report was in 2007. Please see link: http://www.fatf-gafi.org/topics/mutualevaluations/documents/mutualevaluationoffinland.html The latest follow-up report was in 2013. Please see link: http://www.fatf-gafi.org/countries/d-i/finland/documents/finland-fur-2013.html

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	There is no minimum Euro threshold for taking customer due diligence measures. Customer due diligence must be followed when transactions are unusual. Due diligence must take place if one of the following is true: a) if the reporting entity is planning to engage in a permanent business relationship with a customer; b) if the transaction or transactions related to the same business amounts to EUR15,000 or more and the relationship between the reporting entity and a customer is occasional; c) if the customer is a gambling service provider; d) if the transaction is suspicious or the reporting entity is suspecting that the money related to the transaction is used to finance terrorism; or e) if the reporting entity is questioning the reliability of the information previously used to identify the customer.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Full name, date of birth, identification number (for foreign citizens: citizenship and passport number). Required documents for individuals: passport, driving licence or official identity card. Legal entities: Name, business identification number, date of registration (and name of registration authority), field of activity as well as full name, date of birth and citizenship of members of the statutory bodies and the person(s) representing the legal entity. Required documents for legal entities: trade register extract or equivalent official extract from a relevant public register and relevant documents for the individuals previously mentioned.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	A certified copy signed by two qualified individuals is required. The qualified individual does not have to be a notary, lawyer or accountant.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The name, date of birth and identification number of the beneficial owner(s) (for foreign citizens, citizenship and passport number) must be verified.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced/simplified due diligence arrangements are available if the risk of money laundering or the financing of terrorism connected to the customer, product, service or field of activity is low. For example, simplified due diligence arrangements are available to: a) Finnish authorities; b) public companies listed on the Finnish or any other European Economic Area (“EEA”) country exchange; c) credit institutions; d) financial institutions; e) investment firms; f) management companies/custodians; and g) insurance companies with concession in Finland or another EEA country.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence measures are required if there is a high risk of money laundering or the financing of terrorism in connection to the customer, product, service or field of activity. Enhanced due diligence is also required if the transaction is connected to a state in which systems for preventing and clearing money laundering does not meet international standards.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	Additional due diligence is required if the customer himself is a PEP or is related to a PEP, or is an individual who is known to be the business partner of a PEP.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Firstly, the management of the credit institution has to approve the correspondent banking relationship. Should it be approved, the credit institution has to collect sufficient information about the correspondent bank which includes evaluating the bank's reputation, the quality of its supervision and the correspondent bank's measures to prevent money laundering and the financing of terrorism.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	No.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Additional due diligence is always required if the customer is not physically present for identification.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Money Laundering Clearing House of Finland, which operates within the NBI (https://www.poliisi.fi/en/national_bureau_of_investigation).
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 - 23,062 SARs (which included 558,699 transactions) GDP (in current prices): 2014 - USD272,216.6m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD11.8m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	If customers do not provide the information required for performing customer due diligence or if parties subject to the reporting obligation consider that the information provided is not reliable, the parties must make a suspicious transaction report. A suspicious transaction report must also be made if legal persons cannot be identified or their beneficiaries cannot be established in a reliable way, or if enhanced identification of the person for whom a customer is acting is not possible.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes: a) violation of customer due diligence: fine, unless a more severe punishment for the act is provided elsewhere in the law; b) registration violation: fine, unless a more severe punishment for the act is provided elsewhere in the law; c) violation of the obligation to report money laundering: fine; or d) payment service violation: fine, unless a more severe punishment for the act is provided elsewhere in the law.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	a) yes, the definition of personal data covers any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household; b) the definition of personal data also covers personal information in the corporate context; and c) yes, "sensitive data" is defined as personal data related to or intended to be related to for example race or ethnic origin, the social, political or religious affiliation or trade-union membership of a person, a criminal act, punishment or other criminal sanction, the state of health, illness or handicap of a person or the treatment or other comparable measures directed at a person, the sexual preferences or sex life of a person or the social welfare needs of a person or the benefits, support or other social welfare assistance received by the person. As a main rule, the processing of sensitive data is prohibited but Finnish law provides certain detailed derogations from the prohibition.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes, there are prohibitions on the transfer of such personal data.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes, EU Data Protection Directive 95/46/EC and legislation based on the implementation of the said Directive apply when personal data is transferred from another EU country. If the information is transferred from outside of the EU, local legislation may be applicable. Personal Data Act (523/1999) is applicable on personal data and as special legislation may be applicable, for example Act on the Protection of Privacy in Working Life (759/2004), Employment Contracts Act (55/2001), Act on Cooperation within Undertakings (725/1978), Occupational Safety and Health Act (738/2002) Credit Data Act (527/2007) and other legislation.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes, under the Credit Institutions Act. Bank secrecy protects private individuals, undertakings and other corporations and it applies to information that can be used for identifying a bank's customer. For example, information related to a customer's economic status or an individual's personal circumstances concerning information such as family relations. Business or professional secrets are also subject to regulation.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



France

Key contact: Nicolas Montillot / Sébastien d'Aligny /
Ludivine Gimet
Email: nicolas.montillot@fr.pwc.com /
sebastien.daligny@fr.pwc.com / ludivine.gimet@fr.pwc.com
Tel: +33 (0) 1 56 57 75 65

Postal address: Crystal Park; 63 rue de Villiers;
92208 Neuilly-sur-Seine Cedex;
France

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Fully revised with the transposition of the third AML Directive dated 30 Jan 2009 (The 4 th Directive was in Jun 2015 and will be transposed into French law).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) Autorité de Contrôle Prudentiel et de Résolution ("ACPR") (http://acpr.banque-france.fr/en/acpr.html); b) Autorité des Marchés Financiers ("AMF") (and ACPR if the subsidiary of a bank) (http://www.amf-france.org/en_US/?langSwitch=true); and c) Autorité de Régulation des Jeux en ligne ("ARJEL") (http://www.arjel.fr/) for online games, casinos etc. and DGCCRF: Direction générale de la concurrence, de la consommation for real estate agents.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, guidelines have been provided by ACPR on various topics: a) business relationships and occasional customers; b) beneficial ownership; c) third party introduction; d) exchange of information within a group and non-group; e) reporting suspicious activity; f) politically exposed persons; g) wealth management; h) equivalent third countries; and i) suspicious reports to FIU. Application principles have been published on the ACPR website relating to: a) collective investment schemes; b) correspondent banking; c) transfer of funds; d) insurance sector; and e) insurance third party introduction. Guidelines have been provided by AMF for entities subject to its control (asset management companies and management companies, financial investment advisers, central security depositaries): a) obligation of vigilance in a risk based approach and conditions for implementation of obligation to report to Tracfin; b) Politically Exposed Persons ("PEPs"); c) conditions for implementing specific legislative and regulatory provisions; d) beneficial ownership; and e) third party introduction. Sources of practical guidance includes: a) (http://acpr.banque-france.fr/en/prudential-supervision/amlcft-anti-money-laundering-and-counter-terrorist-financing.html); b) (http://www.amf-france.org/en_US/Reglementation/Doctrine/Doctrine-list/Doctrine.html?category=III+-+Providers&docId=workspace%3A%2F%2FSpacesStore%2Fc59ace50-a95b-4f9e-990f-6433f6405808&docVersion=1.3&langSwitch=true); c) (http://www.economie.gouv.fr/tracfin); d) (http://www.fbf.fr/fr/environnement-europeen-et-international/lutte-anti-blanchiment/_875GT2&Count=8); and e) (http://www.arjel.fr/-Textes-de-reference-.html).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	No. Each institution must implement a risk-based approach which defines the required due diligence depending on the money-laundering risks. Regulation provides examples of low and high risk customers, products, transactions and means of distribution but these lists are not exhaustive. Each institution must define its own risk mapping of customers, products, transactions and means of distribution and the associated due diligence required. This risk-based approach is not approved by the local regulator(s) but periodically examined during on site reviews.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The anti-money laundering and countering the financing of terrorism (AML/CFT) measures in place in France were evaluated by the FATF in 2010. This was updated in Oct 2012: http://www.fatf-gafi.org/topics/mutualevaluations/documents/mutualevaluationoffrance.html

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes. The identification of occasional customers and beneficial owners is not required for transactions under EUR15,000 (and EUR1,000 for remitter) if the transaction is not deemed suspicious. However, this threshold is not applicable for money transfers, custody services when the client is not physically present. The decree of 28 Feb 2013 provides that under certain conditions, the identification of customers and beneficial owners may not be checked for online operations under EUR250 or for a total of EUR2,500 in one year. The decree of 07 May 2013 provides that for money transfers, information concerning the customer and the beneficial owner must be reported to Tracfin (see A18) for transactions over EUR1,000 or which cumulate over EUR2,000 on a calendar month.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: a government-issued document with a photograph (such as a valid passport or a valid photocard driving licence), supporting documents of home address at the date when the documents are collected, occupation, revenues or any other relevant documents which enable the client's resources and his personal assets to be assessed Legal entities: original or certified copy of any deed or extract of an official register stating the company name, address, legal status and identity of the executives, annual reports of the last 3 years and auditors' reports.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Individuals: Original identification documentation must be provided. A bank's employee is required to make a copy of the original documentation and certify it true to the original. Legal entities: Except in the specific case of the presentation of a certified copy of a deed or extract of an official register stating the name, legal form and registered office, original documentation should be provided and a copy shall be made and certified by the bank's employee.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The institution shall identify the effective beneficiary of the business relationship through any means it considers adequate and necessary. It should verify that this identity is based on the documents collected, according to the assessed level of money laundering risk and the documentation shall be kept on record: (https://acpr.banque-france.fr/en/acpr.html)

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Due diligence may be reduced when the money laundering risks associated with a given customer and/or business relationship are considered as low. Low risk customers include: a) financial institutions subject to equivalent AML regulation; b) large corporates whose shares are listed on a regulated stock-exchange incorporated in an EU-country or an equivalent third-party country; and c) public administrative bodies or authorities of an EU country. Low risk products include life insurance contracts with an annual premium under EUR1,000 or with a unique premium under EUR2,500. Furthermore, the decree of 28 Feb 2013 provides that under certain conditions, the identification of customers and beneficial owners may not be checked for online operations under EUR250.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence measures are required in the following cases: a) when the client or his representative is not physically present for the account opening; b) when the client is a Politically Exposed Person; c) when the transaction or the financial instrument facilitates the anonymity of the client; d) when the transaction is carried out by individuals who live or corporates which are incorporated in non-cooperative countries; and e) when the transaction is complex, of an unusual amount or without obvious justification.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Enhanced due diligence is systematically required for non-resident PEPs (with the fourth directive resident PEP will be concerned)
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Institutions must: a) collect sufficient information on its correspondent banking relationships' activities and assess, based on publicly available information, its reputation; b) assess its anti-money laundering arrangements; c) ensure that the decision of establishing this relationship has been approved by an executive of the institution; d) include in the correspondent-banking agreement the requirements to provide the institution with information on demand; and e) ensure that the correspondent-banking counterparty has checked the identity of its clients when the institution has opened accounts which are directly used by the correspondent-banking clients for their own transactions. Guidelines have been provided by the ACPR on the requirements around correspondent banking relationships: http://acpr.banque-france.fr/fileadmin/user_upload/acp/publications/registre-officiel/201303-ACP-Principes-d-application-sectoriels-sur-la-correspondance-bancaire.pdf

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Regulation requires institutions to systematically conduct enhanced due diligence for non face-to-face transactions and/or relationships.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Tracfin (Traitement du renseignement et action contre les circuits financiers clandestins): http://www.tracfin.bercy.gouv.fr/

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 - 38,419 SARs (34,268 in the Financial Sector and 2,447 in the Non-Financial Sector) (Source: Tracfin annual report) GDP (in current prices): 2013 – USD2,829,192m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD73.6m of GDP.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes: a) operations which are particularly complex, an amount which appears to be unusually high or does not appear to have any economic justification, where the bank is unable to establish the identity of the beneficiary or obtain sufficient information regarding the origin and destination fund, the commercial background or the legality of a transaction; b) transactions for which the identity of the originator or the beneficiary could not be established; and c) for money transfers, transactions over EUR1,000 operations or which cumulate EUR2,000 on a calendar month.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	There is no explicit legal or regulatory requirement to use automated ST monitoring technology. Regulation only sets out that the bank shall implement the processes and the tools which it considers necessary to proceed with the AML/CFT surveillance, considering its size, organisation, customers and transactions.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes, the transaction is on "hold" until Tracfin approval is received.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes. If it concerns a country of the European Union or a country which imposes equivalent rules to France with regard to the fight against Money Laundering and Terrorist Financing.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No, but regulation relating to internal control provides that the AML policy should be described and communicated to the audit committee. In addition, a questionnaire is completed on an annual basis concerning AML internal control set up for the ACPR.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	In France, personal data is protected by the law on data processing, data files and individual liberties dated 01 Jan 1978: a) yes; b) corporate data include personal data concerning individuals representing legal entities. The collection and processing of these data are provided in the French law. These data can be collected and transferred for AML purposes (e.g. power of attorney, delegation of authority, identity of directors, officers and shareholders); and c) under French law, sensitive data is any personal data that reveals directly or indirectly racial or ethnic origins, political, philosophical or religious opinions, trade union membership or data related to individual health or sexual life. The collection of sensitive data is prohibited. By exception, sensitive data can be collected with the explicit consent of the person concerned or if the treatment of such data is required for public interest purposes.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Credit reports are protected by banking secrecy rules under French law. Credit reports may be transferred in the following circumstances: a) tax fraud; b) AML/CFT; c) transmission of information to the French authorities (e.g. French financial market authority, Banque de France); and d) exchange of information between regulated entities belonging to the same group. Criminal records are protected under French law and cannot be transferred. By exception, criminal records can be transferred to certain authorities listed by the French criminal Code (ministry of justice, military authorities etc.). Medical data is protected under French law and can be transferred only in particular circumstances provided by the law, for the interest of the patient or for public health purposes.

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Under French law, the transfer of information is governed by: a) the law on data processing, data files and individual liberties dated 06 Jan 1978; and b) the rules related to banking and professional secrecy. These rules aim at protecting the transfer of information and limit it to specific cases.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation?) If so, what data is subject to regulation?
A32.	There is a bank secrecy law in France. This law does not precisely list the data covered by banking secrecy.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Germany

Key contacts

Lars-Heiko Kruse / Oliver Eis

Email: lars-heiko.kruse@de.pwc.com /

oliver.eis@de.pwc.com

Tel: +49 30/2636-2006/ +49 69/9585-3935

Postal address: Kapelle-Ufer 4

D-10117 Berlin; Germany

Friedrich-Ebert-Anlage 35-37

60327 Frankfurt/Main

Last updated:

January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1993 (amended 2003, 2008, 2011, 2014, 2015).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	According to section. 16 of the German Anti Money Laundering Act: a) Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin) (www.bafin.de); b) BaFin, Federal Ministry of Finance ("BMF") (http://www.bundesfinanzministerium.de); and c) Decentralised regulation, communal supervision in each of the sixteen states of Germany e.g. Hessen (http://www.hessen.de/irj/RPDA_Internet?cid=bed0fee03852d9e5286ceb90870b2356).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Guidance for the non-financial services sector on federal state level, for example Hessen (http://www.hessen.de/irj/RPDA_Internet?cid=bed0fee03852d9e5286ceb90870b2356). Guidance for the banking and financial services industry (federal level) (http://www.die-deutsche-kreditwirtschaft.de/die-deutsche-kreditwirtschaft/kontofuehrung/geldwaescheverhinderung.html). This guidance is recognised by BaFin as a regulatory requirement for the banking and financial services industry.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	In accordance with Section 3 paragraph 1 number 4 of the German Anti Money Laundering Act, all client files need to be reviewed and updated on the basis of a risk based approach in appropriate intervals. The files of high risk clients should be reviewed every year, medium risk clients at least every seven years and low risk clients at least every ten years. Alternatively, institutions can also choose to continuously update their files based on trigger events (e.g. undelivered mail, changes of client contact details, missing KYC data).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The most recent report was undertaken in 2010 (http://www.fatf-gafi.org/topics/mutualevaluations/documents/mutualevaluationofgermany.html). The last follow-up report on this Mutual Evaluation was undertaken in 2014 (http://www.fatf-gafi.org/publications/mutualevaluations/documents/follow-up-report-germany-2014.html).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, one-off transactions below EUR15,000 (in total, German Anti-Money Laundering Act), foreign currency cash transactions below EUR2,500 (in total, German Banking Act) and transfer of funds below EUR1,000 (Regulation (EC) 1781/2006).
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Evidence of identity has to be provided by documentary evidence. The physical or electronic record of the individual should contain the full name, address, place and date of birth and nationality. Documentary evidence can be a valid national identity card (ID Card) or a passport, diplomatic passport, passport replacement papers or a resident permit. Exceptions for minors (birth certificate) and elderly/disabled persons (expired documents permitted). Corporates listed in a public register: The physical or electronic record of the institution should contain company, trading name, legal form, commercial register number, the address of its registered office or head office and the names of the members of its representative body or of its legal representative. If a member of its representative body or the legal representative is a legal person, information shall be collected on that legal person's company, partnership or trading name, legal form, commercial register number if available and the address of its registered office or head office. Evidence of identity has to be provided by a certificate of public registration, e.g. commercial register. Corporates not listed in a public register (partnership): The physical or electronic record of the institution should contain company, partnership name, legal form, commercial register number if available, the address of its registered office or head office and the names of the members of its representative body or of its legal representative. If a member of its representative body or the legal representative is a legal person, information shall be collected on that legal person's company, partnership or trading name, legal form, commercial register number if available, and the address of its registered office or head office. Evidence of identity has to be provided by a partnership agreement. In addition, the partners have to be identified like individuals (ID Card, passport).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Individuals and Corporates: In general, the physical presence of the individual (identification document: ID Card/ passport including a photograph of the individual) or an authorised representative of the corporate (identification document: copy of the register) is required. The identity of the individual is then verified by the employee of the bank. Verification for corporates is also done by the bank's employees via accessing commercial registers and similar data bases. The institution may engage third parties in order to fulfil the due diligence requirements, but shall remain ultimately responsible for fulfilling the due diligence requirements. The mentioned third parties include other credit institutions, financial services institutions, lawyers, notaries, auditors and tax advisers, insurance companies and also the German Mail ("Post Ident Verfahren"). They are permitted to carry out the customer identification. Further, the institution can also delegate customer identification process to another person on the basis of a contractual arrangement.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	A "beneficial owner" is any natural person who ultimately owns or controls the contracting party, or the natural person on whose behalf a transaction is ultimately carried out or a business relationship is ultimately established. The term "beneficial owner" includes, in particular: a) in the case of corporate entities that are not listed on an organised market and are not subject to transparency requirements with regard to voting rights consistent with Community laws, or are not subject to equivalent international standards, any natural person who directly or indirectly holds more than 25% of the capital stock or controls more than 25% of the voting rights; b) in the case of foundations with legal capacity and legal arrangements used to manage or distribute assets or property on "Treuhand", or through which third parties are instructed with the management or distribution of assets or property, or similar legal constructs: a. any natural person acting as settlor or who otherwise exercises control over 25% or more of the assets or property; b. any natural person who has been designated as the beneficiary of 25% or more of the managed assets or property; c. where the natural person intended to be the beneficiary of the managed assets or property is yet to be designated, the group of natural persons for whose benefit the assets or property are primarily intended to be managed or distributed; and d. any natural person who otherwise directly or indirectly exercises a controlling influence on the management of assets or property or the distribution of income; and c) in the case of a party acting on behalf of another, the other person. Where contracting parties act as "Treuhänder", they are deemed to be acting on behalf of another. Documentary evidence has to be provided for the identification of a beneficial owner on the basis of a risk-based approach. At a minimum, the name of the beneficial owner must be recorded and further identification is to be gathered depending on the level of risk of money laundering or terrorist financing in the individual case. Verification of the beneficial owner is risk-based. The guidance of the German Banking industry ("DK – Hinweise") contains examples on how to determine the beneficial owner for different types of entities.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced/ simplified due diligence arrangements are possible in case of a identified low money laundering or terrorist financing risk. This applies to transactions by or for the benefit of and upon establishing business relationships with credit or financial institutions or listed companies in the European Union ("EU") or in an equivalent third country and domestic and foreign ("EU") authorities. Simplified due diligence measures include identification/ verification, and in the case of business relationships, continuously monitoring the business relationship. The scope of measures to verify identity and to monitor may be reduced as appropriate. Also, establishing the identity of the beneficial owner in the case of escrow accounts of lawyers, notaries or other independent legal professionals in Germany, the EU and equivalent third countries can be waived, provided that the institution where the account is held can obtain, on request, information on the identity of the beneficial owner from the holder of the escrow account. The German Banking Act also contains a list of products that are considered low risk (life insurance, leasing).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence ("EDD") is required where there is a high risk of money laundering or terrorist financing. This generally applies to transactions/ business relationships with PEPs (customer or beneficial owner) and non-face-to-face customers/ transactions. Non face to face customers (individuals only): Where the contracting party is a natural person and is not physically present for identification purposes, the Institution shall verify the contracting party's identity by means of a copy of the identification document certified by a notary public or public administrator and using the electronic identification function of the national ID Card or a qualified digital signature. The Institution then must also ensure that the first transaction into the account is carried out directly from a payment account held in the name of the contracting party with an institution within the European Economic Area ("EEA") or with a credit institution domiciled in an equivalent third country. Where factual circumstances or ratings given by national or international agencies justify the assumption that a higher risk exists in other cases, particularly in connection with a certain country, the competent authority ("BaFin") issues circulars requiring institutions to enhance their monitoring of a transaction or business relationship, particularly the origin of the assets or property contributed by a client who resides in such a country and used in the business relationship or transaction, and to fulfil additional risk-adequate due diligence and organisational requirements. The latest circular is Circular 8/2014 (Nov 2014). Also, transactions and client relationships assessed by the institution to bear a higher money laundering / terrorist financing risk, or where the company is engaged in activities that generally bear a higher money laundering risk, these will require further verification and/or monitoring, e.g. clients conducting complex transactions, cash intensive businesses or clients in less transparent jurisdictions.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	For PEPs, EDD is as follows: the establishment of a business relationship is subject to the approval of a superior, adequate measures shall be adopted to determine the origin of the assets or property to be used in the business relationship or transaction and the business relationship shall be subject to enhanced continuous monitoring.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	In the case of correspondent banks based in EU member states or member states of the Basel committee, it should be ensured that a banking license exists. For banks in third countries, EDD is required. The Institution should: - obtain sufficient publicly available information about the correspondent institution and its business and management structure in order to be able to understand fully, both before and during such a business relationship, the nature of the business operations conducted by the correspondent institution and assess its reputation and controls for combating money laundering and terrorist financing as well as the quality of its supervision; - lay down and document the respective responsibilities of both institutions with regard to compliance with the due diligence standards before establishing such a business relationship; - ensure that, before such a business relationship is established, the employee in charge obtains the approval of his/her immediate superior or the next highest management level; - take measures to ensure that the correspondent institution does not establish or maintain a business relationship with a credit institution of which it is known that its accounts are used by a shell bank; and - take measures to ensure that the correspondent institution does not permit transactions via payable through accounts.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Non face-to-face customers (individuals only): In case the contracting party is a natural person and is not physically present for identification purposes, the Institution shall verify the contracting party's identity by means of a copy of the identification document certified by a notary public or public administrator and use the electronic identification function of the national ID Card or a qualified digital signature. The Institution then must also ensure that the first transaction into the account is carried out directly from a payment account held in the name of the contracting party with an institution within the EEA or with a credit institution domiciled in an equivalent third country.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	According to Section 10 and 11 of the German Anti Money Laundering Act, SARS must be made to the local prosecution unit of the relevant state and to the Financial Intelligence Unit ("FIU") of the Federal Criminal Police Office as the central agency. Link to FIU: http://www.bka.de/sid_26E5CB6B4BF97CA6CE5E70B53C60ECD1/DE/ThemenABisZ/Deliktsbereiche/GeldwaescheFIU/geldwaesche_node.html?_nnn=true Guidance on how to make a SAR can be found in BaFin Circular 1/2014: http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1401_gw_verwaltungspraxis_vm.html
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 24,054 SARs (FIU Annual Report 2014) GDP (in current prices): 2014 - USD3,852,556.2m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD160.2m.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Institutions must report suspicious activities, whenever factual circumstances exist that indicate that the assets or property connected with a transaction or business relationship are the product of money laundering or are related to terrorist financing. They must promptly report such transactions, irrespective of the amount involved, or such business relationships to the Financial Intelligence Unit of the Federal Criminal Police Office and the competent prosecution authorities orally, by telephone, fax or via electronic data transmission. The reporting obligation exists as well where factual circumstances indicate that the contracting party failed to comply with their duty of disclosure as to whether or not they are acting on behalf of a beneficial owner.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimise thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Yes, section. 17 I no.14/15 of the German Anti Money Laundering Act outlines the fines for failing to file a report correctly, completely, in due time or at all or disclosing information on a SAR to the instructing party or any third party. Those administrative offences may be punishable by a fine of up to EUR100,000.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Yes, according to sec. 25 h II of the German Banking Act (“KWG”). The Guidance of the German banking industry specifies the requirements for monitoring systems (adequacy, rules, administration rights, database, etc.).

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes, according to sec.11 of the German Anti Money Laundering Act. A requested suspicious transaction may not be executed before the public prosecutor's office has informed the institution of its consent to proceed, or before the expiry of the second working day following the transmission date of the SAR unless the transaction's execution was prohibited by the public prosecutor's office. In this respect Saturday shall not be considered a working day. If it is impossible to postpone the transaction, or if doing so could frustrate efforts to pursue the beneficiaries of a suspected criminal offence, the execution of the transaction shall be permitted and the suspicious transaction report must be filed subsequently without undue delay.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes, see sec. 29 II German Banking Act and sec. 26 and 27 PrüfbV (German Audit Regulation) for details. The AML system of banks and financial institutions is part of the annual audit and the report contains information on the MLRO, monitoring systems, risk assessments, SARs and customer due diligence / simplified due diligence / enhanced due diligence. An additional questionnaire provided by BaFin must be answered (giving “grades” to the different elements of the AML system) and submitted along with the report.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) annually or bi-annual (depending on balance sheet total); for institutions within the 2 year audit cycle, the AML questionnaire must be submitted annually; b) the regulator ("BaFin"); and c) yes.
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) yes; b) yes; and c) yes.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	a) yes; b) the focus of the German Data Protection Act is mainly on individuals (natural persons); however in the German Telecommunication Act, certain information about certain legal persons (e.g. PLCs) is protected; and c) all personal data is considered sensitive data. Additionally sensitive data is considered data about ethnic and racial origins, political opinion, religious or philosophical views, union affiliations, health and sex life.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	No, explicit prohibitions exist, as AML has precedence, however all transferred information must be in line with the Data Protection Act. For example, criminal records will only be requested from a person applying for a job if that job is senior management or requires a special level of reliability as there needs to be a valid reason to request that sensitive information.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No express Banking Secrecy Act exists, but case law acknowledges the existence of banking secrecy and thus banks are only required to disclose information about their customers if not doing such would itself break the law. Obligations to confidentiality extend to other professions as well (e.g. lawyers or a notary public).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Gibraltar

Key contact: Isabel Tellez
Email: Isabel.tellez@gi.pwc.com
Tel: +350 20066842 Ext 108

Postal address: International Commercial Centre,
Casemates Square,
Gibraltar

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1996 (amended in 2005 and 2007).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The Gibraltar Financial Services Commission ("FSC"): http://www.fsc.gi
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, the Anti-Money Laundering and Terrorist Financing Guidance Notes: http://www.fsc.gi/amlgn/
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, only for clients of Banks and Fiduciary service providers licensed by the FSC.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, amendments introduced and applicable from 15 Dec 2007.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, one-off transactions below EUR15,000.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Physical identity (e.g. name, date of birth, registration number), address and the source of their income/wealth. Passports or identity cards should be used for verification of physical identity and utility bills or alternatives, such as checking the electoral register/telephone directory, should be used for verification of address. Companies: Copy of the latest report and accounts, board resolution to open the relationship and the empowering authority for those who will operate any account and certificate of incorporation/certificate of trade or equivalent. Also required are authorised signatories for the account/transaction, holders of powers of attorney to operate the account/transaction as well as ultimate beneficial owners ("UBOs") and shareholders if different from the UBOs.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Where verification of identity is required, the documents should be independently verified by the institution itself. High risk customers should have their identification, address and source of income/wealth verified using at least two independent sources other than the document in question. Certified documents must be signed and dated by an external third party, such as a notary, lawyer, accountant etc.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	It is considered appropriate to verify the identity of beneficial owners holding 25% or more. Where a principal owner is another corporate entity or trust, the firm should take measures to look behind that entity and establish the identities of its beneficial owners or trustees, unless that company is publicly quoted. The firm will then judge which of the beneficial owners exercise effective control, and whose identities should therefore be verified.

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	The level of documentation required should be adapted according to the risk profile of the customer, the level and nature of the business, the risk tolerance of the institution and any existing relationships with that customer. Local guidance requires that institutions have a methodology which classifies the different types of customers into risk categories and processes that adequately mitigate the risks posed by these.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Where an entity is known to be linked to a Politically Exposed Person, or to a jurisdiction assessed as carrying a higher money laundering / terrorist financing risk, or where the company is engaged in activities that are assessed to carry a higher money laundering risk, further verification and/or monitoring may be required.

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	The systems of control that firms must adopt to reduce the risks associated with establishing and maintaining business relationships with PEPs include: a) establishing and documenting a clear policy and internal guidelines, procedures and controls regarding such business relationships; b) maintaining an appropriate risk management system to determine whether a potential customer or an existing customer is a PEP; c) ensuring that decisions to enter into business relationships with PEPs are only taken by senior management; and d) ensuring that business relationships which are known to be related to PEPs must be subject to proactive monitoring of the activity on such accounts.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The following controls amongst others need to be implemented for correspondent banking relationships: a) a firm must gather sufficient information about a respondent institution to fully understand the nature of their business; b) senior management approval must be obtained prior to establishing new correspondent relationships; and c) the firm must assess the respondent institution's AML and terrorist financing controls.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	The additional controls required in respect of non face-to-face customers are: a) ensuring that the customer's identity is established by additional documents, data or information; b) supplementary measures to verify the documents supplied, or requiring an eligible introducer to certify the customer identification documents; and c) ensuring that the first payment of the operation is carried out through an account in the customer's name at a credit institution. A common mechanism adopted by many firms is to permit the use of certified customer identification documents provided in lieu of having had sight of the originals.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Gibraltar Financial Intelligence Unit, which is a member of the Egmont Group.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	There are three offences that could be committed by an individual: a) assistance; b) tipping off; and c) failure to file a SAR.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.
Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	a) Yes the relevant legislation is the Data Protection Act 2004 ("DPA"); b) The definition of personal data as defined by the DPA is "any information relating to a data subject" and so it does cover material likely to be held for KYC purposes. It does not however, apply to corporate data which is not personal data (e.g. financial data about a company); and c) Yes, Section 8(1) of the Act defines "Sensitive data" as: a. data revealing racial or ethnic origin; b. data revealing political opinions; c. data revealing religious or philosophical beliefs; d. data revealing trade-union membership; e. data concerning health or sex life; f. data concerning the commission or alleged commission of any offence by the data subject; g. data concerning any proceedings for any offence committed; or h. alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. The additional protection for the processing of sensitive personal is that processing sensitive personal data is prohibited save where sections 6 and 11 on data quality and data security are satisfied and at least one of the conditions in section 7(1) (criteria for making data processing legitimate) is met, and at least one of the following conditions is met: a. the data subject has explicitly consented to the processing of the sensitive personal data; b. the processing is necessary for the purposes of carrying out any legal obligation or right which is conferred or imposed by law on the data controller in connection with employment and the right of data subjects to privacy is safeguarded; c. the processing is necessary to prevent injury or other damage to the health of the data subject or another person or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where consent to the processing cannot be given by or on behalf of the data subject; or the data controller cannot reasonably be expected to obtain such consent, or the processing is necessary to prevent injury to, or damage to the health of, another person, or serious loss in respect of or damage to, the property of another person, in a case where such consent has been unreasonably withheld; d. processing is carried out in the course of the data controller's legitimate activities, in accordance with appropriate safeguards for the rights and freedoms of data subjects, and subject to such requirements as may be prescribed, by a non-profit-seeking body with a political, philosophical, religious or trade-union aim on condition that (i) the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes, and (ii) the sensitive data is not disclosed to third parties without consent of the data subject; e. the information contained in the data has been made public as a result of steps deliberately taken by the data subject; f. the processing is necessary (i) for the administration of justice, (ii) for the performance of a function conferred on a person by or under an enactment, or (iii) for the performance of a function of the Government or a Minister of the Government; g. the processing (i) is required for the purpose of obtaining legal advice or for the purposes of, or in connection with, legal proceedings or prospective legal proceedings, or (ii) is otherwise necessary for the purposes of establishing, exercising or defending legal rights; h. the processing of the sensitive data is required for the purposes of preventive medicine, medical diagnosis, the provision of medical care or treatment, medical research or the management of health-care services, and the sensitive personal data are processed by a person registered under the Medical and Health Act 1989, who is under an enforceable obligation of professional secrecy, or by another person who, in the circumstances, owes a duty of confidentiality to the data subject; i. the processing is necessary in order to obtain information for use, subject to and in accordance with the Statistics Act, only for statistical, compilations and analysis purposes; j. the processing is carried out by political parties, candidates for election to, or holders of, elective political office in the course of electoral activities for the purpose of compiling data on political opinion on condition that the sensitive data is not disclosed to third parties, in a form which permits identification of the data subject, without consent of the data subject; k. the processing is necessary for the purpose of the assessment, collection or payment of any tax, duty, levy or other moneys owed or payable to the Crown and the data has been provided by the data subject solely for that purpose; l. the processing is necessary for the purposes of determining entitlement to or control of, or any other purpose connected with the administration by the Crown of any benefit, pension, assistance, allowance, supplement or payment, or any non statutory social security scheme; or m. the processing is authorised by regulations that are made by the Minister and are made for reasons of substantial public interest.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes, relevant UK case law provides legal precedent.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Greece

Key contact: Andreas Riris
Email: andreas.riris@gr.pwc.com
Tel: +30 210 6874 646

Postal address: 268 Kifissias Avenue,
GR-152 32 Athens,
Greece

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1995 (main amendments in 2005, 2006 and 2008).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The Regulators for AML controls are the public authorities ("Competent Authorities") which supervise the compliance of obliged persons with the provisions of the Greek AML legislation. The Competent Authorities are: a) The Bank of Greece for: credit institutions, leasing companies, factoring companies, bureaux de change, payment institutions, credit companies, electronic money institutions and postal companies, only to the extent that they act as intermediaries in funds transfers and in co-operation with the Ministry of Transport and Communications and the National Telecommunications and Post Commission, insurance companies, insurance intermediaries, undertakings other than credit institutions whose business is to acquire participations and carry out similar activities; b) The Hellenic Capital Market Commission for: portfolio investment companies in the form of a societe anonyme, management companies of mutual funds, management companies of mutual funds investing in real estate, management companies of mutual funds for venture capital, investment firms, investment intermediary firms, venture capital firms and companies providing business capital; c) The Accounting and Auditing Standards Oversight Board for chartered accountants and audit firms; d) The Ministry of Economy and Finance (General Directorate of Tax Audits) for: tax consultants, tax-accountants and related firms, independent accountants and private auditors; real estate agents and related firms; auction houses, dealers in high value goods, auctioneers, and pawnbrokers; e) The Gambling Control Commission of law 3229/2004, as in force, for: casino enterprises, casinos operating on ships flying the Greek flag, companies, organisations and other entities engaged in gambling activities, and betting outlets; f) The Ministry of Justice for notaries and lawyers; g) The Ministry of Development for the natural or legal persons providing services to companies and trusts (trust and companies service providers); and h) for branches in Greece of financial institutions which have their registered office abroad, the competent authority shall be the corresponding authority responsible for domestic financial institutions conducting activities similar to those of such foreign financial institutions.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The Competent Authorities have issued Interpretative Circulars, Decisions and Regulatory Acts, each one giving instructions and interpretations of the AML provision to the obligated persons under their supervision. The Competent Authorities through such Decisions / Acts have the power to modify the obligations laid down in the Greek AML legislation for the Obligated Persons.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Greek AML legislation states that obligated persons may apply, at the appropriate time, risk-based due diligence measures to both new and existing customers. Decisions of the competent authorities may determine the criteria and the method of application of due diligence to existing customers.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The most recent evaluation was undertaken in 2011: http://www.fatf-gafi.org/countries/d-i/greece/documents/follow-upreporttothemutualevaluationreportofgreece.html

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes. In principle, occasional (one-off) transactions below EUR15,000; a lower threshold of EUR1,000 per insurance contract per year (or of EUR2,500 in the case of a one-off payment). The law also caters for a lower threshold option in relation to electronic funds transfers depending on the decision and guidance provided by the respective regulatory authority.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: For identifying individuals, a police identity card or passport plus any other document that provides evidence of his/her residential and business address, as well as his/her profession and tax registration number. Legal Entities: Most recent legal documentation as defined by Greek law depending on the type of entity, identifying: a) business name, address and purpose of the entity; b) representation and signing authorities of the entity; c) any changes and amendments on the statutes of the entity and/or its representatives; d) police identity cards or passports of the legal representative(s) of the entity as well as evidence of their current residence; e) tax registration number; and f) Beneficial Owner(s). Notwithstanding the above, and specifically for credit and financial Institutions, the Bank of Greece Governor's Act No. 2652/29.2.2012 and article 68 para.7 of L. 4174/2013, as in force, determined that the customer's income shall be verified through the customer's income tax clearance form or, in the case of legal persons, the income tax returns filed (including confirmation of their filing that includes the tax payable), with the exception of the cases where the customer is exempted from the obligation to file income tax returns in accordance with the relevant provisions of the Income Tax Code, as in force.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Copies of identification documents may be certified by a state authority, a notary public or a lawyer. Copies may also be certified by an authorised employee of a financial institution upon presentation of the originals. In specific for the obligated persons under the supervision of the Hellenic Capital Market Commission ("HCMC") it has been recently decided that the certification documents of their clients which have been categorised as high risk and having a capital for investment exceeding the amount of EUR75,000 should be authenticated by a public authority, or an EU bank, or other bank of a country applying the FATF recommendations (art 2. para.10 of HCMC Decision 1/506/8.4.2009).
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Beneficial owners are, in the case of corporate entities: a) the natural person(s) who ultimately own(s) or control(s) a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings (other than a company listed on a regulated market that is subject to disclosure requirements consistent with community legislation or subject to equivalent international standards - a percentage of 25% plus one share shall be deemed sufficient to meet this criterion); or b) the natural person(s) who otherwise exercise(s) control over the management of a legal entity. In the case of legal entities, such as foundations and legal arrangements, and trusts, which administer and distribute funds: a) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25% or more of the property of a legal arrangement or entity; b) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates; or c) the natural person(s) who exercise(s) control over 25% or more of the property of a legal arrangement or entity.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Under local legislation it is up to the discretion of the relevant party to decide not to perform identity checks (unless there is a suspicion of money laundering) for credit and financial institutions or organisations situated in the EU or in a third country which impose requirements equivalent to those laid down in Directive 2005/60/EC and are supervised for compliance with those requirements. In addition, there are reduced due diligence requirements (no verification requirement) for other types of entities such as: a) listed companies whose securities are admitted to trading on a regulated market in one or more Member States which are subject to disclosure requirements consistent with Community legislation; b) companies operating as undertakings for collective investment in transferable securities and are based in the European Union and operate in consistency with the provisions of Directive 85/611/EEC as currently in force; c) Greek public law legal entities and state owned organisations of at least 51%; and d) public authorities or public bodies which satisfy certain requirements. Moreover there are reduced due diligence requirements (no verification requirement) for: a) life insurance policies where the annual premium is no more than EUR1,000 or the single premium is no more than EUR2,500; b) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme; c) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; and d) electronic money, where the maximum amount stored in the device is no more than EUR250, or where, if the device can be recharged, a limit of EUR2,500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR1,000 or more is redeemed in that same calendar year by the bearer.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	On a risk-sensitive basis, enhanced customer due diligence measures are required, especially for: a) transactions without the physical presence of the customer; b) cross border correspondent banking; and c) politically exposed persons. Moreover, most of the Competent Authorities have issued guidance that the following type of customers should be considered as high risk for money laundering purposes and should be subjected to enhanced due diligence procedures: a) companies with bearer shares; b) offshore companies; c) non-profit entities or organisations; d) persons from countries that do not adequately implement FATF recommendations; e) trust or similar Foreign Law Entities; f) non-residents' accounts; g) portfolio management accounts of important clients; and h) business relationships and transactions that entail high risks related to tax evasion (this high risk category shall at least include: (i) Self-employed persons whose total income credited on their own accounts or on accounts of which they are the beneficial owners exceed EUR200,000 during the previous calendar year (ii) Legal persons whose total cash deposits or cash withdrawals exceed EUR300,000 during the previous calendar year).
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	In all circumstances where PEPs are acting either as customers of obliged persons or beneficial owners of such customers.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	In respect of cross-frontier correspondent banking relationships with respondent institutions from third countries, credit institutions shall: a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision; b) assess the respondent institution's anti-money laundering and anti-terrorist financing controls; c) obtain approval from senior management before establishing new correspondent banking relationships; d) document the respective responsibilities of each institution; and e) with respect to payable-through accounts, be satisfied that the respondent credit institution has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Additional due diligence is required to mitigate the higher risk profile associated with non-face-to-face transactions. Where a customer approaches a firm remotely (by post, telephone or over the internet), the firm should have appropriate procedures to carry out non-face-to-face verification, either electronically or by reference to documents, by having in place additional verification checks to manage the risk of identity fraud. In this respect, obligated persons should take specific and adequate measures to counter the higher risk in cases where the customer is not physically present for identification purposes, mainly by applying one or more of the following measures: a) ensuring that the customer's identity is verified by additional documents, data or information; b) taking supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution based in the European Union; and c) ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution based in the European Union. Obligated persons should pay special attention to any product or transaction which might favour anonymity and which, by nature or by virtue of information about the profile of the characteristic features of the customer, may be associated with money laundering or terrorist financing and take appropriate measures to avert this risk.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Greek FIU (Anti-Money Laundering, Counter Terrorist Financing and Source of Funds Investigation Authority): http://www.hellenic-fiu.gr/index.php?lang=en
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 – 4,071 SARs (cases Closed: 3,210; cases under Investigation: 861) GDP (in current prices): 2013 – USD239,509.85m (Source: data.worldbank.org) This results in a ratio of 1 SAR for every USD58.8m of GDP.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	There are Competent Authorities who have issued instructions to the obligated persons under their supervision for reporting, apart from suspicious transactions for money laundering and terrorist financing, criminal activities (predicate offences, especially those connected with tax evasion) as well as unusual transactions / activities. Moreover, the Compliance Officers of certain Obligated Persons (including credit and financial institutions) are required to prepare a report, on an annual / bi-annual basis, providing considerable input for the assessment of the obliged person's compliance with the AML/TF provisions / policy with specific references in most cases to high risk clients / transactions. Such reports are assessed by the obliged persons' management (e.g. Board of Directors) and are submitted to the relevant Competent Authority in electronic form or in a hard copy. Credit Institutions, Payment Institutions and Electronic Money Institutions which have obtained license for establishment and operation in Greece as well as foreign Credit Institutions, Payment Institutions and Electronic Money Institutions which provide payment services (carry out transfer of funds) through established Greek branches or agents) are required to submit to the Competent Authority (Bank of Greece) on a regular basis, inter alia, data for the total number and amount of cross border transfer of funds from and to abroad (inbound and outbound funds), per country of payer's establishment (for inbound funds) or beneficiary's (for outbound funds) (Template I203, Bank of Greece Governor's Act 2651/20.1.2012, section I2, as in force). Moreover, Credit Institutions submit to the Bank of Greece, on a semi-annual basis, data and information relating to products, services and clients characterised as "high risk" in order that the ML and TF risk to which the Credit Institution is exposed be assessed (Template I204, Bank of Greece Governor's Act 2651/20.1.2012, section I2, as in force). In addition credit and financial institutions are obliged (pursuant to article 15 para 4 of L. 4174/2013 and Min. Circular POL 1033/28.1.2014, as in force) to forward electronically to the Greek Ministry of Finance (General Secretariat of Information Systems) files with customer data having a financial and tax interest. This data, inter alia, cover: a) self-employed persons whose total income credited on their own accounts or on accounts of which they are the beneficial owners exceed the relevant amount set each time by Banking and Credit Committee Decision of the Bank of Greece (currently EUR200,000) during the previous calendar year; and b) legal persons whose total cash deposits or cash withdrawals exceed the relevant amount set each time by Banking and Credit Committee Decision of the Bank of Greece (currently EUR300,000) during the previous calendar year).
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	An employee of an obligated legal entity or any other person obliged to report suspicious transactions shall be penalised with a term of imprisonment for up to two years if he/she intentionally fails to report to the competent authorities suspicious or unusual transactions or activities or provides false or misleading data, in breach of the relevant legal, administrative or regulatory provisions and rules, provided that his/her act is not punishable with heavier criminal sanctions. Furthermore, the Competent Authorities have the power to impose on the obligated legal person a wide range of administrative sanctions if they fail to comply with their obligations under Greek AML legislation.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	According to a Bank of Greece Governor's Act, Credit Institutions (and to some extent Financial Institutions) have the obligation to install adequate IT systems and effective procedures for continuously monitoring accounts and transactions, in order to detect, monitor and assess high-risk transactions and customers. IT systems should be capable of providing timely, reliable and necessary information for detecting, analysing and effectively monitoring customers' accounts and transactions. Accounts and transactions should be monitored in relation to the typology of transactions, the customer's profile, and the anticipated operation of the account in relation to the operation of other accounts in the same customer category. IT systems should be used for obtaining information on defective customer identification, the customer's profile and overall data on the Credit Institution's business relationship with the customer.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	The obligated persons must refrain from carrying out transactions, engaging in activities or providing any services, which they know or suspect to be related to money laundering and terrorist financing offences, unless refraining in such manner is impossible or likely to frustrate efforts to pursue the customers, the beneficial owners or the persons on behalf of whom the customers may be acting. In the latter case the obligated persons shall execute the aforementioned operations and simultaneously inform the Greek FIU.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Law provides that: "Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another country, provided that would be a predicate offence if committed in Greece and are punishable according to the law of such other country." Furthermore the Greek FIU have the power to request the obligated persons to provide all information required for the performance of their duties, including grouped information about certain categories of transactions or activities of domestic or foreign natural or legal persons or entities.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes. Pursuant to the Bank of Greece Governor's ("BoCG") Act 2577/9.3.2006 as in force, such reporting is included in a relevant assessment report evaluating the adequacy of the bank's overall Internal Control Systems.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	Based on the abovementioned BoCG Act requirements, the report is provided every three years by independent certified public accountants (other than the statutory ones) and is communicated to the bank and to the Bank of Greece (Department for the Supervision of Credit and Financial Institutions).

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	The report evaluates the adequacy of the bank's anti-money laundering and anti-terrorist financing procedures, in particular with respect to classification procedures in terms of ML risk of transactions and/or customers.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of “personal data” cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of “sensitive data”? How is it defined and what are the additional protections?
A29.	Greece has established data protection laws. The main piece of legislation is Law 2472/1997 which has implemented in all material respects the EU Directive 95/46. The definition of “personal data” in the data protection law covers material likely to be held for KYC purposes. Greek data protection law applies only to individuals and not to corporate data. There is a separate definition of “sensitive data” (art. 7 of law 2472/1997) which is in accordance with the definition/additional protections as set out by EU Directive 95/46 (article 8).
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes. However the Greek AML law permits the exchange of information between credit or financial institutions situated in Greece or in another Member State and belonging to the same group. This also applies to the exchange of information between credit or financial institutions situated in Greece and similar institutions of the same group which are situated in a third country that imposes requirements at least equivalent to those laid down in the Greek AML law and which are subject to supervision of their compliance with those requirements. In addition, obligated persons (credit & financial institutions, audit firms, tax consultancy firms, notaries and lawyers) who are situated or conduct their business in Greece may exchange information with persons from the same professional category regarding the same customer and the same transactions or activities involving two or more of the above persons. The foregoing shall also apply to the exchange of information between resident obliged persons and natural or legal persons from the same professional category situated or conducting their business in another Member State or in a third country that imposes requirements at least equivalent to those laid down in the Greek AML law, provided that such persons are from the same professional category and are subject to at least equivalent obligations as regards professional secrecy and personal data protection. The information exchanged is used exclusively for the prevention and suppression of the offences of money laundering and terrorist financing.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	There are various secrecy/confidentiality laws. In relation to banks the most important piece of legislation is L.D 1059/1971, pursuant to the disclosure of information relating to the existence, nature and balance of bank deposits is prohibited. This special banking secrecy rule applies to all banks operating in Greece and their officers, directors, employees and agents. In accordance, however, with the applicable legislation on lifting banking and professional secrecy, a Registry of Bank & Payment Accounts electronic System has been set up by virtue of articles 62-63 of L. 4170/2013 and Min. Circular POL 1258/5.12.2013 as in force, through which certain Greek authorities (i.e. the Secretary General for Public Revenues, the Economic Crimes Enforcement Agency, the Economic Police, the Economic District Attorney, the District Attorney for Corruption Crimes and the Greek FIU) have, under specific procedures, the ability to request from credit and payment institutions to provide them with data and information of clients maintained by such institutions (e.g. details of accounts, balances, transactions effected).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Guernsey

Key contact: Nick Vermeulen
Email: nick.vermeulen@gg.pwc.com
Tel: +44 (0) 1481 752089

Postal address: Royal Bank Place,
1 Glatigny Esplanade;
St.Peter Port; Guernsey, GY1 4ND

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Criminal Justice (Proceeds of Crime) (Bailiwick of Guernsey) Law was issued in 1999. It is supplemented by the Criminal Justice (Proceeds of Crime) (Financial Services Businesses) (Bailiwick of Guernsey) Regulations 2007 ("the Regulations") and the Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing 2012 ("the Handbook").
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	AML legislation requiring customer due diligence procedures was introduced in 2002. The 2007 Regulations and Handbook represent an update to the 2002 requirements.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	For a), b) and c) the regulator is Guernsey Financial Services Commission: www.gfsc.gg
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, the Handbook has specific guidance for financial services businesses on the application of AML requirements.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	By 31 March 2010, financial services businesses were required to have taken any necessary actions to remedy any identified deficiencies and satisfy itself that CDD information appropriate to the assessed risk is held in respect of existing customers.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, the Regulations and Handbook became effective on 15 Dec 2007 for regulated financial services businesses. The regulations were extended in Sep 2008 and Oct 2010 to cover certain services offered by lawyers, accountants and estate agents. The Handbook is not intended to provide an exhaustive list of appropriate and effective policies, procedures and controls to counter money laundering and the financing of terrorism. The structure of the Handbook is such that it permits a financial services business to adopt a risk-based approach appropriate to its particular circumstances. The financial services business should give consideration to additional measures that may be necessary to prevent its exploitation and that of its services/products and delivery channels by persons seeking to carry out money laundering or terrorist financing. A financial services business should be able to take a risk-based approach with regard to being used for the purposes of money laundering and terrorist financing; ensure its policies; procedures and controls are appropriately designed and implemented; and are effectively operated to reduce the risk of the financial services business being used in connection with money laundering or terrorist financing.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, MONEYVAL fourth round assessment in October 2014; no report is available at time of writing. IMF Assessment in January 2011: http://www.imf.org/external/pubs/ft/scr/2011/cr1112.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, one-off transactions (single or linked) under GBP10,000 do not require customer due diligence.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: name, residential address, date of birth, nationality, occupation, official personal identification number. No specific documents are mandatory, but local guidance dictates that evidence of identity should be obtained from documents issued by reputable sources, for example a passport or other national identity card. Separate verification of other details is also required. The Handbook provides suggestions for documents and evidence that can be obtained to verify identify. Legal Entities: Specific requirements vary depending on the risk profile of the applicant for business. Minimum evidence for a legal entity expected is one of: a) original or certified copy of the certificate of incorporation and memorandum and Articles of Association or equivalent constitution document; b) company registry search; c) latest audited financial statements; d) a copy of the Directors' Register; e) a copy of the shareholders' register; f) independent information sources, including electronic sources; or g) a personal visit to the principle place of business. The Handbook also provides guidance for dealing with Trusts, Foundations, Life Insurance Companies, Pension Schemes and Employee Benefit Schemes. In addition, identification and verification must be completed for individuals ultimately owning 25% or more of the legal entity and individuals (including directors and beneficial owners) with ultimate effective control over the assets of the legal entity.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Where non face-to-face identification and verification is carried out, a certified copy of the identification documentation is required. For certification to be effective, the certifier will need to have seen the original documentation and, where certifying evidence of identity containing a photograph, have met the individual in person. Where certified copy documents are accepted, the financial services business must satisfy itself, where possible, that the certifier is appropriate, for example, by satisfying itself that the certifier is not closely related to the person whose identity is being certified. A suitable certifier must certify that he has seen original documentation verifying identity. The certifier must also sign and date the copy identification data and provide adequate information so that contact can be made with the certifier in the event of a query. A consultation paper was published in May 2015 that seeks feedback on a proposal to make changes to the Handbook in order to recognise that technology is changing traditional methods of undertaking due diligence.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Beneficial owners and controllers must be identified and verification documentation obtained, including, at a minimum, those holding 25% or more interest in the capital of the entity.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced and simplified arrangements are available for identification and verification procedures of regulated institutions and publically traded companies. There is also some limited scope for reliance to be placed on procedures already conducted by intermediary regulated institutions.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced measures are required for those potential clients deemed to be of higher risk. This might take into account factors such as Politically Exposed Persons ("PEPs") risk, client not physically present for identification purposes, correspondent banking relationships, jurisdictional risk and types of activity.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Additional due diligence and enhanced scrutiny is required on all accounts that have links with PEPs, in particular those with links to countries that are vulnerable to corruption.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Local requirements specifically identify correspondent banking relationships as a trigger for enhanced measures. Specific measures required include: a) gathering sufficient information to understand the nature of the respondent's business; b) determining the reputation of the institution from publically available information; c) assessing the respondent institution's AML policies; d) obtaining senior management approval for taking on the client; and e) documenting the respective AML responsibilities of each institution.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In relation to non-resident individual customers for example, additional measures are required for non face-to-face transactions and/or relationships. Examples of such measures include: a) additional verification documentation; b) development of independent contact with the client; c) third party introduction; and d) requiring the first payment to be carried out through a bank account situated in an equivalent jurisdiction.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Guernsey Financial Intelligence Service (“GFIS”) as a division of the Guernsey Border Agency (www.guernseyfiu.gov.gg).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 797 SARs. Comparative GDP data is not available for this specific period.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Whilst there is no specific legal requirement, there is guidance for specific industries (for example, high value goods dealers) on unusual transactions, cash transactions, wire transfers etc. This is part of the AML Handbook.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, there are penalties for "Failure to report", "Assisting" and "Tipping Off".

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes, authorisation is required to proceed if transactions are identified as suspicious.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	The Data Protection (Bailiwick of Guernsey) Law, 2001 ("the Law") is a close copy of the UK Data Protection Act 1998 and organisations that are compliant either with the Act or the Law can be assured that they are compliant with both. The Law and the legislative environment in the Bailiwick has been assessed by the European Commission as providing adequate protection for personal data transferred to the Bailiwick from any EU state, so there should be no Data Protection impediments to the export and processing of personal data locally. The Statutory Instruments giving effect to the Law were made by the Advisory and Finance Committee on 09 Jul 2002 and were laid before the States, enabling the Law to come into force on 01 Aug 2002. Subsequent secondary legislation and amendments to the Law may also be found on the Statutory Instruments page (http://www.guernseylegalresources.gg/article/90621/Statutory-Instruments). a) According to the Law: "personal data" means data which relate to a living individual who can be identified: a. from those data; or b. from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. This would therefore include material likely to be held for KYC purposes. b) No provisions relating specifically to corporate data. c) According to the Law: "sensitive personal data" means personal data consisting of information as to: a. the racial or ethnic origin of the data subject; b. his political opinions; c. his religious beliefs or other beliefs of a similar nature; d. whether he is a member of a labour organisation, such as a trade union; e. his physical or mental health or condition; f. his sexual life; g. the commission or alleged commission by him of any offence; or h. any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data shall not be processed unless at least one of a number of specified conditions are met which include (but are not limited to): a. explicit consent by the person concerned; b. legal right or obligation conferred on the data controller in connection with employment; c. it is necessary to protect the vital interests of the data subject or another person where consent cannot be obtained or where data has been unreasonably withheld; d. processing in the course of legitimate activities by not for profit bodies or associations that exist for political, philosophical, religious or trade union purposes subject certain additional preconditions and safeguards; e. information contained in personal data has been made public as a result of steps deliberately taken by the data subject; f. processing is necessary for legal proceedings, obtaining legal advice or establishing, protecting and defending legal rights; g. it is necessary for the purposes of the administration of justice; and h. it is necessary for medical purposes and is undertaken by a health professional.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Credit reports: An individual is entitled to where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, whether his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking. A data controller is not obliged to supply this information unless he has received: a) a request in writing; and b) except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require. Where a data controller cannot comply with the request without disclosing information relating to another individual who can be identified from that information, he is not obliged to comply with the request unless: a) the other individual has consented to the disclosure of the information to the person making the request; or b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual. Criminal records: Personal data are exempt from the subject information provisions in respect of persons not ordinarily resident in the Bailiwick or any part of the Bailiwick (in this paragraph referred to as "non-resident subjects"), if they consist of records of criminal convictions or cautions of non-resident subjects to which those subjects are able to obtain access under and subject to the law of a jurisdiction other than that of the Bailiwick or any part of the Bailiwick. Medical data: Data for medical purposes can only be processed by a health professional or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional. The term "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	The Data Protection (Bailiwick of Guernsey) Law, 2001 ("the Law") is the primary legislation for Data Protection in Guernsey. There is no requirement for standard contractual clauses to be applied to the export of data to Guernsey. However, if a Guernsey organisation has personal data processed for them in the UK or elsewhere in the EEA it is recommended that they take the following actions: a) ensure that a contract or agreement exists between the Guernsey organisation and the UK/EEA based organisation that is processing the data and that it provides sufficient authority to show that they are processing the data on the Guernsey organisation's behalf; and b) provide confirmation to the UK/EEA organisation processing the data, that the Guernsey organisation is in compliance with the Data Protection (Bailiwick of Guernsey) Law, 2001 and that the Bailiwick of Guernsey has been assessed as providing adequate protection by the European Commission. All organisations located in the Bailiwick are reminded that it is an offence to process, or have processed on your behalf, personal data without having notified such processing unless a valid exemption applies. In general, provided that a data controller established in the Bailiwick has notified their processing to the Guernsey Data Protection Office, there should be no need to notify in the UK, unless they have a separately established business in the UK.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Guernsey meets or exceeds all OECD, EU and UK standards on tax transparency and information exchange, including commitment to apply the Automatic Exchange of Information (“AEOI”) agreements. It has no banking secrecy laws and has automatically exchanged information under the EU Savings Tax Directive. Guernsey is a tax transparent, co-operative jurisdiction with an economic model that complements and enhances UK Plc tax competitiveness. Guernsey should be considered neither a “tax haven” nor a “secrecy jurisdiction”.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We’re a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, “PwC” refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Hungary

Key contact: Paul Grocott
Email: paul.grocott@hu.pwc.com
Tel: +36 1 461-9260

Postal address:
Bajcsy-Zsilinszky út 78;
H-1055 Budapest; Hungary

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The AML Act – Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing came into effect on 14 Dec 2007 and is still currently in force.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website
A3.	a) Hungarian National Bank (http://www.mnb.hu/en); b) Hungarian National Bank (http://www.mnb.hu/en); and c) casinos: national tax authority (National Tax and Customs Administration) (http://en.nav.gov.hu/). Other: a) auditors: Chamber of Hungarian Auditors (http://www.mkvk.hu/); b) attorneys, law firms, notaries, etc. – local Bar which they are the member of; c) trading companies (http://mkeh.gov.hu/); and d) tax advisors and advisors dealing with real estate issues (Financial Intelligence Unit (FIU)) (http://en.nav.gov.hu/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, each regulator, indicated above in A3, issued guidance and/or template AML documents. Template policies are published by the supervisory bodies listed above on their websites.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, in cases where there are doubts surrounding the verification or adequacy of the customer identification data obtained previously.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, simplified and enhanced customer due diligence.

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	This information is not publicly available.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes - one-off transactions below EUR15,000 (other than where there are two or more such transactions which the firm believes are linked, and which together would amount to EUR15,000 or more) or any amount which is viewed to be of a suspicious nature.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	For the purposes of identification and verification procedures, service providers require the following documents to be presented: Natural persons: a) personal identification document (official identity card) and official address card of Hungarian citizens; and b) passport or personal identity card for foreign nationals or documentary evidence of the right of residence or a valid residence permit. Legal persons and business associations: a) the application for registration or the document of registration for recognised legal persons, or the articles of incorporation of legal persons and business associations lacking legal status whilst not yet registered by the registrar of companies, court or appropriate authority; and b) for non-resident legal persons and business associations lacking the legal status of a legal person, the document proving that the person or body has been registered under the law of the country in which it is established.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Certified copies of the documents shall be accepted for identification procedures if certified by the competent authority of the country where it was issued or by the competent Hungarian foreign representative. Certified copies of the documents referred to above shall be accepted for the verification of the identity of the customer if: a) it was prepared by the officer of a Hungarian consular post or by a notary public and certified accordingly; b) the officer of a Hungarian consular post or the notary public has provided an endorsement for the copy to verify that the copy is identical to the original presented; or c) the copy was prepared by an authority of the country where it was issued, if such authority is empowered to make certified copies and the competent Hungarian consulate officer has provided a confirmatory certification of the signature and seal of the authority.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	A beneficial owner is defined as: a) the natural person who directly or indirectly owns or controls at least 25% of the shares or voting rights in a legal person or business association lacking the legal status of a legal person, if that legal person or business association lacking the legal status of a legal person is not listed on a regulated market and is subject to disclosure requirements consistent with European Community legislation or subject to equivalent international standards; b) the natural person who has a dominant influence on a legal person or business association lacking the legal status of a legal person; c) the natural person on whose behalf a transaction is carried out; d) in case of foundations: a. where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of twenty-five per cent or more of the property of the foundation; b. where the individuals benefitting from the foundation have yet to be determined, the natural person(s) in whose interest the foundation is set up or operates; or c. the natural person(s) who exercise control in the management of the foundation or exercise control over twenty-five per cent of the property of a foundation, or who is authorised to represent the foundation; or e) in lack of a natural person listed above, the executive officer of the legal entity or company without legal entity. When establishing a business relationship, the customer acting on behalf of the beneficial owner shall indicate in a written statement the details of the beneficial owner such as surname, forename, address and nationality. The service provider may request the customer to supply other details of the beneficial owner (e.g. number/type of identification document, place of residence in Hungary for foreign nationals, date of birth and mother's name) to prevent and combat money laundering and terrorist financing. Where there is any doubt concerning the identity of the beneficial owner, the service provider must take measures to check the beneficial owners' identification data in publicly available records and registers.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified customer due diligence applies where the customer is: a) a service provider engaged in carrying out the activities defined in the law (financial services, investment services, insurance services, commodity exchange, postal financial intermediation services and voluntary mutual insurance fund services) in the territory of the European Union ("EU"), or a service provider that is engaged in these activities and situated in a third country which imposes requirements equivalent to those laid down in the Money Laundering Act; b) a listed company whose securities are traded on a regulated market in one or more member states, or a listed company from a third country that is subject to disclosure requirements consistent with European Community legislation; and c) a supervisory body mentioned in the law/central government body or a local authority/a body of the European Community. Simplified customer due diligence also applies for insurance policies with a low-level annual/single premium and insurance policies for pension schemes if there is no surrender clause and where the funds payable to the insured person cannot be used as collateral for any credit or loan arrangement. An insurance company shall not be required to apply customer due diligence measures for identifying a customer whose identity has already been established by an independent insurance intermediary for the same purpose.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence is applicable for: a) customers that have not been physically present for identification purposes or the verification of their identity; b) correspondent banking relationships; c) PEPs; and d) transactions for the exchange of money involving a sum of EUR2,000 or more. The service provider will record further information pertaining to the business relationship and the transaction order e.g. the type, subject matter and term of the contract of the business relationship and the subject matter and the value of the transaction order.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Customers residing in another member state or in a third country are required to provide a statement as to whether they are considered politically exposed according to the national law of their country. In respect of transactions or business relationships with PEPs residing in another member state or in a third country, approval from the management body, as defined in the organisational and operational regulations, is required.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Service providers engaged in the provision of financial services or in activities auxiliary to financial services are required, before establishing correspondent banking relationships with respondent institutions from third countries to: a) assess, evaluate and analyse the respondent service provider's anti-money laundering and anti-terrorist financing controls; b) be satisfied that the respondent service provider has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to monitor access to the accounts of the correspondent on an ongoing basis; and c) be satisfied that the respondent service provider is able to provide relevant customer due diligence data to the correspondent institution, upon request. Approval from the management body must be obtained to engage in correspondent banking relationships.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, service providers engaged in financial services activity or in activities auxiliary to financial services are prohibited to engage in or continue a correspondent banking relationship with a shell bank or with a service provider that is known to permit its accounts to be used by a shell bank.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Reporting entities are required to consider the additional risk posed by non face-to-face business in accordance with the risk based approach and procedures they have adopted. Service providers are required to record all data and particulars specified in the law, where the customer has not been physically present for identification purposes or for the verification of his identity.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The FIU which is currently the Hungarian Customs and Finance Guard within the National Tax and Customs Authorisation: http://nav.gov.hu/nav/penzmosas/pei

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 9,618 SARs GDP (in current prices): 2014 – USD138,300m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD14.3m.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, up to two years imprisonment for non-reporting.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Work needs to be ceased at reporting. Written information is required from the FIU in order to continue.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Service providers under the AML Act are required to incorporate details on their AML systems and controls in their internal AML policies. The policies are not subject to reporting but can be reviewed by the FIU upon inspection.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Act 112 of 2011 on information governance and information freedom regulates the issues of personal data protection: a) yes. Personal data is any data that can be connected to the individual, especially the name, any identification codes or numbers, or one or more pieces of information on the physical, physiological, mental, economic, cultural or social identity, and further any consequences that can be drawn therefrom; b) the same rules apply as long as the corporate data contains any individuals personal data, otherwise, corporate data is not subject to any special protection; and c) sensitive data are called special data in Hungarian terms. These are any personal data that refer to race, nationality, political views, party connections, religion or other religious beliefs, any memberships and sexual life. Furthermore, all personal data on health status and addictions and criminal records. The latter may only be controlled with the written consent of the individual.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Within the boundaries of the EU, if data controlling rights are available, personal data can be transferred without any additional requirements (such transfers are considered as transfer within the territory of Hungary). To any other country, personal data may only be transferred with the express consent of the individual or if otherwise the conditions for data controlling are met and in the third country the level of protection of personal data is high (as per the Act, this is granted if the obligatory legal norm of the EU states so, or if there are multi or bi-lateral agreements in effect between the given third country and Hungary).
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	The AML Act itself regulates the transfer of information.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Ireland

Key contact: Iarla Power / Sinead Ovenden

Email: iarla.power@ie.pwc.com / sinead.ovenden@ie.pwc.com

Tel: +353 (0) 1 7926398 / +353 (0) 1 792 6422

Postal address: One Spencer Dock;

North Wall Quay; Dublin 1;

Ireland

Last updated:

January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (CJA 2010) commenced on 15 Jul 2010: http://www.oireachtas.ie/documents/bills28/acts/2010/a0610.pdf The 2010 Act was subsequently amended by the Criminal Justice Act 2013 (CJA 2013).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The law previously did not adopt the utilisation of a risk-based approach. Different levels of CDD and ongoing monitoring was not a requirement.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) Central Bank of Ireland (http://www.centralbank.ie/Pages/home.aspx); b) Central Bank of Ireland; and c) The Anti-Money Laundering Compliance Unit ("AMLCU") is the supervisory body for auditors, external accountants, tax advisers, trust or company service providers, private members' gaming clubs and high value goods dealers (http://www.antimoneylaundering.gov.ie/en/AML/Pages/WP10000040).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Industry guidance notes have been prepared by a committee representing various sectors of the financial services industry. The Core Guidelines have been drafted jointly by various sectors of the financial services industry. The guidelines are stated to be for the purpose of guiding designated persons on the application of Part 4 of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010. While these guidelines have not been approved under Section 107 of the Act, the Central Bank will have regard to these guidelines in assessing compliance by designated persons with the Act. Links to the various guidelines can be located via: http://www.finance.gov.ie/viewdoc.asp?DocId=-1&CatID=16

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	CDD in relation to existing customers must be conducted where: a) the designated body has reasonable grounds to doubt the veracity or adequacy of documents or information previously obtained; and/or b) there are doubts concerning previously obtained customer identification data.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	The CJA 2013 provides expressly for risk-based measures to be applied by designated persons.
Q7.	Has the country been the subject of a FATF (of FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The last mutual evaluation conducted by FATF was in Jun 2013: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/Ireland-FUR-2013.pdf The Fourth Round of MERs commenced in 2014. A review of Ireland under the Fourth Round is set to take place in 2016. A national risk assessment is being prepared and a national steering committee chaired by the Department of Finance comprised of representatives of relevant competent authorities and state bodies (including the Central Bank) is engaged in preparations for the next FATF MER. The Central Bank is engaging with stakeholders domestically and at the international level to ensure that it is implementing international best practice for an effect AML/CFT regulatory regime for the financial services industry.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	In relation to “occasional transactions” where the total amount of money paid by the customer in a single transaction or series is greater than EUR15,000. For more information see A12 (“SCDD”).

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The CJA 2010 specifies in section 33(2)(a) that the measures to be applied under section 33(1) of the Act include identifying the customer, and verifying the customer's identity on the basis of documents (whether or not in electronic form), or information that the designated person has reasonable grounds to believe can be relied upon to confirm the identity of the customer, including: a) documents from a government source (whether or not a State government source); or b) any prescribed class of documents, or any prescribed combination of classes of documents. The Guidance states that the following information should be obtained and verified: Individuals: Name, Date of Birth and Current Address. Documentary Verification: “One plus One” approach – one item from the list of photographic IDs (typically to verify name and date of birth) and one item from the list of non-photographic IDs (typically to verify address). Photographic ID: a) current valid passport; b) current valid driving licence; and c) current valid National Identity Card. Non Photographic ID: a) official documentation / cards issued by the Revenue Commissioners and addressed to the individual; b) official documentation / cards issued by the Department of Social and Family Affairs and addressed to the individual; c) instrument of a court appointment (such as liquidator, or grant of probate); d) current local authority document e.g. refuse collection bill, water charge bill (including those printed from the internet); e) current statement of account from a credit or financial institution, or credit/debit card statements (including those printed from the internet); f) current utility bills; (including those printed from the internet); and g) current household/motor insurance certificate and renewal notice. Legal persons: Name, legal form and proof of existence, address of registered office and main place of business, the nature of the business and its ownership and control structure) and directors or equivalent (either two directors or one director and one authorised signatory) and beneficial owner(s) to be verified as warranted by the risk. Documentary verification: a) a search of the relevant company or other registry; b) a copy, as appropriate to the nature of the entity, of the certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust or other official documentation proving the name, form and current existence of the customer; c) in cases regarded by the Designated Person as higher risk, use of more than one source of information may be warranted; and/or d) obtain a copy of the annual audited accounts listing directors.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	The Guidance states that the following, and potentially their equivalents in other jurisdictions, are considered suitable persons to certify documentation, where they are willing to do so: a) Garda Siochana / Police Officer; b) Practising Chartered & Certified Public Accountants; c) Notaries Public / Practising solicitors; d) Embassy / Consular Staff; e) Regulated financial or credit institutions; f) Justice of the peace; g) Commissioner for oaths; or h) Medical professional.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	How to identify: Identify any beneficial owner connected with the customer or service concerned. This information can be provided by the customer (or on the customer's behalf by the customer's duly authorised representative) or obtained from a reliable, independent source. This should include designated persons taking reasonable measures to understand the ownership and control structure of the customer. This would comprise: a) any natural person who owns or controls more than 25% of the shares or voting rights in the legal person or arrangement; or b) any natural person who exerts ultimate control over the legal person through its management or otherwise. If, exceptionally, due to the nature or structure of the legal person or arrangement, it is not feasible to identify any natural person who meets either of the definitions at a) or b) above, the designated person may treat as exercising control the directors (or equivalent) or other persons having the power to legally bind the customer. The designated person must record the basis for their decision in reaching the conclusions it has in relation to the ownership / control of the customer. How to verify: Verify the identity of the natural persons who own or control more than 25% of the shares or voting rights or otherwise exercises control over the management of the legal person or arrangement. The extent of this verification is dependent on the relevant risks. This would be satisfied by verifying identity in line with the requirements for individuals. This could also be satisfied by one or more of the following alternative approaches in line with the risk policy of the designated person. In high risk scenarios a designated person should use more than one source to verify information. a) obtaining a copy of the annual audited accounts listing shareholders, directors or other persons exercising control over the customer (where the information is considered by the designated person to be current and reliable); b) for complex structures, (particularly where a company is registered abroad) a relevant and up-to-date legal opinion from a source on which the designated person is prepared to rely, documenting due diligence conducted, including in relation to information on the shareholding / control structure and directors (or equivalent); c) placing reliance on information provided / certified by counterparties / agents (e.g. in syndicated deals) where such persons are regulated credit or financial institutions or are legal or accountancy professionals subject to equivalent AML/CTF obligations; d) having a notary public (or equivalent) certify the validity of the information provided by or on behalf of the customer; or e) placing reliance on information provided / certified by a Company Secretary (or equivalent), e.g., copies of constitutional documentation (e.g., Memo & Articles/Certificates of Incorporation / Trust Deed) and shareholder certification. In line with the designated person's risk assessment the process may include verifying a beneficial owner's personal identity (the extent of verification required will depend on the risk) in line with the requirements for personal customers. Such verification should be considered the norm for any customer regarded by the designated person as higher risk.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Specified Customers: a) credit and financial Institutions; b) listed companies; c) public bodies; and d) beneficial owners of Pooled Accounts held by Solicitors and other Legal Professionals. Specified Products: a) electronic money (If the device cannot be recharged, the maximum amount stored in the device is no more than EUR250 or EUR500, if the device cannot be used outside the State. Where the device can be recharged, a limit of EUR2,500 is imposed on the total amount transacted in a calendar year, except where an amount EUR1,000 or more is redeemed in that same calendar year by the bearer of electronic money); b) life assurance policy (having an annual premium of no more than EUR1,000 or a single premium of no more than EUR2,500); and c) pensions.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence is required in respect of: a) a correspondent banking relationship; b) a business relationship or transaction with a non-resident PEP; and c) a higher risk customer (including non-face to face).
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	The CJA 2010 requires designated persons to apply enhanced measures to PEPs that are resident outside the State but not to domestic PEPs (under the definition of a PEP, an individual ceases to be so regarded one year after he has left office).
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Section 38(1) of the CJA 2010 states that prior to commencing the relationship, the credit institution: a) has gathered sufficient information about the respondent institution to understand fully the nature of the business of that institution; b) is satisfied on reasonable grounds, based on publicly available information, that the reputation of the respondent institution and the quality of supervision or monitoring of the operation of that institution in the place are sound; c) is satisfied on reasonable grounds, having assessed the anti-money laundering and anti-terrorist financing controls applied by the respondent institution, that those controls are sound; d) has ensured that approval is obtained from the senior management of the credit institution; and e) has documented the responsibilities of each institution in applying anti-money laundering and anti-terrorist financing controls to customers in the conduct of the correspondent banking relationship.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, under Section 59 of CJA 2010.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Section 33(4) of CJA 2010 contains a supplementary obligation on a designated person where a customer who is an individual does not present in person. This is not an alternative obligation but a supplementary one. The subsection provides that, without prejudice to the generality of section 33(2)(a), one or more of the following measures shall be applied by a designated person under section 33(1) of the Act, where a customer who is an individual does not present to the designated person for verification in person of the customer's identity. e.g. verification of the identity with additional documentation; robust anti-fraud checks, etc.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.	
A18.	An Garda Síochána Detective Superintendent, Financial Intelligence Unit (FIU), Garda Bureau of Fraud Investigation, Harcourt Square, Dublin 2 Phone No: 01-6663714 Fax No: 01-6663711	Revenue Commissioners Suspicious Transactions Reports Office Block D, Ashtowngate, Navan Road, Dublin 15 Phone No: 01-8277542 Fax No: 01-8277484
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.	
A19.	Information on the volume of SARs is not publicly available.	
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?	
A20.	Section 43 CJA 2010 requires a relevant person to report any service or transaction which is connected with a place that does not have adequate procedures in place for the detection of money laundering or terrorist financing (the power to designate a jurisdiction is contained in section 32 CJA 2010).	

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, failure to report suspicious activity is a criminal offence which carries a penalty pursuant to section 43(2) CJA 2010: a) on summary conviction, to a fine not exceeding EUR5,000 or imprisonment for a term not exceeding 12 months (or both); or b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years (or both).

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	According to section 42(7) of CJA 2010, a designated person who is required to make a report shall not proceed with any suspicious transaction or service connected with the report, or a transaction or service with the subject of the report, prior to the sending of the report to the Garda Síochána and the Revenue Commissioners unless: a) it is not practicable to delay or stop the transaction or service from proceeding; or b) the designated person is of the reasonable opinion that failure to proceed with the transaction or service may result in the other person suspecting that a report may be (or may have been) made or that an investigation may be commenced or in the course of being conducted. Nothing in subsection (7) authorises a designated person to proceed with a service or transaction if the person has been directed or ordered not to proceed with the service or transaction under section 17 and the direction or order is in force.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes: a) yes; b) the laws apply to Personally Identifiable Information ("PII") but not to other aspects of Corporate Data; and c) yes, sensitive data includes Personally Identifiable information and other sensitive personal data, such as medical records. Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. Sensitive personal data means personal data as to: a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject; b) whether the data subject is a member of a trade union; c) the physical or mental health or condition or sexual life of the data subject; d) the commission or alleged commission of any offence by the data subject; or e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. Additional rules apply regarding transfer of data to third countries (i.e. those outside the European Economic Area EEA). The rules regarding transfers to third countries can be summarised as follows: a) the general rule is that personal data cannot be transferred to third countries unless the country ensures an adequate level of data protection. The EU Commission has prepared a list of countries that are deemed to provide an adequate standard of data protection; b) if the country does not provide an adequate standard of data protection, then the Irish data controller must rely on use of approved contractual provisions or one of the other alternative measures, provided for in Irish Law; and c) the Data Protection Commissioner retains the power to prohibit transfers of personal data to places outside of Ireland, if he considers that data protection rules are likely to be contravened, and that individuals are likely to suffer damage or distress as a result.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes, EU laws apply - EU Data Protection Directive (95/46/EC).
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Isle of Man

Key contact: Jonathan Whiting
Email: jonathan.d.whiting@iom.pwc.com
Tel: +44 (0) 1624 689689

Postal address: Sixty Circular Road; 3rd Floor;
Douglas IM1 1SA,
Isle of Man

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Proceeds of Crime Act 2008 became fully effective in 2009, and in 2011 the Anti-terrorism and Crime (Amendment) Act was introduced. The Acts are supplemented by secondary legislation which was last updated by the Money Laundering and Terrorist Financing (Online Gambling) Code 2013 which came into force on 01 May 2013 and by the Anti-Money Laundering and Countering the Financing of Terrorism Code 2015 which came into force on 01 Apr 2015.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The 2015 Code has been expanded to include domestic PEPs, addition of Specified Non-Profit Organisations, clarification on the types of risk assessments and internal/external disclosures.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) The Isle of Man Financial Services Authority ("IOMFSA") is the regulator for banks, investment businesses, fiduciary service providers, collective investment schemes, insurance, pensions and Designated Non-Financial Businesses and Persons (www.iomfsa.im); and b) The gaming industry is regulated by the Gambling Supervision Commission ("GSC") (http://www.gov.im/gambling/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The IOMFSA provides guidance in the form of the Anti-Money Laundering and Countering the Financing of Terrorism Handbook and in the Guidance Notes on Anti-Money Laundering and Preventing the Financing of Terrorism – for Insurers: http://www.iomfsa.im/handbooks/guides/AML/amlcftrequirementsguidance.xml Guidance Notes on the Prevention of Money Laundering and Countering of Terrorist Financing are provided by the GSC covering the online gambling industry: http://www.gov.im/gambling/licensing/
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	The 2015 Code under paragraph 9 requires the licence holders to ensure all information for the purposes of customer due diligence is up to date and appropriate (https://www.gov.im/lib/docs/ipa/2015sd0102amlcftcode2015.pdf).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, this has been effective since 2008.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	MoneyVAL performed a third round progress report for Isle of Man and its report was published in Sep 2013 (https://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/progress%20reports/MONEYVAL(2013)14-ProgRep_IoM.pdf).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	There is no requirement to verify the identity of customers if the transaction qualifies as an "exempted one-off transaction", defined as a single transaction or a series of linked transactions which has an (aggregate) value of less than: a) EUR3,000 for holders of Casino licences and bookmakers; b) EUR5,000 for bureaux de change, or cheque encashment facilities; c) EUR1,000 for money transmission business; or d) EUR15,000 in all other cases.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: The elements of identity which must be verified comprise: a) all customers: Name and date of birth and permanent residential address; and b) standard and higher risk customers: Nationality, place of birth, and national identification number. Legal Entities: For all companies that are not listed on a recognised stock exchange (or their wholly owned subsidiaries), the elements of identity which must be verified comprise: a) name; b) official identification number; c) date and country of incorporation; d) registered office address of the legal person; and e) address of the principal place of business where this is different to the registered office.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Suitable persons to certify verification of identity documents include: a) a member of the judiciary, a senior civil servant, a serving police or customs officer; b) an officer of an embassy, consulate or high commission of the country of issue of documentary verification of identity; c) a lawyer or notary public who is a member of a recognised professional body; d) an accountant who is a member of a recognised professional body; e) a company secretary who is a member of a recognised professional body; and f) a director, company secretary or manager of a business regulated on the Isle of Man or an external regulated business as defined in the Code. g) a manager or other senior officer within the relevant person's group.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	In all cases, it is a requirement to identify underlying principals and/or beneficial owners at the outset of the business relationship, irrespective of the geographical origin of the client, or of any introducer or fiduciary.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	The criteria for simplified due diligence is stated in the 2015 Code paragraph 20: https://www.gov.im/lib/docs/ipa/2015sd0102amlcftcode2015.pdf
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Where a customer poses a higher risk of ML/FT as assessed by the customer risk assessment or in the event of any unusual or suspicious activity.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	A relevant person must maintain appropriate procedures and controls for the purpose of determining whether any of the following is a PEP: a) any customer; b) any natural person having power to direct the activities of a customer; c) any beneficial owner or known beneficiaries. A relevant person must maintain appropriate procedures and controls for requiring the approval of its senior management before any business relationship is established with, or before any occasional transaction is carried out with, or before a business relationship is continued with, a domestic PEP who has been identified as posing a higher risk of ML/FT, or any foreign PEP.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Before entering into a business relationship or occasional transaction, a relevant person must: a) obtain sufficient information about the respondent institution or designated business to understand fully the nature of its business; b) determine from publicly available information: a. the reputation of the respondent institution or designated business; b. the quality of the supervision to which it is subject; and c. whether it has been subject to investigation or regulatory action in respect of ML/FT; c) assess the AML/CFT procedures and controls maintained by the respondent institution or designated business, and ascertain that they are adequate and effective; d) ensure that the approval of the relevant person's senior management is obtained; and e) clearly understand the respective responsibilities of the relevant person and the respondent institution or designated business with respect to AML/CFT measures.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Where the licence holder deals with an applicant for business other than face-to-face, it must take adequate measures to compensate for any risk arising as a result.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Isle of Man Financial Crime Unit ("FCU"): https://www.gov.im/categories/home-and-neighbourhood/emergency-services/police/police-support-services/financial-crime-unit/suspicious-transaction-reports/

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Under the Proceeds of Crime Act 2008, the penalty for failure to report is a fine and/or a prison sentence of up to five years. The penalty for tipping off is a fine and/or a prison sentence of up to two years.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Consent is required from the FCU to proceed with a current/ongoing transaction that is identified as suspicious.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes. Data Protection Act 2002: a) yes; b) controllers of data must comply with the Act and the Eight Data Protection Principles; and c) yes. Sensitive personal data means personal data consisting of information as to: a) the racial or ethnic origin of the data subject; b) his political opinions; c) his religious beliefs or other beliefs of a similar nature; d) whether he is a member of a trade union (within the meaning of the Trade Unions Act 1991); e) his physical or mental health or condition; f) his sexual life; g) the commission or alleged commission by him of any offence; or h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Before personal information can be transferred outside the Island an organisation must ensure that adequate protection exists for the information in the receiving country. Countries within the European Economic Area, that is, European Union member states plus Norway, Iceland and Liechtenstein are deemed to have adequate protection. In addition, the European Commission has made adequacy findings for other countries, including Argentina, Guernsey, Jersey, Switzerland and Canada, and US companies that have "signed up" to the Safe Harbour provisions. On the 28 Apr 2004, the European Commission formally decided that the Isle of Man has adequate data protection legislation.

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	See A30.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Italy

Key contact: Mario Cristina
Email: mario.cristina@it.pwc.com
Tel: +39 348 1505244

Postal address: Via Monte Rosa, 91
20149 Milano,
Italy

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1991 (amended in 2004, 2006, 2007, 2009, 2010, 2013, 2014 and also due in 2015).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The new KYC rules of the Bank of Italy, issued in Apr 2013, give more specific details on how to conduct customer due diligence, AML risk profiling and information recording in the Single Electronic Archive ("AUI"). Moreover, IVASS (Istituto per la Vigilanza sulle Assicurazioni), the controller and public authority ruling of the insurance industry, has issued, through its provision dated Jul 2014 (in force as of 2015), much more specific rules for life-insurance companies concerning customer due diligence and risk profiling activities.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.)? Please include link to the regulator(s) website.
A3.	a) Financial Intelligence Unit of Bank of Italy (i.e. Unità di informazione finanziaria) (http://www.bancaditalia.it/UIF/); b) IVASS (for life insurance companies) (http://www.ivass.it/ivass/imprese_jsp/HomePage.jsp); and c) CONSOB (Commissione Nazionale per le Società e la Borsa) (auditors) (http://www.consob.it/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, guidelines for Organisation and Internal Controls for AML purposes and Guidelines for KYC rules for the Banking and Financial sector.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, banks, financial institutions, non-financial businesses and professionals have to verify the identity of customers in the case of transactions, a new relationship or as soon as they come into contact with the customer.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	The Italian system provides strict and detailed provisions on anti-money laundering and terrorist financing requirements. In general, it is possible to assign these obligations on the basis of risk (the risk based approach became effective in Dec 2007). Furthermore, KYC rules issued by the Bank of Italy provide more details on the application of a risk-based approach.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The most recent FATF Mutual Evaluation Report on Italy was published in Feb 2006: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Italy%20full.pdf The most recent update on Italy's performance is contained in the Second Biennial Update to the Mutual Evaluation of Italy dated Feb 2013: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/Second_Biennial_Update_Feb2013_Italy.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, one-off transactions below EUR15,000 (other than where there are two or more such transactions which the firm believes are linked and which together would amount to EUR15,000 or more) and EUR1,000 for cash and bearer instruments.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Any person who: a) opens, changes or closes a current, savings or deposit account or has another 'continuing relationship'; or b) carries out a single transaction, or several transactions which appear to be linked, involving the transmission, handling or the transfer of means of payment or bearer instruments in an amount of EUR15,000 or more; must be identified and must indicate in writing the full details of the person, if any, on whose behalf the transaction is carried out. Identification must take place each time a transaction is executed. Individuals: evidence of identity should be obtained such as name, address, date and place of birth, tax code and a government issued document e.g. an identity card, passport or driving licence. Legal persons: evidence of the identity of the firm, as well as the identity of the person physically present at the transaction, should be obtained such as the company name, registrar office, tax code and evidence of the identity of the beneficial owner.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Financial institutions, designated non-financial businesses and professionals cannot rely on a copy of an identification document. An exception is provided for copies validated by public officers.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	In Italy, customers have to provide all information regarding beneficial ownership of transactions/relationships. Joint stock companies are required to publish lists of their shareholders and lists of persons who hold rights on securities. This information is available to the authorities and to the public upon request (including online).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Other than for telephone and internet banking, there are specific provisions allowing for simplified due diligence. Customer due diligence is not required in the following cases: a) transactions and account relationships between equivalent financial institutions; b) the transfer of funds within the State Treasury and payments arranged by the public administration, through the State Treasury, with the exception of payment operations linked to the national debt; c) the accounts, deposits and other continuing relationships between provincial sectors of State treasuries, the Bank of Italy and the Financial Intelligence Unit ("FIU"); d) relationships and transactions between banks, other licensed intermediaries that have their head office or branch in Italy and banks or branches located abroad. This exemption applies regardless of whether the countries in which the banks/branches are located have effectively implemented the FATF Recommendations; and e) when the customer is a listed company.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	There are specific provisions requiring enhanced due diligence for higher risk categories of customers (for example PEPs), operations or transactions such as financial products distributed via the internet (or when the customer is not physically present), companies incorporated in a tax haven or a country listed on the Organisation for Security and Co-operation in Europe ("OSCE") grey list.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Article 28(5) of Legislative Decree 231/2007 requires the application of enhanced due diligence measures to foreign PEPs which comprise: a) establishing adequate risk-based procedures to determine whether the customer is a politically exposed person; b) obtaining the authorisation of the general manager, his delegate or a person performing an equivalent function before establishing a continuous relationship with such customers; c) taking all necessary measures to establish the source of wealth and source of funds that are involved in the continuous relationship or the transaction; and d) conducting enhanced ongoing monitoring of the continuous relationship or professional service.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	For correspondent banking relationships, banks, financial and non financial institutions as well as professionals have to perform enhanced due diligence and acquire information as provided by the public register. In addition, where possible, they must evaluate the internal control system of their correspondent bank and can only start the business relationship with the authorisation and responsibility of senior management.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, there are specific provisions that prohibit financial institutions from entering into or continuing correspondent banking relationships with shell banks. Moreover, there are specific provisions that prohibit financial institutions from establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	The 'Decalogo' of the Bank of Italy requires financial intermediaries to adopt special precautions for transactions relating to telephone or electronic accounts, and to take steps to ensure adequate knowledge of the customer and his business in cases of relationships with customers in non face-to-face situations.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	SARs must be reported to the Financial Intelligence Unit (i.e. Unità d'Informazione Finanziaria - UIF), which is a special agency of the Banking Supervisory Authority (Banca d'Italia): http://www.bancaditalia.it/UIF
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 71,758 SARs GDP (in current prices): 2014 - USD2,141,000m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD29.9m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	There is an obligation to report all financial transactions above EUR3,000 made by credit card or e-payment, but this is not specifically for AML purposes. This type of report is made to the tax agency (Agenzia delle Entrate).
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	See answer to A20 above.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes. There is a penal sanction for tipping off.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Even if there is not a strict requirement to use automated suspicious transaction monitoring technology, there is the possibility to use an automated monitoring tool in order to support suspicious transaction reporting.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Usually financial intermediaries define internal authorisation procedures to proceed with current/ongoing suspicious transaction.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	There is a general requirement for auditors to report on the bank's systems and internal controls.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) the report must be provided frequently, usually every 6-12 months; b) board of directors / controls offices; and c) no.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	a) yes; b) N/A; and c) N/A.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Customers' information acquired by a financial intermediary is usually used only internally, also for AML purposes.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	N/A
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Jersey

Key contact: Neil Howlett
Email: neil.howlett@je.pwc.com
Tel: +44 (0) 1534 838349

Postal address: 37 Esplanade,
St Helier, Jersey,
Channel Islands, JE1 4XA

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Proceeds of Crime (Jersey) Law was issued in 1999. It is supplemented by the Money Laundering (Jersey) Order 2008 and the Jersey Financial Services Commission ("JFSC") Handbook for the Prevention and Detection of Money Laundering and the Financing of Terrorism.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The Order and the Handbook issued in Feb 2008 updated existing subordinate legislation and detailed guidance which supported the 1999 law.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	For a), b) and c) the regulator is Jersey Financial Services Commission: www.jerseyfsc.org
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, the AML Handbook has specific guidance for industries on the application of AML requirements. The Handbook applicable to most financial services business is the entitled "For Financial Services Business Regulated under the Regulatory Laws", which can be found at the following link: http://www.jerseyfsc.org/anti-money_laundering/regulated_financial_services_businesses/index.asp Note: All of the AML Handbooks were amended on 01 Jan 2015 and 24 Mar 2015, implementing various pre and post-MONEYVAL visit amendments and providing guidance in relation to changes brought about by Money Laundering(Amendment No. 8) (Jersey) Order 2015, which came into force on the same date.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes. The sixth amendment to the Money Laundering (Jersey) Order 2008 was enacted in December 2013 which required, by 31 Dec 2014, every relevant person to: a) hold information for every continuing business relationship that takes into account a relevant person's assessment of the risk of that relationship, or be taking action under Article 14(7) of the Money Laundering Order; or b) have agreed a bespoke remediation plan with the JFSC.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, the Handbook was issued and effective on 04 Feb 2008 for regulated financial services businesses. The answers below are taken from that guidance. On 19 Feb 2008, customer due diligence requirements were extended to lawyers, accountants, estate agents and others.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, MONEYVAL fourth round assessment in Jan 2015 – no report is available at time of writing. In Sep 2009 the IMF published its report on 'Jersey: Financial Sector Assessment Program Update – Detailed Assessment of Observance of AML/CFT': http://www.imf.org/external/pubs/ft/scr/2009/cr09280.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, as per Article 13 of the Money Laundering (Jersey) Order 2008. If the transaction is not made as part of a business relationship and meets the criteria for a single (or linked) one-off transaction per Article 4 of the Money Laundering (Jersey) Order 2008, then a threshold of EUR15,000 applies.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Legal name, any former names (such as maiden name) and any other names used; principal residential address and date of birth are required for all customers. In the case of standard risk customers additional details include: place of birth, nationality and sex should be obtained. Higher risk customers also require Government issued personal identification number (or equivalent). No specific documents are mandatory, but local issued guidance dictates that evidence of identity should be obtained from documents issued by reputable sources. Identity verification: Current passport (providing photographic evidence of identity), current national identity card (providing photographic evidence of identity), current driving licence (providing photographic evidence of identity) where the licensing authority carries out a check on the holder's identity before issuing or independent data sources. Address verification: Correspondence from a central or local government department, letter from regulated entity, personal visit to residential address, a bank statement, tenancy contract or utility bill. Legal entities: Name of company, any trading names, date and country of incorporation/registration, official identification number, registered office address, mailing address (if different), principal place of business/operations, names of all directors, identification information of all directors who have and exercise authority to operate a relationship or to give the relevant person instructions concerning the use or transfer of funds or assets and identification information of individuals ultimately holding a 25% or more interest in the capital of the company. Verification of identity of the company can be demonstrated where the name of the company, date and country of incorporation/registration and official identification number are verified. In the case of standard and higher risk customers, the registered office address and principal place of operations should also be verified. Components of identity can be verified using one or more (in the case of standard and higher risk customers) verification methods: - original or certified copy of the certificate of incorporation; - memorandum and Articles of Association; - company registry search; - latest audited financial statements; - independent data sources, including electronic sources; and - personal visit to principle place of business. In circumstances where information is not already publically available/held, minimum requirements are to verify the identity of directors or similar persons who have authority to operate a relationship or give instructions concerning the use/transfer of assets. Verification of other directors and beneficial owners should also be considered depending on the risk profile. The AML Handbook also provides guidance on Trusts, Foundations, Partnerships and Employee Pension Schemes.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Where non face-to-face identification and verification is carried out, a certified copy of the identification documentation is required (by a Notary Public or other qualified professional able to legally certify documents). A consultation paper was published in October 2015 that seeks feedback on a proposal to add a new chapter to the Handbook in order to recognise that technology now offers the possibility of collecting information about a customer who is an individual and obtaining evidence of that individual's identity in new and different ways.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	A new three-tiered approach for identifying beneficial owners and controllers was introduced on 01 Jan 2015. This requires identification of individuals having a material controlling ownership interest, if none, individuals exercising control through other means should be identified and, again if none, individuals exercising executive control through senior management positions should be identified. These need to be identified and verified in line with the requirements for individuals detailed in A9. Material interest is deemed to be those holding 25% or more interest in the capital of the entity. Enhanced CDD measures must be applied on a risk-sensitive basis where an owner or controller of a customer or other person that must be identified under Article 3 of the Money Laundering Order is not physically present for identification purposes. For low risk customers, relevant identification information on the beneficial owners and controllers must be collected and reasonable measures must be taken to verify the identity of any beneficial owners and controllers of the applicant.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced and simplified arrangements are available for identification and verification procedures of institutions in equivalent jurisdictions and publically traded companies. There is also some scope for reliance to be placed on procedures already conducted by intermediary regulated institutions. It should be noted that the recent amendment to the Money Laundering (Jersey) Order 2008 would require businesses to exclude the application of any simplified due diligence where the customer is resident in a country which is not compliant with FATF Recommendations (currently in appendix D1 and D2 to the Handbook).
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	The Handbook in conjunction with Article 15 of the Money Laundering Order requires that a relevant person apply enhanced CDD measures using a risk based approach where: a) a relevant person must apply enhanced CDD measures where an owner or controller of a customer (including an individual concerned with a trust or a foundation) or other person that must be identified is not physically present for identification purposes; b) customer has a "relevant connection" to an "enhanced risk state"; c) customer, or some other prescribed person, is a PEP; d) relevant person provides a correspondent banking service to a bank outside Jersey; e) customer is a non-resident; f) customer is provided with private banking services; g) customer is a personal asset holding vehicle; or h) customer is a company with nominee shareholders or issues bearer shares.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Circumstances: Article 15(5A) of the Money Laundering Order requires that a relevant person that has or proposes to have a business relationship or proposes to carry out a one-off transaction with a PEP (or relationship or transaction that has a prescribed connection to a PEP) must be subject to additional due diligence. For the purposes of determining whether a person is a close associate of a PEP a relevant person need only consider information that it holds or is publicly known. Procedures: Article 15(5A) of the Money Laundering (Jersey) Order 2008 requires that: a) any new business relationship or continuation of such a relationship or any new one-off transaction to be approved by the senior management of the relevant person; and b) the source of the wealth of the PEP and the source of the funds involved in the business relationship or one-off transaction must be established.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Article 15(4B) of the Money Laundering (Jersey) Order 2008 requires the adoption of specific and adequate measures which include: a) gathering sufficient information about the institution to understand fully the nature of its business; b) determining the reputation of the institution and the quality of its supervision, including whether it has been subject to any money laundering investigation or regulatory action; c) assessing the institution's systems and controls to combat money laundering in order to determine whether they are consistent with the requirements of the FATF recommendations and their effectiveness; d) requiring any new relationship to be approved by the senior management of the relevant person; e) recording the respective responsibilities of the relevant person and the institution to prevent and detect money laundering so that both parties clearly understand those responsibilities; and f) being satisfied that, in respect of customers of the institution who have services provided directly by the relevant person, that the institution has applied customer due diligence measures at least equivalent to those set out in this Order and is able to provide a copy, at the request of the relevant person, of the evidence, documents, data and information obtained when applying such measures. Further guidance on enhanced due diligence can also be found in Section 7 of the Handbook.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Article 23A of the Money Laundering (Jersey) Order 2008 prohibits relationships with shell banks.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Additional measures are required for relationships established or transactions conducted remotely, or where the identity of an individual is to be verified using documentary evidence when the individual is not physically present. Issued guidance suggests that certified copies of verification documents such as passports should be obtained which have been certified by a 'suitable certifier'. Enhanced CDD measures must be applied where an owner or controller of a customer (including an individual concerned with a trust or a foundation) or other person that must be identified is not physically present for identification purposes.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Jersey Financial Crimes Unit: (http://www.jersey.police.uk/about-us/departments/crime-services/financial-crime/)
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 2,281 SARs (Source: http://www.jersey.police.uk/media/299015/Annual-Report-2014-Feb15.pdf) Comparative GDP data is not available for this specific period.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Whilst there is no specific legal requirement, there is guidance for specific industries (for example, high value goods dealers) on unusual transactions, cash transactions, wire transfers etc. This is part of the AML Handbook.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, there are penalties for "Failure to report", "Assisting" and "Tipping Off".

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No, but section 5.3 of the AML Handbook provides guidance on the use of automated monitoring.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes, authorisation is required to proceed if transactions are identified as suspicious.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Not currently.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes. Data Protection (Jersey) Law 2005: a) yes; b) not specifically defined; and c) yes – section 2. Sensitive personal data is personal data in relation to the data subject (which qualifies for an additional level of protection under the Law) containing information as to: a) racial or ethnic origin; b) political opinions; c) religious or other similar beliefs; d) union membership; e) physical or mental health or condition; f) sexual life; g) the commission or alleged commission of any criminal offences; or h) any criminal proceedings or convictions (including verdict and sentencing).

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes, in all cases specified above there are some restrictions as detailed in the Data Protection (Jersey) Law 2005.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes, the Data Protection (Jersey) Law 2005 applies to the transfer of information to Jersey.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Jersey meets or exceeds all OECD (the Organisation for Economic Co-operation and Development), EU and UK standards on tax transparency and information exchange, including commitment to apply the AEOI (Automatic Exchange of Information) agreements. It has no banking secrecy laws and has automatically exchanged information under the EU Savings Tax Directive. Jersey is a tax transparent, co-operative jurisdiction with an economic model that complements and enhances UK Plc tax competitiveness. Jersey should be considered neither a “tax haven” nor a “secrecy jurisdiction”.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Kazakhstan

Key contact: Baurzhan Burkhanbekov
Email: Baurzhan.burkhanbekov@kz.pwc.com
Tel: +77273303200

Postal address: PricewaterhouseCoopers LLP,
34 Al-Farabi Ave. Building A, 4th floor,
050050, Almaty, Kazakhstan

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Since Mar 2009.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non-financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The Committee on Financial Monitoring of the Ministry of Finance of the Republic of Kazakhstan: http://www.kfm.gov.kz/en/
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The requirements in respect of the AML Law can be found at: http://www.kfm.gov.kz/en/
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	There is no risk based approach in the AML Law, though it was agreed with the Ministry of Finance that auditors will report their findings, to the extent of which they come across suspicious transactions or those exceeding special thresholds, as part of their normal audit tests.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Kazakhstan is a member of the Eurasian Group on combating money laundering and the financing of terrorism ("EAG"). This evaluation was conducted by the EAG and was then discussed and adopted by the EAG Plenary in Jun 2011: http://kfm.gov.kz/en/mutual-evaluation/report-on-mutual-evaluation-of-the-republic-of-ka/

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, these are explained in Article 4. Transactions in Money and (or) Other Assets Liable to Financial Monitoring, Law No. 191 of 28 Aug 2009 of the Republic of Kazakhstan concerning counteraction to legalisation (laundering) of income gained in an illegal way and the financing of terrorism: http://kfm.gov.kz/en/regulatory-framework/is-the-current-legislation.html
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Please refer to Article 5 of the AML Law.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Customer identification information includes obtaining the following: Individuals: a) Kazakh residents: personal ID and tax ID are required; or b) non-residents: personal ID/passport and Tax ID are required in addition to a document confirming registration of the individual with migration authorities. Legal entities: a) management's ID; b) entity's legal documents (Charter, State Registration Certificates, Tax ID, Statistical ID, Licenses etc.); and/or c) identification for the owners of the business (except for Joint Stock Companies). The documents should be either originals or notarised copies.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	ID for owners of the business (except for Joint Stock Companies) should be obtained.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	No specific guidance in this respect. The approach is the same regardless of circumstances.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	No specific guidance in this respect. The approach is the same regardless of circumstances.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	As Article 8 reads: In relation to foreign public official persons, entities of financial monitoring shall be obliged: a) to check that the public official person is connected to the entity; b) to perform an evaluation of the reputation of the said foreign public official person in relation to their participation in cases associated with the legalisation of income gained in an illegal way (laundering) and the financing of terrorism; c) to receive a permit of an executive officer of the organisation for the establishment and continuation of business relations with such clients; and d) to undertake measures to establish a source of funds. There is no other specific guidance for Politically Exposed Persons.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Article 9. Proper Checking Correspondent Banks by Entities of Financial Monitoring: Besides the measures provided for by paragraph 3 of Article 5 of this Law, in relation to correspondent banks, entities of financial monitoring shall be additionally obliged: a) to gather information on the reputation of correspondent banks; b) to make an evaluation of participation of a correspondent bank in cases associated with the legalisation (laundering) of income gained in an illegal way and the financing of terrorism; and c) to receive a permit of an executive officer of the organisation to establish new correspondent relations.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	The following is subject to reporting to the Committee of Financial Control: Placement of or transfer to a client's bank account of money that is performed by a natural person or legal entity which has a registration, place of residence or place of location, respectively, in an offshore zone, and equally which has a bank account registered in an offshore zone, or a transfer of money by a client for the benefit of the mentioned category of persons both as a one-time transaction, and also as a transaction that is made within seven sequential calendar days.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Please refer to Article 4 of the AML Law: http://kfm.gov.kz/en/regulatory-framework/is-the-current-legislation.html

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Committee of Financial Monitoring of the Ministry of Finance of the Republic of Kazakhstan: http://www.kfm.gov.kz/en/

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Transactions above a certain threshold should be reported. Please refer to Article 4 of the AML Law: http://kfm.gov.kz/en/regulatory-framework/is-the-current-legislation.html

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	There are some de-minimis thresholds depending on the nature of transactions. Please refer to Article 4 of the AML Law for details: http://kfm.gov.kz/en/regulatory-framework/is-the-current-legislation.html

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Tipping off is considered as a breach of the Law. There are penalties for non-compliance with reporting requirements.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Not for auditors.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	As we understand if a transaction was stopped then authority should be obtained from Committee of Financial Monitoring of the Ministry of Finance of the Republic of Kazakhstan to proceed.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Not aware of the requirements in this respect.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	In Nov 2013 Law on personal data was enacted. a) it is likely that the definition covers personal data; b) it does not include a definition of "corporate data" and it does not apply to corporate data; and c) it does not include a separate definition of "sensitive data", but includes the following article: Article 11. Confidentiality of personal information: a. owners and (or) operators, and also the third parties who have access to personal information of limited access, provide their confidentiality by not allowing the distribution without prior consent of the subject or his lawful representative or existence of other lawful basis; b. persons for whom personal information of limited access in connection with profession, office need and also labour relations, are obliged to provide their confidentiality; and c. confidentiality of biometric data is established by the legislation of the Republic of Kazakhstan.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	With written consent only.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	In accordance with the Law of the Republic of Kazakhstan "Concerning Personal Data and Their Protection" dated 21 May 2013, No 94-V, the cross-border transfer of personal data to the territory of foreign states shall be performed provided that this state ensures the protection of the personal data transferred, and if such protection is not ensured, it is a requirement to obtain the subject's or legal representative's written consent.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Please refer to Article 29.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Latvia

Key contact: Ilandra Lejiņa
Email: ilandra.lejina@lv.pwc.com
Tel: +371 67094400

Postal address: Valdemāra 21-21
Riga, Latvia
LV-1010

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2008.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) Financial and Capital Markets Commission ("FCMC"); b) FCMC; and c) Control service (http://www.prokuratura.gov.lv/public/29881.html) (in Latvian; information on Control Service (Kontroles dienests)).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Control service (http://www.prokuratura.gov.lv/public/29881.html) (in Latvian; information on Control Service (Kontroles dienests)). Practical guidance for certified auditors (www.lzra.lv), although please note this information is locked with a password.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, there are new developments with a deadline of 31 Mar 2017.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	EUR15,000 (if there are no other indicators).

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Latvian residents: document with name, surname and personal code. Non-residents: documents which allow the individual to be in Latvia, including a passport. Legal entities: Registration documents, information of legal address, identity of representatives.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Originals should be provided.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Residents: name, surname, personal code. Non-residents: name, surname, date of birth, verification document number and date, state and institution who issued the document.

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	A credit institution or financial institution registered in Latvia or EU Member State: - a credit institution or financial institution registered in a country which complies with the EU requirements; - a public municipal entity (ministry, city council, etc.) or a public or municipal capital company with inherently low money laundering; - a merchant whose shares are traded in a regulated market in the EU or a third country in respect of which disclosure requirements that are similar to those of the EU exist; - a person, in the name of which a public notary or a lawyer from the EU Member State or a country complying with the EU requirements; and - a person with a low inherent money laundering risk (all the feature must be taken into account): - the client has been engaged in public administration duties under the EU law; - the information identifying the publicly available, transparent, reliable; - the client's activities and accounting methods are transparent; and - client business.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	a) if the client was not participating in identification personally; b) for PEPs; and c) for cross border banking relations with respondents from third countries.

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	For all transactions with PEPs, board approval is required along with risk-based actions to determine the origin of funds and the origin of well-being.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	a) obtaining the information on respondent for full understanding the nature of transaction, publicly available information about reputation and the quality of monitoring of the related bank or investment entity; b) evaluating AML actions undertaken by the respondent; c) receiving approval of the Board before establishing new correspondent relationships; and d) documenting respondent liability with regards to AML. Banks should ensure that they have no relationships with other financial institutions that are known to have transactions with shell banks.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In all circumstances.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Office for Prevention of Laundering of Proceeds Derived from Criminal Activity (FIU Latvia): https://zinojumi.kd.gov.lv/

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 17,041 SARs GDP (in current prices): 2014 - USD31,287m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD1.8m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	a) unusual transactions; b) cash transactions over EUR60,000 for banks or over EUR40,000 for other entities; c) currency exchange transactions over EUR8,000 without the use of bank accounts; d) cash debited from the account immediately after crediting it; e) potential fraud; f) suspicious transactions abroad; and g) cash change over EUR2,000 (of one currency).
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	See thresholds above in A20.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	There are certain monetary and administrative penalties in force, depending on the type of institution who has not complied with the reporting requirements.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Yes, for financial institutions.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	N/A

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	N/A

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	N/A

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Luxembourg

Key contact: Michael Weis / Roxane Haas
Email: michael.weis@lu.pwc.com / roxane.haas@lu.pwc.com
Tel: +352 49 48 48 4153 / +352 49 48 48 2451

Postal address: 2 rue Gerhard Mercator
B.P. 1443, L-1014 Luxembourg,
Luxembourg

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1993 (amended 2004, 2008, 2010, 2012, 2015). The EU's fourth AML Directive 2015/849/EC was issued on 20 May 2015. It has not been transposed in Luxembourg law yet. Laws & Regulations in force in Luxembourg for AML: a) Law of 12 Nov 2004 as amended on the fight against money laundering and terrorist financing (http://www.cssf.lu/fileadmin/files/Lois_reglements/Legislation/Lois/L_121104_AML_upd240715_eng.pdf); b) Grand-ducal regulation of 01 Feb 2010 providing details on certain provisions of the amended law of 12 Nov 2004 on the fight against money laundering and terrorist financing (http://www.cssf.lu/fileadmin/files/Lois_reglements/Legislation/RG_NAT/gdr_aml_ft_01022010_upd050815_eng.pdf); c) Law of 27 Oct 2010 enhancing the anti-money laundering and counter terrorist financing legal framework; organising the controls of physical transport of cash entering, transiting through or leaving the Grand Duchy of Luxembourg; implementing United Nations Security Council resolutions as well as acts adopted by the European Union; concerning prohibitions and restrictive measures in financial matters in respect of certain persons, entities and groups in the context of the combat against terrorist financing (http://www.cssf.lu/fileadmin/files/Lois_reglements/Legislation/Lois/L_271010_AML_TF.pdf); d) Grand-ducal regulation of 29 Oct 2010 (co-ordinated version) enforcing the law of 27 Oct 2010 implementing United Nations Security Council resolutions as well as acts adopted by the European Union concerning prohibitions and restrictive measures in financial matters in respect of certain persons, entities and groups in the context of the combat against terrorist financing (http://www.cssf.lu/fileadmin/files/Lois_reglements/Legislation/RG_NAT/GDR_291010_restr_meas_upd030811.pdf); CSSF(Commission de Surveillance du Secteur Financier) Regulation N°12-02 of 14 Dec 2012 on the fight against money laundering and terrorist financing (http://www.cssf.lu/fileadmin/files/Lois_reglements/Legislation/RG_CSSF/RCSSF_No12-02eng.pdf); e) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN); and f) Regulation (EU) No 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds (http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0847&from=EN).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	A Grand-ducal regulation was published on 05 Aug 2015 on the possibility to apply reduced/simplified due diligence for online payment services and electronic money.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The supervisory authorities are as follows: a) banking: CSSF (http://www.cssf.lu/en/); b) other financial services: CSSF (http://www.cssf.lu/en/); and c) non-financial sector: lawyers (barrister of the Bar) and Insurance: CAA (Commissariat aux Assurances) (http://www.commassu.lu/).

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	A practical guide for the funds industry has been published by the Association of the Luxembourg Fund Industry (“ALFI”): http://www.alfi.lu/sites/alfi.lu/files/files/Alfi%20guidelines%20and%20recommendations/Guidelines-ABBL-ALCO-ALRIM-final.pdf
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. CSSF Regulation 12-02 stresses that all AML/CTF measures taken have to be properly aligned to the assessed risk. The risk based approach methodology set forth in the Regulation comprises a risk assessment based on various criteria such as client risk, country risk, risk associated with products, transactions or the distribution/selling of the product. For the investment fund industry, the latter risk variable will be of particular relevance. With regards to the written AML/CTF risk assessment of the professionals’ own activity, an obligation as required by the Law of 12 Nov 2004, as amended, and Article 5 of the Regulation specifies that: a) the risk assessment of each new client and for each new product needs to be done prior to client acceptance/product launch; b) the risk score of each client must be kept up to date; and c) the professional must be in a position to communicate its risk assessment to the CSSF.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The most recent assessment was completed in 2010: http://www.fatf-gafi.org/countries/j-m/luxembourg/documents/mutualevaluationofluxembourg.html

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, one-off transactions (single or linked) under EUR15,000 for occasional customers.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Pursuant to Article 18 of the Regulation 12-02, the identity of a customer must be verified by means of a valid official document issued by a competent authority and bearing a photo and signature. In addition to passports and identity cards, other official documents such as residential permits can be accepted. Article 24 of the Regulation now clearly states that when establishing the client relationship, the information on the origin of funds must be part of this initial customer due diligence. Corporates: Articles of Association (or equivalent), extract of the Commercial Register (or equivalent), business authorisation if the entity manages funds of third parties, identification of the beneficial owners and of the persons with authorised signatures.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	If non face-to-face business is conducted, the copy should be certified as true by a competent authority, for example a consulate, embassy, police station or notary.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Beneficial owners must be identified and their identification needs to be verified in line with the requirements applicable to a natural person. Article 23 of the Regulation 12-02 confirms that a beneficial owner can, notwithstanding the 25% of ownership threshold, be a person who owns or controls less than 25% of a legal structure but who is nevertheless the person who ultimately controls the legal structure. According to Article 17 of the Regulation 12-02, the professionals are required to obtain a declaration of beneficial ownership signed by their clients. The beneficial owner is no longer required to sign such a declaration himself, but the client must inform the professional in case of any change in beneficial ownership.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence arrangements are listed in Article 3-1 of the Luxembourg AML Law. Examples of simplified due diligence arrangements include: a) where the customer is a credit or financial institution subject to equivalent AML regulations and which is supervised; b) on certain conditions, pooled accounts held by notaries and other legal independent professionals; c) where the customer is a Luxembourg public authority; d) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; e) pension schemes that provide retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the transfer of rights; and f) where the customer is a listed company whose securities are admitted to trading on a regulated market within the meaning of Article 1-11 of the law of 13 Jul 2007 in one or more European Union ("EU") Member States or a listed company in a third country subject to disclosure requirements consistent with EU legislation. The new Grand-ducal regulation dated 05 Aug 2015 states in Article 2 simplified due diligence may be applied when online payment services fulfilling each of the following conditions are carried out: a) the transaction concerns the provision of payment services listed under number 3, second and third indents, number 4, second and third indent, number 5 and number 7 of the Annex to the law of 10 Nov 2009 on payment services, as amended; b) the transaction is executed via accounts held with payment service providers located in the EU or in a third country which imposes equivalent requirements relating to the fight against money laundering and terrorist financing; c) the transaction does not exceed a unit amount of EUR250; and d) the total amount of the transactions executed for the customer during the 12 months preceding the transaction does not exceed EUR2,500. It also applies to professionals with respect to electronic money referred to in Article 3-1(4)(d) of the Law of 12 Nov 2004.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence measures are required in situations which by nature present a higher risk of money laundering or terrorist financing and at least in the cases listed in Article 3-2 of the Luxembourg AML Law (for example non face-to-face business, foreign PEPs and cross-frontier correspondent banking relationships with respondent institutions from non EU countries).
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Enhanced due diligence measures are required for foreign PEPs, including the implementation of an appropriate risk-based procedure to detect such foreign PEPs. Such measures should include senior management approval of customer acceptance, ascertaining the source of wealth/income and ensuring enhanced on-going monitoring of the relationship.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	For correspondent banking relationships and similar relationships, the correspondent bank must: a) gather sufficient information about the respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision; b) assess the respondent institution's AML and CTF controls; c) obtain approval from senior management before establishing new correspondent banking relationships; d) document the respective responsibilities of each institution; and e) with respect to payable-through accounts, be satisfied that the respondent credit institution has checked the identity of and performed on-going due diligence on the customers having direct access to the accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution upon request.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, it is prohibited to enter into, or continue a correspondent banking relationship with a shell bank or with a bank that is known to permit its accounts to be used by a shell bank.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Enhanced due diligence measures are required for non-face-to-face customers. These include: a) obtaining additional documents, data or information that ensures adequate identification of customers; b) performing additional measures to verify or certify the identification documents (for example, copies of identification documents certified true by a credit or financial institution or by a competent authority); or c) first payment to be drawn on an account opened in the customer's name with a credit institution.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Financial Intelligence Unit ("FIU") of the Luxembourg Public Prosecutors: http://www.justice.public.lu/fr/publications/index.html

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 - 4,891. GDP (in current prices): 2013 - USD60,383m (Source: data.worldbank.org). This results in a ratio of 1 SAR for every USD12.3m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No, all suspicious transactions, regardless of the amount have to be reported.
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Offenders who knowingly violate AML/CTF legislation could face a fine up to EUR1.25m and those guilty of professional negligence could face administrative and disciplinary sanctions.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Yes, Regulation CSSF 12-02 Art. 39 defines that IT tools are mandatory, unless the volume or nature of transactions are such that the control is otherwise effective.
Q24.	Is there a requirement to obtain authority to proceed with a current/on-going transaction that is identified as suspicious?
A24.	Professionals must refrain from carrying out a transaction which they know or suspect to be related to money laundering or terrorist financing before having informed the FIU. The FIU can give instructions not to execute one or more operations relating to the transaction or the customer. Where a transaction is suspected of giving rise to money laundering or terrorist financing and where to refrain in such manner is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the professionals concerned shall submit the necessary information immediately afterwards.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	In practice, because of professional confidentiality, the monitoring of transactions is not performed outside the jurisdiction. However, credit institutions and professionals of the financial sector forming part of a financial group shall guarantee to the group’s internal control bodies, where necessary, access to information concerning specific business relations, to the extent that this is needed for the global management of legal risks and risks to their reputation in connection with money laundering or the financing of terrorism within the meaning of the laws of Luxembourg. Special precautionary measures must be taken such as encryption to guarantee confidentiality of data.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	Yes.
Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) annually; b) The Regulator (CSSF or the CAA for insurances); and c) yes, in the Long Form Report.
Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) yes; b) yes; and c) yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, the Law of 02 Aug 2002 on the protection of personal data transposes the EU Directive 95/46/CE: a) to the extent that KYC material includes information about individuals this falls within the definition of "personal data"; b) the Law does not cover corporate data but only personal data. Corporate entities related data are not in the scope of the Law; and c) no. The Law adopts the EU directive definition for data of a sensitive nature. In some cases, the processing of such data is prohibited; in other cases it requires an approval from the local Data Protection Authority.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	No, such processing is not prohibited but requires consent and to pass the "loyalty", "legitimacy", "proportionate", etc. usual tests. Criminal record data cannot be processed except when so authorised by law. Medical data might be processed for life insurance purposes, subject to compliance with the legal requirements (consent, etc.).
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation?) If so, what data is subject to regulation?
A32.	Yes, there is a bank secrecy imposed by law to financial institutions and other financial players. Any breach is subject to criminal sanctions. This covers all client related data without any limit of time. Client's consent does not waive the professional secrecy duty.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Malta

Key contact: Lucienne Pace Ross
Email: lucienne.pace.ross@mt.pwc.com
Tel: +356 25647118

Postal address: 78 Mill Street
Qormi, QRM3101,
Malta

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Prevention of Money Laundering Act was enacted in 1994 and was subject to a number of amendments thereafter.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The Financial Intelligence Analysis Unit ("FIAU") serves as Malta's FIU and is the entity designated to fulfil the responsibilities of an FIU set out in the European Union's Third Money Laundering Directive (Directive 2005/60/EC) and the FATF 40 Recommendations: http://www.fiumalta.org/ The Malta Financial Services Authority ("MFSA") is the single regulator for financial services. This is a fully autonomous public authority, which reports to the Maltese Parliament on a regular basis. As an agent of the FIAU, the MFSA undertakes a number of on-site Anti-Money Laundering checks on its License Holders during its compliance visits.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The Prevention of Money Laundering Act and the Prevention of Money Laundering and Funding of Terrorism Regulations ("PMLFTR") are supplemented by the Implementing Procedures issued by the FIAU (http://www.fiumalta.org/implementing-procedures). Sectorial procedures are also in place for the banking sector and land based casinos.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	The PMLFTR require subject persons to apply customer due diligence ("CDD") measures to existing customers at appropriate times on a risk sensitive basis and when the subject person becomes aware that changes have occurred in the circumstances surrounding the established business relationship. The PMLFTR do not impose an obligation on subject persons to update all CDD documentation of all existing customers prior to 31 Jul 2008 when the PMLFTR came into force. However, since the PMLFTR require subject persons to update documentation of existing clients at appropriate times on a risk sensitive basis, subject persons are required to update the documentation of customers posing a higher risk, determined on the basis of the subject persons procedures for risk assessment and risk management, as soon as reasonably practicable. With respect to other customers, subject persons should update CDD documentation when certain trigger events occur, such as when an existing customer applies to open a new bank account or to establish a new relationship, or where an existing relationship changes.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, in Mar 2012: http://www.fiumalta.org/moneyval-evaluations/fourth-round

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	One off transactions (single or linked) under EUR15,000 do not require customer due diligence.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: The following information should be obtained: a) official full name; b) place and date of birth; c) permanent residential address; d) identity reference number, where available; and e) nationality. These should be verified against photographic evidence of identity listed through one of the following: a) a valid, unexpired passport; b) a valid, unexpired national identity card; or c) a valid, unexpired driving licence. The verification of the residential address shall be carried out by making reference to any one of the following documents: a) a recent statement from a recognised credit institution; b) a recent utility bill or any similar document as may be specified in sectoral implementing procedures issued by the FIAU; c) a correspondence from a central or local government authority, department or agency; d) a record of a visit to the address by a senior official of the subject person; or e) any government issued document listed above, where a clear indication of residential address is provided. Legal entity: The subject person is required to first identify the private company by gathering the following information: a) the company's official full name; b) the company's registration number; c) the company's date of incorporation or registration; and d) the company's registered address or principal place of business. These should be verified by viewing one or more of the following documents: a) the certificate of incorporation; b) a company registry search, including confirmation that the private company has not been, and is not in the process of being dissolved, struck off, wound up or terminated; or c) the most recent version of the Memorandum and Articles of Association or other statutory document.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Certification of the documentation is required by: a) a legal professional; b) an accountancy professional; c) a notary; d) a person undertaking relevant financial business; or e) a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Beneficial ownership refers to direct or indirect ownership or control of more than 25% of the shares or voting rights. Refer to A9.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	a) applicants for business, which are authorised to undertake relevant financial business, including regulated entities in the financial sector. This provision also applies to applicants for business which are licensed or authorised to carry out activities equivalent to relevant financial business in another Member State of the European Community or in a reputable jurisdiction; b) legal persons listed on a regulated market and which are subject to public disclosure requirements. These entities may either be authorised under the Financial Markets Act (42), an equivalent regulated market within the Community, or in a reputable jurisdiction; c) beneficial owners of pooled accounts held by notaries or independent legal professionals; d) certain domestic and foreign public authorities or bodies; and/or e) legal persons who present a low risk of ML/TF.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	The PMLFTR refer to three specific types of relationships in respect of which enhanced due diligence ("EDD") measures must necessarily be applied: a) where the applicant for business has not been physically present for identification purposes; b) in relation to cross-border correspondent banking relationships; and c) in relation to a business relationship or occasional transaction with a PEP.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Subject persons are required to apply EDD measures to all foreign PEPs as defined in the PMLFTR. Domestic PEPs need to be identified as such and EDD measures applied on a risk based approach.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Where a credit institution seeks to establish such correspondent banking relationships it has to ensure that: a) it fully understands and documents the nature of the business activities of its respondent institution, including from publicly available information: a. the reputation of the institution; b. the quality of supervision of that institution; and c. whether that institution has been subject to a ML/TF investigation or regulatory measure; b) it assesses the adequacy and effectiveness of the internal controls of the institution for the prevention of ML/TF; c) it obtains prior approval of senior management; d) it documents the respective responsibilities for the prevention of ML/TF; and e) it is satisfied that, with respect to payable through accounts, the respondent credit institution has verified the identity of and performed ongoing due diligence of the customers having direct access to the accounts of the respondent institution and that it is able to provide relevant CDD data upon request.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Credit institutions are prohibited from entering into, or continuing, correspondent banking relationships with shell banks.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Where the applicant for business has not been physically present for identification purposes, subject persons are required to apply one or more of the following measures: a) establish the identity of the applicant by using additional documentation and information; b) verify or certify the documentation supplied using supplementary measures; c) require certified confirmation of the documentation supplied by a person carrying out relevant financial business; and/or d) ensure that the first payment or transaction into the account is carried out through an account held by the applicant for business in his name with a credit institution authorised under the Banking Act or otherwise authorised in another Member State of the Community or in a reputable jurisdiction. Also refer to A13.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The Financial Intelligence Analysis Unit serves as Malta's FIU and is the entity designated to fulfil the responsibilities of an FIU set out in the European Union's Third Money Laundering Directive (Directive 2005/60/EC) and the FATF 40 Recommendations: http://www.fiumalta.org/
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 202 SARs (Source: FIAU 2014 Annual Report) Comparative GDP data is not available for this specific period.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	a) subject persons shall examine with special attention, and to the extent possible, the background and purpose of any complex or large transactions, including unusual patterns of transactions, which have no apparent economic or visible lawful purpose, and any other transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism, establish their findings in writing, and make such findings available to the Financial Intelligence Analysis Unit and to the relevant supervisory authority in accordance with applicable law. b) subject persons shall pay special attention to business relationships and transactions with persons, companies and undertakings, including those carrying out relevant financial business or a relevant activity, from a jurisdiction that does not meet the criteria of a reputable jurisdiction as defined in regulation (2), and; where the provisions of sub regulation (1) apply to such transactions, subject persons shall proceed as provided for in sub regulation (1).
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Non compliance with procedures, including tipping off, shall on conviction be liable to a fine ("multa") not exceeding EUR50,000 or to imprisonment for a term not exceeding two years, or both.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Appropriate consent is the consent of the FIAU to proceed with a transaction that is suspected or known to be related to ML/TF, in accordance to Article 28 and Regulation 15(7). The subject person will need to inform the FIAU before executing the transaction. After acknowledging receipt of the information, the FIAU will determine whether the execution of the transaction should be delayed. The execution of the transaction may be delayed by 1 working day and notice of such delay of execution shall be immediately given to the subject person. The FIAU can further extend the execution by another working day. In such instances, notice to the subject persons shall be given before the lapse of the initial period.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	The FIAU, the body established for the implementation of the AML/CFT regime in Malta, has administrative powers, meaning that the investigative and law enforcement powers are vested in the Police. The FIAU is given additional powers for co-operating and exchanging information with local and foreign supervisory authorities and foreign FIUs.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of “personal data” cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of “sensitive data”? How is it defined and what are the additional protections?
A29.	Yes: a) in terms of the Data Protection Act (Chapter 440 of the Laws of Malta) ("DPA") the term ‘personal data’ means ‘any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’; b) the DPA expressly provides that its provisions are to ‘...apply to the processing of personal data, wholly or partly, by automated means and to such processing other than by automated means where such personal data forms part of a filing system or is intended to form part of a filing system.’ Hence, the DPA should apply to data which falls within the definition of ‘personal data’. Furthermore, non-living entities should fall outside the scope of the DPA; and c) the DPA defines the term ‘sensitive data’ as ‘...personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, membership of a trade union, health, or sex life’. The general rule is that sensitive personal data may only be processed if the data subject: a. has given his explicit consent to processing; or b. has made the data public.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	In general, the data subject should be required to give his/her consent to the disclosure of personal data by the Controller to third parties. In addition, in terms of the DPA the '...transfer to a third country of personal data that is undergoing processing or intended processing, may only take place subject to the provisions of this Act and provided that the third country to which the data is transferred ensures an adequate level of protection.' Furthermore, the DPA expressly provides that 'it is for the Commissioner to decide whether a third country ensures an adequate level of protection. The transfer of personal data to a third country that does not ensure adequate protection is prohibited.' The website maintained by the Office of the Information and Data Protection Commissioner explains that a transfer of personal data to another country constitutes processing and as such must be notified to the Commissioner in the same way as other processing operations. However, no restrictions or other formalities apply in relation to the transfer of personal data to: a) EU Member States; b) member countries of the EEA; and c) third countries (i.e. countries that are not Member States of the European Union) which are from time to time recognised by the EU Commission to have an adequate level of protection. In the case of entities licenced under the Banking Act, institutions part of a global network, can share data with other members of the group without customer's explicit consent, provided the sharing is necessary for the proper carrying out of their activities. The Professional Secrecy Act also prohibits the sharing of customer information with third parties unless customer consent is held. This act does not distinguish between personal and corporate customers. In cases of investigations carried out MLROs, sharing of data relating to the transaction/s being under scrutiny can be shared in very limited circumstances with other MLROs depending on the type of licenced activity carried out.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	We are not aware of any case law, laws or regulations that may impact upon the transfer of information to Malta. However, as noted on the Office of the Information and Data Protection Commissioner website (http://idpc.gov.mt/), the Commissioner is required to collaborate with supervisory authorities of other countries to the extent necessary for the performance of his duties, in particular by exchanging all useful information, in accordance with any convention to which is a party or other international obligation. Hence, bilateral agreements are in place with third countries for the transfer of data.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. Article 257 of the Criminal Code (Chapter 9 of the Laws of Malta) ("CC") provides that the disclosure of secret information by any person, who by reason of his calling, profession or office, becomes the depositary of any secret confided in him, is an offence. This should not apply if such person would have been compelled by law to disclose such information.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Netherlands

Key contact: Andre Mikkers
Email: andre.mikkers@nl.pwc.com
Tel: +31 88 792 6348

Postal address: Thomas R. Malthusstraat 5,
1066 JR, Postbus 9616, 1006 GC
Amsterdam

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1993 (amended 2003). Revised legislation as per Jul 2008.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) De Nederlandsche Bank ("DNB") (http://www.dnb.nl/en/home/index.jsp); b) DNB and Authority for the Financial Markets (Autoriteit Financiële Markten) ("AFM") (http://www.afm.nl/en); and c) DNB, Dutch Tax Administration (http://www.belastingdienst.nl/wps/wcm/connect/bldcontenten/belastingdienst/individuals/) and Financial Supervision Office (Bureau Financieel Toezicht) ("BFT") (www.bureaufn.nl)
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	a) (http://www.dnb.nl/en/home/index.jsp); b) (http://www.afm.nl/en); and c) (http://www.belastingdienst.nl/wps/wcm/connect/bldcontenten/belastingdienst/individuals/) and (www.bureaufn.nl).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The latest FATF Mutual Evaluation Report on the Netherlands is dated 25 Feb 2011: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Netherlands%20ES.pdf A follow-up report was issued in Feb 2014.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, Customer Due Diligence is not required for business relationships leading to one or more transactions with a total value of less than EUR15,000.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Verification of individual customer identification information includes: a valid passport, a valid Dutch identity card, a valid identity card issued by the competent authorities in another Member State and bearing a photograph of the holder indicating the holder's name, a valid Dutch driver's licence, a valid driver's licence issued by the competent authorities in another Member State and bearing a photograph of the holder indicating the holder's name, travel documents for refugees and aliens or aliens' documents issued pursuant to the Aliens Act 2000. Corporates: For the identification of Dutch legal persons: an (online) extract from the Chamber of Commerce/Trade Register; a deed or statement drawn up or issued by a lawyer, a civil-law notary, a junior civil-law notary or a comparable, independent legal professional resident in the Netherlands or in another Member State; a document showing that a religious community, or a religious body in which it is united, is affiliated with the Interchurch Contact in Government Affairs (Interkerkelijk Contact in Overheidszaken) or that the religious community or religious body has been designated as an institution as referred to in section 6.33(1)(b) of the Income Tax Act 2001(Wet Inkomstenbelasting 2001); a document showing that an independent section of a religious community forms part of that religious community and the religious community fulfils the statutory provisions.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	If documents do not originate from public authorities or the courts, the institution will question if the documents are sufficiently reliable. Usually, such documents will, in and by themselves, be insufficient to verify identity in an adequate manner.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Ultimate Beneficial Owners need to be identified for legal entities. Their identity needs to be verified based on independent, reliable documents. Both identification and verification can be performed in a risk-based manner.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence arrangements are available for customers with a specific legal personality and a very technical and detailed set of products.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Based on the risk profile of the customer, transaction, product or country concerned, enhanced due diligence must always be carried out if: a) the customer is not physically present; b) the customer is a PEP; c) there is a correspondent banking relationship; or d) if facts or circumstances, including the country where the customer lives or is established, suggest a higher risk of money laundering or terrorist financing.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Enhanced due diligence measures are required in the case of transactions or business relationships with PEPs who live in a different country or Member State (regardless of their nationality), or who live in the Netherlands with a non-Dutch nationality.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Enhanced due diligence is required for all correspondent banking relationships outside the EU, whereby a number of factors need to be taken into account including, but not limited to: a) obtaining sufficient information to obtain a full picture of the nature of the bank's activities; b) evaluation of the reputation of the bank and quality of oversight based on publicly available information; and/or c) evaluation of procedures and measures to prevent money laundering and terrorist financing.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	It is forbidden to enter into a correspondent banking relationship with a shell bank. In addition, banks are not permitted to enter into or continue a correspondent banking relationship with a credit institution that allows shell banks to use their accounts.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Identification in person is not obligatory in all circumstances. In summary, payment of services has to be done from a bank account. There are no additional requirements in local regulations or guidance. If identification cannot be done face-to-face this is regarded as high risk and is required to be adequately mitigated by enhanced due diligence.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Financial Intelligence Unit-Nederland: www.fiu-nederland.nl
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 – 202,164 SARs GDP (in current prices): 2013 – USD864,169m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD4.27m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Institutions with a duty to report are required to report unusual transactions. Guidance on objective and subjective indicators by industry sector which may indicate unusual transactions is provided on the FIU's website: http://en.fiu-nederland.nl/content/list-indicators
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	There are several different thresholds in place for a variety of objective indicators. There is no threshold for subjective indicators. See a list of thresholds on the FIU's website: http://en.fiu-nederland.nl/content/list-indicators
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	There are penalties for non-compliance with the legal requirements.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Monitoring of the business relationship needs to be performed by the institution itself.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	The Netherlands has an established Data Protection Act: Wet bescherming persoonsgegevens (Wbp: Dutch Data Protection Act). a) personal data is defined in a very broad manner in the Netherlands: "personal data shall mean: any information relating to an identified or identifiable natural person"; (art. 1 sub a. Wbp). It is therefore very likely that personal data held for KYC purposes is covered by this Act; b) art. 2 Wbp states: "This Act applies to the fully or partly automated processing of personal data, and the non-automated processing of personal data entered in a file or intended to be entered therein". Given the scope definition, corporate data is not covered by the Dutch Data Protection Act; and c) article 16 Wbp contains a prohibition on the processing of sensitive personal data (such as religion, race, political persuasion, health and criminal past), unless one of the exemptions listed in articles 17-23 Wbp apply. Pursuant to Article 23(1)f Wbp, the Dutch DPA may grant an exemption, if this is required in view of substantial general interest and appropriate guarantees are offered to protect personal privacy.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	a) there are no specific restrictions on the transfer of credit reports; b) concerning criminal records, art. 16 Wbp states that the processing of criminal personal data is not permitted: "It is prohibited to process personal data concerning a person's religion or philosophy of life, race, political persuasion, health and sexual life, or personal data concerning trade union membership, except as otherwise provided in this Section. This prohibition also applies to personal data concerning a person's criminal behaviour, or unlawful or objectionable conduct connected with a ban imposed with regard to such conduct." However, art. 22(2)a Wbp lists an exception: "The prohibition does not apply to responsible parties who process these data for their own purposes with a view to: a. assessing an application by data subjects in order to take a decision about them or provide a service to them". This exception only applies if the company is analysing the data itself. If third parties are involved, art. 31(1)c applies and a prior investigation has to be performed: "The Data Protection Commission shall initiate an investigation prior to any processing for which responsible parties plan to process data on criminal behaviour or on unlawful or objectionable conduct for third parties other than under the terms of a licence issued under the Private Security Organisations and Investigation Bureaus Act." Companies within a concern are not subjected to a prior investigation; and c) concerning medical data, the restriction of art. 16 Wbp also applies. Exceptions are stated in art. 21 Wbp. Regarding Pension Funds, art. 21(1)f states: "The prohibition on processing personal data concerning a person's health, as referred to in Article 16, does not apply where the processing is carried out by: administrative bodies, pension funds, employers or institutions working for them, provided that this is necessary for: 1°. the proper implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the state of health of the data subject, or a. 2°. the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity."

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	There are no specific restrictions on the transfer of personal data to the Netherlands. Transfer of data within the European Union: The Wbp does not have any individual provisions governing data movements within the European Union ("EU"), as the Wbp implements the European Directive for the Dutch jurisdiction. Data movement from the Netherlands to another EU Member State thus only has to conform to the general requirements of the Wbp. Transfer to countries outside the European Union: The Wbp has specific provisions for the movement of data to countries outside the European Union, the third countries (Chapter 11 Wbp). Third countries are all countries outside the European Union, with the exception of the countries of the European Economic Area ("EEA"). The countries of the EEA (Norway, Liechtenstein and Iceland) have undertaken to implement the directive in their own legislation. Appropriate level of protection: The primary rule is that personal data may only be transferred to a third country if the general requirements of the Wbp have been conformed to and the third country ensures an adequate level of protection. For a number of countries, the European Commission has adopted decisions regarding the adequacy of the level of protection. No adequate level of protection: If a third country does not provide an adequate level of protection, there are two possibilities for still being entitled to transfer data to these third countries: a) Transfer based on the exceptions mentioned in the Act (Art 77(1) Wbp); or b) Transfer based on a permit issued from the Minister of Justice. Such a permit will be made subject to additional conditions that serve as a guarantee for the protection of personal data. To apply for the permit, a form must be used. The granting of such a permit will be facilitated if the model contracts prepared by the European Commission are used for the transfer.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Norway

Key contact: Gunnar Holm Ringen
Email: gunnar.holm.ringen@no.pwc.com
Tel: +47 95 26 0175

Postal address: P.O.Box 748 Sentrum,
N-0106 Oslo,
Norway

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	15 Apr 2009. A new Circular No. 8/2009 was published by the Financial Supervisory Authority of Norway on 23 Jun 2009.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	For (a) and (b): Finanstilsynet (The Financial Supervisory Authority of Norway): http://www.finanstilsynet.no/en
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, guidance by The Financial Supervisory Authority of Norway – Circular no 8/2009: http://www.finanstilsynet.no/no/Artikkelarkiv/Rundskriv/2009/2-kvartal/Veiledning-til-ny-lov-og-forskrift-med-tiltak-mot-hvitvasking-og-terrorfinansierin
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, risk based customer due diligence and monitoring customer relationships on an ongoing basis.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, the report is dated Dec 2014: http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/Mutual-Evaluation-Report-Norway-2014.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No. However in some exceptions the limit is: NOK40,000 (approx. USD4,559). For example, dealers in movable property, including auctioneers, commission agents and etc.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: A natural person's identity is normally verified by producing a document issued by a public authority, which normally contains full name, signature, photograph and personal identity number or D-number (non-residents liable to pay tax are registered with a unique D-number). Examples of suitable documents include a passport, bank card and driving licence. Corporates: A legal person's identity is verified by the Certificate of Registration/Certificate of Incorporation from the Public Register.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Normally, the establishment of a non-face-to-face business relationship is not allowed and the customer must physically appear either at the reporting financial institution or at an agent or outsource company where identification and verification is performed. Copies can be certified in exceptional circumstances and must be verified by authorised persons, including postal employees, the police and lawyers or two adult persons.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The Money Laundering Act ("MLA") requires financial institutions (and many others) to verify the identity of beneficial owners on the basis of reasonable measures. The MLA defines 'beneficial owners' generally as the 'natural persons who ultimately own or control the customer and/or on whose behalf a transaction or activity is being carried out'. The definition is then further elaborated to describe five situations where a person 'in all cases' is to be regarded as a beneficial owner.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Norway has introduced simplified customer due diligence procedures. If a customer or transaction falls into specific cases, simplified customer due diligence will apply, such as: a) financial undertakings listed in the Money Laundering Regulations; b) a financial institution in the European Union ("EU") and European Economic Area ("EEA"), and their correspondent financial institutions, which are compliant with the relevant FATF Recommendations; c) financial undertakings listed in the Money Laundering Regulations; d) a financial institution in the European Union ("EU") and European Economic Area ("EEA"), and their correspondent financial institutions, which are compliant with the relevant FATF Recommendations; e) a financial institution listed or regulated in an EEA state or a financial institution subject to disclosure requirements consistent with those that apply to listing on a regulated market in an EEA state; and f) a Norwegian state or municipal administrative body.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	The MLA requires financial institutions to apply 'other customer due diligence measures', in addition to the basic customer due diligence measures stipulated in the MLA in the following cases: a) situations that by their nature involve a 'high risk of transactions associated with proceeds of crime' or certain designated offences listed in the Criminal Code (including terrorist financing and terrorism offences); b) business relationships and transactions with PEPs; and c) correspondent banking relationships.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Reporting entities are required to conduct 'appropriate customer due diligence measures' to verify whether the customers are PEPs. Such measures include: a) obtaining approval from senior management before establishing a customer relationship; b) taking appropriate measures to ascertain the origin of the customer's assets and of capital involved in the customer relationship or the transaction; and c) carrying out enhanced ongoing monitoring of the relationship.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	When establishing cross-border correspondent banking relationships with institutions outside the EEA area, institutions are required to: a) gather sufficient information concerning the correspondent institution to fully understand the nature of its activities and, on the basis of publicly available information, to determine the reputation of the institution and the quality of supervision; b) assess the institution's control measures; c) ensure that the decision maker obtains approval from senior management before establishing a new correspondent relationship; d) document the respective responsibilities; and e) ascertain that the correspondent institution conducts ongoing monitoring of customers.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	The former requirement of face-to-face relationships is replaced by the implementation of risk based customer due diligence and ongoing monitoring of customer relationships.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	To ØKOKRIM; (Norwegian FIU), the National Authority for Investigation and Prosecution of Economic and Environmental Crime in Norway: http://www.okokrim.no/artikler/in-english

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 - 795 SARs GDP (in current prices): 2014 - USD499,817m (Source: data.worldbank.org) This results in a ratio of 1 SAR for every USD628.7m of GDP.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	International wire transfers, foreign exchange and foreign credit and debit card transactions are reported to the: a) foreign Exchange; b) foreign Currency Register with the Norwegian Directorate of Customs; and c) excise.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, breaches of the Money Laundering Act can be punished with fines or imprisonment for up to one year when special aggravating circumstances exist.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Yes, financial institutions have an obligation according to the Money Laundering Act to use electronic suspicious transaction monitoring systems.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes, as the principal rule, suspicious transactions shall not proceed before a report is made to the FIU (ØKOKRIM). ØKOKRIM can decide that the actual transaction shall not be effected.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	This is not mentioned in the regulations.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	Yes, with reference to ISA 250.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) every year; b) to the owners of the company, and in some cases to authorities; and c) yes.

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	It is risk based. Can be none of the above, some or even more.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	a) yes; b) it is unclear and complicated; and c) yes, sensitive personal data includes information relating to: a. racial or ethnic origin, or political opinions, philosophical or religious beliefs; b. the fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act; c. health; d. sex life; and e. trade-union membership.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes, prohibitions exist.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Specific privacy legislation exists for certain sectors e.g. public sector, telecom sector which apply in addition to the Privacy Act.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No, this is likely to not be the case.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Poland

Key contact: Damian Kalinowski
Email: damian.kalinowski@pl.pwc.com
Tel: +48 519-507-197

Postal address: Aleja Armii
Ludowej 14
00-638 Warszawa

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Act on Countering Money Laundering and Terrorist Financing (2000) became effective in 2001. The Act was amended to provide for implementation of the Third EU Anti-Money Laundering Directive which took place on 25 Jul 2009 and came into effect on 22 Oct 2009.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) the Polish Financial Supervisory Authority (http://www.knf.gov.pl/index.html) supervises financial institutions in full cooperation with the General Inspector of Financial Information ("Generalny Inspektor Informacji Finansowej") within the Ministry of Finance (http://www.mf.gov.pl/en/aml-ctf/news); and b) the National Bank of Poland is responsible for the supervision of the currency exchange officers and the National Savings and Credit Cooperative Union supervises the credit unions.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The Polish Banking Association ("ZBP") developed guidance concerning AML practices. The Regulator provides limited guidelines concerning AML procedures which are published on the website of the General Inspector of Financial Information.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The most recent Report on Fourth Assessment Visit on Poland was conducted by MONEYVAL and published on 11 Apr 2013: http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round4/PL4-SUMMMONEYVAL%282013%292_en.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Any obligated institution shall apply financial security measures for its clients. Their scope is determined on the basis of risk assessment as for money laundering and terrorist financing, resulting from the analysis, taking into account in particular type of a client, economic relationships, products or transactions. There is no minimum threshold, under which customer due diligence is not required. However, any obligated institution, taking into account the risk of money laundering or terrorist financing, may waive the above for: a) life insurance policies, where an annual premium shall not exceed the equivalent of EUR1,000, or a single premium shall not exceed the equivalent of EUR2,500; and b) electronic money, if: – the maximum amount stored in the device does not exceed the equivalent of EUR250 - in the case of a device that cannot be recharged – the maximum amount of transfers of electronic money does not exceed the equivalent of EUR2500 per calendar year in question – unless the redemption amount of electronic money shall be at least equivalent of EUR1,000 per calendar year in question.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Determining and noting the distinguishing features of a document confirming the person's identity pursuant to separate regulations, or of a passport, as well as the first name, last name, the citizenship and address of the person executing the transaction, and furthermore the PESEL (national citizens' registry) number in the case of the identification on the basis of identity card or date of birth for a person without a PESEL number, number of ID for foreigners and country code in the case of the passport. Legal entities: Up-to date information from a court registry extract or other document specifying its name, the organisational form of the legal entity, its location, address and tax ID number, as well as the name, surname and PESEL or date of birth of the person executing the transaction to represent the legal entity.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Not stated in local regulations or guidance regarding external third party certification. Certification of copies of identification documents may be made by a state authority, a notary public or a lawyer.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Local guidance requires verification of the identity of appropriate beneficial owners holding 25% or more. Where a principal owner is another corporate entity or trust, the firm should take measures to establish the identities of its beneficial owners or trustees, unless that company is publicly traded. The entity will then judge which of the beneficial owners exercise effective control, and whose identities should therefore be verified.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence arrangements may be applied for: a) customers providing financial services, registered in EU or in equivalent country; b) central/local government entities; c) life insurance arrangements (if year contribution is less than EUR1,000 or one time contribution is less than EUR2,500); d) insurance policy if the policy cannot be transferred to a different person and cannot be credit provision; e) electronic money if the value is less than EUR250; f) transactions where the supplier can track the transfer and it is less than EUR1,000; or g) companies whose securities are admitted to public trading on a regulated markets in at least one European Union member state or in an equivalent country. However, the institutions always need to take into account the risk of money laundering and terrorist financing.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence is required in situations that might pose higher money laundering or terrorist financing risk, particularly for: a) transnational relations with institutions acting as correspondents based in countries other than EU or equivalent; b) PEPs; or c) the establishment of a non-face-to-face business relationship.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	The Act on counteracting money laundering and terrorism financing 16 Nov 2000 highlights that PEP status applies only to PEPs domicile outside the territory of the Republic of Poland. Article 9e requires that in the case of PEPs obligated institution: a) apply measures, adequate to the risk determined by the institution, in order to establish the source of funds; b) maintain constant monitoring of conducted transactions; c) conclude a contract with a client after having obtained the consent of the board, the designated member of the management board or a person designated by the board or a person responsible for the activities of the obligated institution; and d) may collect written statements on whether a client is a person holding a politically exposed position, which are given under the penal liability for providing data incompatible with the facts.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Article 9e of the Act requires that enhanced due diligence should involve further consideration of the following elements, designed to ensure that the bank has secured a greater level of understanding with corresponding banks overseas (other than those based in the EU or other states with equivalent AML regulations): a) collect information allowing the correspondent to determine the scope of operations and whether the respondent is supervised by a competent regulator; b) assess measures taken by the respondent in counteracting money laundering / terrorism financing; c) prepare documentation determining the scope of responsibilities of the correspondent and respondent; d) ascertain with respect to payable through accounts that the respondent has taken appropriate actions in accordance with procedures on the application of CDD measures in respect of clients having direct access to the respondent's bank accounts and that such information could be provided upon request; and e) obtain consent of senior management.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Article 9e of the Act requires that establishment of a non-face-to-face business relationships require enhanced due diligence. As a minimum, one of the following actions is required: a) verification of the customer's identity against additional documents; b) certification of copies of identification documents by an appropriate authority; or c) confirmation that the customer's initial transaction was made through an account in the customer's name with another financial institution.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	General Inspector of Financial Information: http://www.mf.gov.pl/en/aml-ctf/news

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 3,637 SARs (Source: General Inspector of Financial Information – activity report for the year 2014). GDP (in current prices): 2014 – USD548.0m (Source: data.worldbank.org). This results in a ratio of 1 SAR for every USD150.6m of GDP.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, Article 8 requires that certain transactions above the threshold of EUR15,000 as well as related transactions where the aggregated amount exceeds the threshold should be registered. In case of casino obligation involves any purchase or sale of gambling chips of the value equivalent to at least EUR1,000. Article 8 provides exemptions to the requirement to report <i>inter alia</i> in the case of incoming transfers unless they are cross border, or transfers between accounts of the same customer, transfers on the interbank market. In addition according to Article 8 any obligated institution is required to register a transaction, the circumstances of which may suggest that it was related to money laundering or terrorist financing, regardless of its value and character.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Article 34a provides for fines where an obligated institution fails to register any transactions above the required threshold of EUR15,000. Article 34c provides that such fines will be for an amount not higher than PLN750,000 (approx. USD185,000). In accordance with Article 35(1) failure to register a transaction, to submit documentation relating to the transaction to General Inspector of Financial Information or to store the register of such transactions or documentation for the required period of time, maintain financial security measures, to report suspicious activity, to suspend a transaction or block an account, to introduce internal AML/CTF or designate a person responsible for fulfilling obligations stated in the Act can result in the punishment of imprisonment for up to three years. Pursuant to Article 35(2) tipping off is subject to a sentence of imprisonment for up to three years. Pursuant to Article 36, refusal to submit information or documents to the General Inspector, submission of false data or concealing real data on transactions, accounts or persons can result in punishment up to five years. If substantial damage had been caused as a result of committing acts described above, guilty person might be a subject to the punishment of imprisonment up to eight years.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Suspicious transactions reported to the regulator should be suspended for 24 hours. If the regulator does not request further suspension of a transaction it can be processed. Based on the regulator's request a transaction can be suspended or account blocked for further 72 hours. A prosecutor can suspend a transaction or block an account for up to three months.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	The Act provides that as a rule it is the Polish General Inspector of the Financial Information that is officially authorised to monitor the transactions. However, bearing in mind that the Act implements the EU regulations (that should have been implemented by all Member States), it is likely that a transaction may be subject to monitoring outside Poland, on the basis stipulated by the local law of the foreign party of the transaction, especially in cases where a given transaction is performed with or via a foreign entity.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, Poland has established personal data protection laws. a) yes; b) although corporate data is not considered as personal data, the processing of natural persons data (such as the representatives of a company) is subject to personal data protection law; and c) Polish data protection law provides a catalogue of "sensitive personal data". They include data on: racial or ethnic origin, political opinions, religious or philosophic beliefs, religion, party or trade-union membership, data concerning health, genetic code, addictions, sexual life, data relating to convictions, decisions on penalty, fines and other decisions issued in any court or administrative proceedings. The processing of such data, as a general rule, is prohibited, unless one of the requirements permitting such processing is provided (e.g. the data subject provides written consent in that respect, such data processing is necessary to protect the data subjects interests, specific provisions of law enable such data processing etc.). Additional protections that apply to the processing of sensitive personal data include: prohibition of processing sensitive personal data before a data filing system is registered in the Polish Data Protection authority's register, an obligation to apply medium security level for protecting the data processed within IT systems without connection to the internet and high security level for protecting the data processed within IT systems connected to the internet.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Information included in the credit reports is covered by the banking secrecy rules, which provide for a general prohibition on the data transfer (with certain exceptions). Criminal record and medical data constitute in turn sensitive data, which is subject to the limitations described in A29.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Polish Personal Data Protection Act, Polish Banking Law and other regulations on professional secrecy (brokerage secrecy, insurance secrecy etc.) including, amongst others, the Act on Financial Instruments Trading, Act on Insurance Activity and Act on Payment Services. Poland does not have a case law in the meaning of institution of common law. However the jurisprudence of Polish courts and the decisions of the Polish Data Protection authority provide guidelines how to transfer such information.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. The relevant law is contained in the Polish Banking Law, Act on Financial Instruments of Trading, National Bank of Poland Act, Act on Insurance Activity and the Act on Payment Services. The Polish Banking Law applies in the case of banks, their employees and anyone through whom the bank undertakes banking acts. They are bound by banking secrecy, which is applicable to all information regarding a banking act, whether obtained in the course of negotiations, or during the conclusion or performance of an agreement on the basis of which the bank undertakes the act. Some financial institutions and their employees are also obliged to keep their professional secrecy and there are specific regulations as to when data sharing may take place. Usually, this may happen upon written consent of their client. In addition, certain information of technical, technological, commercial or organisational character regarding the entrepreneur is covered by law concerning trade secrecy and cannot be revealed to third parties, if it was not disclosed to the public and the trade partner was directly advised by the client not to disclose such information.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Portugal

Key contact: Ines Correia Neves
Email: ines.correia.neves@pt.pwc.com
Tel: +351 21 359 93 35

Postal address: Palacio Sottomayor;
Rua Sousa Martins 1-2; 1069-316;
Lisbon; Portugal

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Law No.25/2008 came into effect on 10 Jun 2008 and gave effect to the EU Third Money Laundering Directive. Law no. 52/2003 (Anti-Terrorism Law) was amended in 2007 which created a new independent and free standing offence of financing terrorism.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	Article 38 of Law No.25/2008 provides that the supervisory authorities with responsibility for AML controls are as follows: a) The Bank of Portugal (Banco de Portugal) (http://www.bportugal.pt/en-US/Pages/inicio.aspx); b) Securities Market Commission (Comissão do Mercado de Valores Mobiliários) ("CMVM") (http://www.cmvm.pt/en/Pages/default.aspx) and Insurance and Pension Funds Supervisory Authority (Autoridade de Supervisão de Seguros e Fundos de Pensões) ("ASF") (http://www.asf.com.pt/EN); and c) The Service for Gambling Inspectorate in respect of casinos and operators awarding betting or lottery prizes (Serviço de Inspeção de Jogos do Turismo de Portugal), Institute for Construction and Real Estate for real estate agents as well as agents buying and reselling real estate and construction entities selling property directly (Instituto da Construção e do Imobiliário), Economy and Food Safety Authority for persons trading in goods, only to the extent that such payments are made in cash in an amount of EUR15,000 or more (Autoridade de Segurança Alimentar e Económica), The Order of Statutory Auditors (Ordem dos Revisores Oficiais de Contas), Chamber of Chartered Accountants (Câmara dos Técnicos Oficiais de Contas), The Institute for Registrars and Notaries (Instituto dos Registos e do Notariado), The Bar Association (Ordem dos Advogados) and The Chamber of Solicitadores (Câmara dos Solicitadores).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	N/A
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No, however entities should retrospectively review documentation to identify pre-existing customers based on materiality and risk criteria, namely the characteristics of the account, the customer and the business relationship with the customer in order to identify accounts that need an immediate update.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, Article 10 of Law No.25/2008 provides that in compliance with identification and diligence duties, financial institutions can adapt the nature and scope of the verification and due diligence procedures, taking into account the risk associated with the type of customer, the business relationship, the product, the transaction and the origin or the purpose of the funds.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The last IMF Country Report was published in Apr 2014. The report is the eleventh country review under the extended arrangement and request for the extension of the arrangement and waivers of applicability of End-March Performance Criteria. The report can be accessed here: http://www.imf.org/external/pubs/cat/longres.aspx?sk=41494.0 Portugal has not been subject to an FATF review in the last three years. The most recent Third Round Mutual Evaluation Report was published on 13 Oct 2006. The most recent Second Biennial Update to the Mutual Evaluation of Portugal was published in Sep 2010: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/PT_SecondUpdateReport_2010.pdf An on-site evaluation is scheduled for 2017.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, Article 7 of Law No.25/2008 provides an exemption for occasional transactions under EUR15,000. For financial institutions, according to Notice 5/2013 of Banco de Portugal, the threshold is EUR15,000 in the case of one off or linked transactions and EUR10,000 and EUR5,000 for cash deposits respectively made by the client or a third person (when the client is considered as high risk client).
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: should provide a valid document with: Full name, signature, date of birth, nationality, address, profession, work address, tax identification number and photo and politically exposed job/function, purpose. Legal persons: should provide a valid document with the headquarters address, identification number (should be made through the card named Cartão de Identificação de Pessoa Colectiva), shareholder identification for individuals who hold more than 25% of the voting rights and identification of the board of directors. For non-resident entities, equivalent documentation is required.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	The copies of documentation can be certified by external third parties such as notaries.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Management Board and shareholder identification must be obtained for individuals who hold more than 25% of the voting rights. Identification and verification requirements for beneficial owners are the same as those for individuals or companies listed above.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Articles 11 and 25 provide that except where there are suspicions of money laundering or terrorist financing, simplified due diligence can be adopted in the following situations: a) financial entities shall not be subject to the identification requirement where the customer is a financial entity set up in a European Union Member State or in a third country which imposes equivalent requirements in respect of money laundering and terrorist financing prevention; b) the customer is a listed company whose securities have been admitted to trading in a regulated market in any EU Member State, as well as listed companies in third country markets, which are subject to equivalent reporting obligations; c) the customer is the State, autonomous regions, local authorities, a legal person governed by public law, of any nature, integrated in the central, regional or local governments; d) the customer is a public authority or body with transparent accounting practices and subject to monitoring; e) the customer is the entity providing postal services or is the Treasury and Government Debt Agency; f) issuance of electronic money, whose monetary value is stored on an electronic device and represents a claim on the issuer, issued on receipt of funds or an amount not less than the monetary value issued and accepted as a means of payment by undertakings other than the issuer; g) life insurance policies, pension fund contracts or similar savings schemes where the annual premium or contribution is no more than EUR1,000 or the single premium is no more than EUR2,500; h) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral; and i) pension superannuation or similar schemes that provide retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Article 12 provides that entities should apply enhanced due diligence measures in respect of customers and transactions which by their nature or characteristics present a higher risk of money laundering or terrorist financing. This includes: a) non-face-to-face transactions and in particular to those operations that may favour anonymity; b) operations carried out with PEPs resident outside the jurisdiction; and c) correspondent banking operations with credit institutions established in third countries and any others designated by the competent supervisory or monitoring authorities.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Article 12(4) provides that a non-resident PEP relationship requires additional due diligence. When establishing a relationship with a non-resident PEP entities should: a) have appropriate risk-based procedures to determine whether the customer is a PEP; b) have senior management approval for establishing business relationships with such customers; c) take adequate measures to establish the source of wealth and the source of funds that are involved in the business relationship or occasional transaction; and d) conduct enhanced ongoing monitoring of the business relationship.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Enhanced due diligence is not required in the case of correspondent banking relationships with financial institutions in EU Member States. Article 26 provides in the case of cross border relationships with institutions in third countries that the following enhanced due diligence measures should be adopted: a) the correspondent should gather sufficient information about a respondent institution to fully understand the nature of the respondent's business, to assess the respondent institution's anti-money laundering and anti-terrorism financing controls and to determine from publicly available information the reputation of the institution and the characteristics of its supervision; b) approval should be obtained from senior management before the establishment of a new banking relationship and the respective responsibilities documented; and c) if the correspondent relationship involves payable through accounts, the institution shall be satisfied that the respondent has verified the identity of the customer and performed due diligence on the customer having direct access to the accounts, ensuring that all these elements of information can be provided upon request.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Article 12 provides that non face-to-face relationships (especially those that can favour anonymity) require enhanced due diligence. In these cases, the institution should demand additional documentation or information considered adequate to check or certify the data provided by the customer and ensure the first credit or debit is made through an account opened in the customer's name.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	SARs are made to Policia Judiciaria: http://www.pj.pt/

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Articles 16 and 53 provide that failure to report suspicious activity is an offence. Articles 19 and 53 provide that disclosure as to the making of such a report constitutes an offence. Article 54 provides that breaches of regulations outlined in Article 53 shall be punishable as follows: a) where the offence is committed within the scope of activity of a financial entity: a. by a fine from EUR25,000 to EUR2.5m, where the offender is a legal person; and b. by a fine from EUR12,500 to EUR1.25m where the offender is a natural person; b) where the offence is committed within the scope of activity of a non-financial entity, with the exception of lawyers and solicitors: a. by a fine from EUR5,000 to EUR500,000, where the offender is a legal person; and b. by a fine from EUR2,500 to EUR250,000, where the offender is a natural person. Article 55 provides for the imposition of additional penalties which includes prohibition or publicity.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.
AML Audits	
Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Notice of Banco de Portugal No 9/2012 defines the risk management information report regarding anti-money laundering and terrorism financing internal control. This report must be attached with a formal opinion from the bank's audit committee or equivalent body.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) the report is provided annually; b) the report is submitted to Banco de Portugal; and c) no.
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	a) yes; b) notice 25/2008 does not prevent financial institutions and non-financial entities exchanging information that concerns a joint business relationship on the same client, if their sole purpose is preventing money laundering and terrorist financing. In addition, all entities are subject to equivalent obligations of professional secrecy and protection of personal data is established in other Member States of the European Union or equivalent third country prevention of money laundering and terrorist financing; and c) yes.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	There are no prohibitions within the EU.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes.



At PwC United Kingdom, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com/UK.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2016 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

151103-144408-LA-OS

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Romania

Key contact: Ana Sebov
Email: ana.sebov@ro.pwc.com
Tel: +40 212 25 3608

Postal address: Lakeview Office,
301-311 Barbu Vacarescu Street,
RO-020276, Bucharest, Romania

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Law No. 656 on prevention and sanctioning of money laundering, as well as for establishing measures for the prevention of and fight against financing terrorist acts was published in 2002 with subsequent amendments. In 2008, the Regulation to the Law 656 was published, and issued through the Government Decision No. 594. Law 535 on prevention and sanctioning of terrorism was published in 2004. In 2006, the Decision of the National Office for Prevention and Control of Money Laundering No 496 was published, setting out the local regulatory framework for the prevention and sanctioning of money laundering, as well as for establishing measures for the prevention of and fight against the financing of terrorist acts for the entities not being supervised by specialised authorities In 2007, the Chamber of Financial Auditors issued Decision No. 91 applying the specific legislation for the prevention and sanctioning of money laundering and financing terrorist acts by the financial auditors. This Decision is being reviewed now and it is expected that it will be replaced in early 2016. In 2012 the Chamber of Fiscal Consultants issued the Decision No. 7 approving the Norms for the prevention and sanctioning of money laundering and financing terrorist acts by fiscal consultancy activities
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) The National Office for Prevention and Control of Money Laundering (www.onpcsb.ro) and National Bank of Romania (www.bnro.ro); b) The National Office for Prevention and Control of Money Laundering (www.onpcsb.ro) and the Financial Supervision Authority (www.asfromania.ro); and c) The National Office for Prevention and Control of Money Laundering (www.onpcsb.ro), the Chamber of Financial Auditors (www.cafr.ro) and the Chamber of Fiscal Consultants (www.ccfiscali.ro).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The National Office for Prevention and Control of Money Laundering organises training seminars at least once a year regarding the prevention of money laundering and of financing of terrorist acts. In addition, the National Office for Prevention and Control of Money Laundering has issued a number of guides and handbooks (http://www.onpcsb.ro/html/instruire.php?section=3).

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes. Article 14 of Law 656/2002 includes the requirement to apply KYC measures also to historic clients as soon as possible.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, the 2008 amendments to the Law 656/2002 established the standard, simplified and enhanced customer due diligence rules and procedures.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, in Apr 2014. Please see (http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round4/ROM4_MERMONEYVAL(2014)4_en.pdf).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, transactions below EUR15,000. However, the KYC procedure must be performed for all clients where a transaction appears suspicious and a report should be made to the National Office for Prevention and Control of Money Laundering even if the transaction is lower than EUR15,000. Exceptions: a) casino chip exchange below EUR2,000; and b) life insurance, where the premium or yearly payment of these are lower or equal to the equivalent in of EUR1,000.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals need to provide the following details: a) name and surname; b) date and place of birth; c) personal identity number or, if is the case, another similar unique element for identification; d) the domicile and, if is the case, the residence; e) telephone number, fax, electronical address, if is the case; f) citizenship; g) qualification as resident or non-resident; and h) the public function, for foreigners that are residents of another country, if is the case. Part of the details above can be verified by an identity card or passport. Legal entities need to provide the following details: a) number, series and the date of the certificate/document of registration with the National Office of Trade Registry or other authorities; b) name; c) unique registration code, or its equivalent for foreign legal entities; d) credit institution and the International Bank Account Number ("IBAN"); e) the complete address of headquarters or, if is the case, of the subsidiary; f) telephone, fax and, if is the case, the email and the internet page; and g) the scope and nature of the transactions/operations performed with the customer. Part of the information can be verified by an official extract from The National Trade Registry Office which proves existence of the entity. This applies to customers and beneficiaries as well.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	There are no special requirements, but the verification via independent sources is required for specific clients based on the risk assessment.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Beneficial owners are subject to the following requirements: a) identification and verification of their identity by taking risk-based and adequate measures; b) gathering of information on the purpose and nature of the established business relationship; and c) conducting continual monitoring of the business relationship with the respective customer.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence arrangements apply to: a) domestic public authorities; b) life insurance under the conditions mentioned in the law and subscription to pension funds; c) electronic currency as defined by the regulations; d) a credit or financial institution from an European Union ("EU") member state or from the European Economic Area ("EEA"), or a credit or financial institution from a non-EU state or from a state outside the EEA that imposes similar anti-money laundering and counter terrorist financing requirements and supervision; e) entities admitted to trading on EU-based regulated markets or non-EU regulated markets that ensure a similar level of protection; f) beneficial owners from transactions that are performed through collective accounts managed by public notaries, lawyers or similar officers from EU Member States or non-EU states that ensure a similar level of protection; and g) transactions and products that are low risk in respect of money laundering and the financing of terrorist acts.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence measures are required in the following cases: a) non face-to-face transactions; b) in the case of correspondent relationships with credit granting institutions from non-EU countries and those countries that are not part of the EEA; c) transactions or business relationships with politically exposed persons who are resident in another EU member state or in the EEA, or in non-EU countries or countries outside the EEA; and d) in any other cases where it is considered that due to their nature, a high risk in respect of money laundering and the financing of terrorist acts is present.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Additional due diligence is required for transactions or business relationships with PEPs who are resident in another EU member state or in the EEA, or in non-EU countries or countries outside the EEA.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Enhanced due diligence must be performed for cross-border correspondent banking relationships with credit institutions in third countries.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, the law specifies that credit institutions will not enter into correspondent relationships with a fictitious bank or with a credit institution where it is known that it allows a fictitious bank to use its accounts.
Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	Additional due diligence is required for all non-face-to-face transactions.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The National Office for Prevention and Control of Money Laundering (http://www.onpcsb.ro/html/english.php).
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, cash transactions in excess of EUR15,000 have to be reported to National Office for Prevention and Control of Money Laundering by individuals and other legal entities that sell goods and services.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Yes, cash transactions below EUR15,000 are not required to be reported unless the respective transaction is identified as suspicious.
Q22.	Are there any penalties for noncompliance with reporting requirements e.g. tipping off?
A22.	Non-compliance is considered a misdemeanour and certain sanctions may be applied for noncompliance, ranging from fines to the closure of the entity breaching its obligation to report.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	There are regulatory requirements, applicable only to banks and other financial institutions.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Local persons who are obliged to report suspicious transactions may rely upon the KYC checks made by third parties (banks and financial institutions) from other Member States or from third countries applying KYC rules similar or equivalent to Romania there in.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	There is no specific legal requirement for an external auditor/other external organisation to report on the bank's AML systems and controls.
Q27.	If an external report on the bank's AML systems and controls is required: - how frequently must the report be provided? - to whom should the report be submitted? - is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: - sample testing of KYC files? - sample testing of SAR reports? - examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: - does the definition of "personal data" cover material likely to be held for KYC purposes? - how do the laws apply to corporate data? - does this country have a separate definition of "sensitive data"? How it defined and what is are the additional protections?
A29.	Yes, Romania's personal data protection legislation exists mainly in Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data. - yes; - they only apply in relation to the personal data of individuals; and - yes, it refers to "special categories of data", and it includes personal data regarding ethnic or racial origin, political, religious or philosophical beliefs or those of a similar nature, trade-union allegiance, as well as personal data regarding the state of health or sex life, personal data regarding criminal or minor offences, as well as personal identification numbers or of other personal data with a general identification function. Additional protection depends on the category of data. In general, the additional protection consists of the requirement to process such data based exclusively on the express and unequivocal consent of the person. However, the processing of data regarding ethnic or racial origin, political, religious or philosophical beliefs or those of similar nature, trade-union allegiance, as well as personal data regarding the state of health or sex life is prohibited or it is very strictly regulated. Processing personal data regarding criminal offences committed by the data subject, or regarding previous criminal convictions, security measures or administrative or minor offence sanctions applied to the data subject, may be carried out only under the control of public authorities, within the limits of their powers given by law and under the terms established by the specific provisions in this field of law.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes. In general, transfer of data to another data controller means that a new process is made by a new data controller for its own purposes and that the authorisations obtained by the transferor to process any such special category of data may not automatically be transferred to the transferee along with the data. Therefore, such a transferee (data controller) must obtain all the necessary authorisations itself. However, if the transferee is merely a data processor working under the supervision of the data controller (transferor), then the data processor's activity should be deemed covered by the transferor's authorisation. However, should the data processor be located in a country outside of the EEA and which is not recognised as having a similar degree of protection of personal data, such transfer must be authorised by the Romanian Authorities.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Any processing of personal data in Romania falls under the protection of the Romanian laws regarding personal data processing.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. Under Government Emergency Ordinance 99/2006 on credit institutions and capital adequacy, all facts, data and information on the activity performed, as well as of any fact, data or information at the credit institution's disposal, regarding the person, property, activity, business, personal or business relationships of clients, or any information related to the clients' accounts (balances, flows, operations, services or contracts concluded with its clients) is protected by the banking secrecy law.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Russia

Key contact: Irina Novikova / Artem Kalinin
Email: irina.n.novikova@ru.pwc.com /
artem.kalinin@ru.pwc.com
Tel: +7 (495) 223-5106

Postal address: Butyrsky Val 10,
125047,
Moscow

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2001.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The Central Bank of the Russian Federation is the main regulator for AML controls in Russia (www.cbr.ru/eng/). Suspicious transactions are reported to the Federal Service of Financial Monitoring ("FSFM"). FSFM also an AML regulator for non-financial sector (http://www.fedsfm.ru/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	The regulator provides practical guidance in the form of regulations, instructions and official letters.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, KYC requirements are applicable to all clients, including those on-boarded before 2001.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, a risk based approach is approved by the local regulator, however its application is limited (refer to A12 and A13 for more information).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, in October 2013 the FATF recognised that the Russian Federation had made significant progress in addressing the deficiencies identified in the 2008 mutual evaluation report and could be removed from the regular follow-up process (http://www.fatf-gafi.org/countries/n-r/russianfederation/documents/fur-russia-2013.html).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Applicability of minimum transaction thresholds depends on the client type: a) all legal entities are subject to customer due diligence and no minimum transaction thresholds are applicable to such clients; and b) a minimum transaction threshold of RUB15,000 is applicable to specific transactions of natural person clients.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Russian law recognises the following means of verification of customer identification information: a) duly formalised / legalised official documents (irrespective of their source); b) information which can't be verified through official documents (e.g. phone number or actual address) can be verified by formal client representation (original or duly certified copy, signed by a legal representative); and c) information from 'official' sources, available to the bank on 'legal grounds' e.g. the official corporate registry ("EGRYUL") or the Federal Tax Service of Russia ("FTS").

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Russian law requires that identification documentation provided is an original or a duly certified copy. Depending on the type of document its copy can be certified as follows: a) by a notary public; b) by the client: "Certified True Copy of the original" – applicable only to documents issued by the client (special requirements to certifying requisites apply); and c) Bb the employee of the AML regulated entity provided this employee checks the original document (special requirements to certifying requisites apply).

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Russian law defines an Ultimate Beneficial Owner ("UBO") as a natural person who directly or indirectly owns 25% or more of the client's equity, or controls the client. Under Russian law, UBO identification requirements apply both to clients who are legal entities and to clients who are natural persons. There is no requirement to identify UBOs for the following client types: a) Russian government bodies (specific definition applies); b) government-owned entities (50% or more); c) international organisations and foreign governments; or d) companies with securities listed on a Russian exchange. A sole executive body of the client (General Director) may be recognised as the UBO for Russian law purposes if no UBOs under the Russian law definition exist or it is not possible to identify UBOs (proof necessary).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence ("SDD") as a concept is applicable only to natural persons who are provided with money transfers without account opening (including electronic money transfers). The scope of SDD is provided in Federal Law 115-FZ. However, certain limited simplifications are also applicable to other types of clients, e.g. UBO identification exemptions for client types described in A11.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced Due Diligence ("EDD") is not a concept explicitly prescribed by Russian AML legislation. Where SDD arrangements are not applicable, all clients are subject to the same level of Customer Due Diligence ("CDD"). The scope of CDD is provided in Federal Law 115-FZ and Regulations of the Central Bank of Russia 262-P. AML regulated entities may define additional due diligence requirements in their internal AML policies.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Russian law recognises a PEP relationship only in respect of natural person clients and clients' UBOs (however if UBO is a PEP, it triggers as a higher risk). Russian law distinguishes between Foreign and International Organisations' PEPs (according to FATF) and Russian PEPs (closed list of Russian officials). Additional due diligence measures in respect of PEP relationships are as follows: a) natural person clients being PEPs are on-boarded only upon written approval of the head of the organisation or their delegate; b) inquiries into the Source of Wealth are required for PEP relationships; and c) reporting of transactions of Foreign and International Organisations' PEPs is required.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Local regulations state that for the establishment of correspondent relationships, the institution shall request, in addition to standard identification information, documents and information about AML controls of the correspondent bank. The decision on the establishment of such relations shall be adopted with the consent of the head of the organisation or their delegate.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes, AML regulated entities are prohibited to deal with shell banks or with banks that deal with shell banks.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Dealing with natural persons where both natural person and their legal representatives are absent for identification is prohibited.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Reports are made to the Federal Service for Financial Monitoring (“FSFM”): http://www.fedsfm.ru/en
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Reporting requirements are based on multiple criteria (including cash transactions above a certain amount, unusual transactions etc.). Reporting requirements are extremely detailed and onerous and are listed in Federal Law 115-FZ and Regulations of the Central Bank of Russia #375-P.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No such de-minimis thresholds for reporting.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, penalties including revocation of license for non-compliance with reporting requirements can follow.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No. However, financial institutions have the right to reject a transaction that is classified as suspicious and report this rejection to FSFM.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Subject to banking secrecy legislation and inter-governmental agreements.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No. However, a review of AML controls is a mandatory procedure for the external auditor. Material gaps should be reported to authorities.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, Russia has established onerous personal data protection laws. Personal data has a very broad definition (including a person's name or any personal detail) and covers natural persons only (it does not cover company data unless it pertains to natural persons such as UBOs or Legal Representatives etc.). Thus the definition of "personal data" covers material likely to be held for KYC purposes. Consent is required for collecting, processing or transferring personal data. Data of both natural persons and legal entities is protected by banking secrecy regulations.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes, all client data is subject to banking secrecy law. No client information can be disclosed to third parties unless specifically allowed by law (e.g. disclosure to external auditors and regulators is permitted).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Slovakia

Key contact: Katerina Halasek Dosedelova
Email: katerina.halasek-dosedelova@cz.pwc.com
Tel: +420-251151293

Postal address: PricewaterhouseCoopers,
Slovensko s.r.o. Twin City Business Centre, blok A,
Karadžičova 2 815 32 Bratislava, Slovakia

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1994. This has been amended several times, and was fully replaced in 2008 by the Act no 297/2008 Coll., effective from 01 Sep 2008 and last amended in 2015: http://www.minv.sk/swift_data/source/policia/finpol/297_2008en.pdf Please note, the attached link does not reflect the changes according to the latest amendment as a new version of the act has not been translated into English yet. As of the latest amendment, the following minor changes have been adopted: a) in Article 5 sec. 1 subsec. b) a new point (14) has been added according to which a financial institution, agent of financial services and institution of electronic money are also considered as an obliged person; b) in Article 11 sec. 2 subsec. d) the sum of EUR150 has changed to EUR250; and c) in Article 5 sec. 1 subsec. n) has been added, according to which a creditor is also considered as an obliged person.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The key regulator for AML controls is the Financial Analytical Department ("FAU") of the Police under the Ministry of Interior of the Slovak Republic (http://www.minv.sk/?financna-policia) Controls are further regulated by: a) National Bank of Slovakia (www.nbs.sk) which is a supervisory authority of the financial market in the Slovak Republic as well as the Ministry of Finance of the Slovak Republic (www.finance.gov.sk); and b) administrative authorities and the Ministry of Finance supervise lotteries and other similar games, and holders of licenses to operate betting games.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, guidelines for submitting AML notifications issued by the FAU: http://www.minv.sk/?financna-policia AML Guidelines for the financial sector, issued by the National Bank of Slovakia: http://www.nbs.sk/en/financial-market-supervision/prevention-of-legalisation-of-proceeds-of-criminal-activity-and-financing-of-terrorism/recommendations-and-methodical-guidance

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, National bank have issued guidelines in respect of the banking sector: http://www.nbs.sk/_img/Documents/_Dohlad/ORM/BankyAOcp/MU_9_2012_EN.pdf
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last 3 years? If yes, please find a link to a relevant report (if publicly available).
A7.	No, the last was the MONEYVAL assessment, dated Sep 2011: http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Slovakia_en.asp

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, any single transaction below EUR15,000 does not require any customer due diligence unless it is: a) a suspicious transaction; b) an agreement to enter into a business relationship; c) a transaction with a PEP; d) as part of the business relationship when there are doubts about the veracity or completeness of clients identification data previously obtained; or e) a transaction concerning withdrawal of a cancelled final balance of bearer deposit. Also in the case of life insurance, customer due diligence is not required if the insurance premium payable per year does not exceed EUR1,000, or if payable in a lump-sum, does not exceed EUR2,500, as well as in certain situations related to pension scheme agreements (no amount set by law). An ordinary transaction below EUR2,000 does not need customer due diligence.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: Name, surname, birth identification number or date of birth, place of birth, gender, address and citizenship. These would normally be verified by an identity card or passport. Individuals who conduct business: In addition to the above, full name of the business, place of business and identification number needs to be noted. Legal entities: the full name, residency/seat, identification (or similar identification received from foreign offices) showing evidence of the company's existence (i.e. certificate of incorporation, trade register statement or other). The same principles for 'individuals' apply for the identification of individuals in the company's statutory body. If the company's statutory body or the owner is another legal entity, identification documentation must also be collected for that entity. The way of acting of the statutory representatives, acting on behalf of the legal entity must be proven, e.g. visible from the certificate of incorporation, trade register statement or other similar document, or power of attorney must be provided by the client.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	These should be certified by an appropriate person e.g. a notary, local authorities etc. Specific rules apply to credit and financial institutions, where certain employees are authorised to verify these when opening an account, concluding a contract etc.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The shareholders of a legal entity (with a minimum of 25% holding and/or voting rights) must be ascertained up to the level of the ultimate beneficiary of the transaction, if there are suspicions. Direct and indirect ownership identification requirements are the same as for the relevant legal entity and/or individual.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence is applicable in the following situations: a) the client is a credit or financial institution within the EU or EEA; b) the client is a listed entity in the EU or EEA; c) the client is public authority (specific conditions detailed in the law); d) the client is Slovak public authority; e) the client is a credit institution or a financial institution which operates in the territory of a third country which imposes obligations in the area of the prevention and detection of legalisation and terrorist financing equivalent to obligations laid down by the Slovak AML Act and with regard to performance of those duties they are supervised; f) to the extent of identification and verification of identification of the beneficial owner if a pooled account is managed by a notary or an advocate who operates in the EU or EEA or in a third country which imposes obligations in the area of the prevention and detection of legalisation and terrorist financing equivalent to obligations laid down by this Act and if the data on identification of the beneficial owner are available, on request, to the obliged entity that keeps this account; g) the client is a legal entity with securities negotiable on a regulated market in a EU or EEA or is a company which operates in the territory of a third country which imposes obligations in the area of the prevention and detection of legalisation and terrorist financing equivalent to obligations laid down by Slovak laws. In case of a life insurance contract to be concluded if the insurance premium payable per year does not exceed EUR1,000 or if payable in lump-sum does not exceed EUR2,500; and h) in certain situations related to pension scheme agreements, both mandatory and voluntary (no amount set by law).
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced customer due diligence is applicable for: a) a remote financial services agreement; b) a transaction and business relationship with a PEP; and c) a correspondent bank relationship with a foreign credit or similar institution ("correspondent institution").
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	All transactions with PEPs are subject to due diligence including the provision of information and supporting documentation relating to: a) the purpose and intended nature of the transactions or business relationship; b) the beneficial owner, if the client is a legal entity; c) the information required for continuous monitoring of the business relationship; and d) a review of the income source.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Prior to the creation of a correspondent banking relationship, the following is required: a) sufficient information on the relevant correspondent institution and the nature of its operations; b) publicly sourced information to establish the quality of supervision overseeing the correspondent institution; c) an evaluation of measures applied by the correspondent institution against the legitimisation of proceeds of crime and financing terrorism; d) understanding if approval of relevant lead employee to open the corresponding bank relationship was granted; and e) in the case of wire transfers, confirmation from the correspondent bank that it has identified the account holder.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In the case of a remote financial services agreement: a) the first payment under this agreement shall be made via an account kept in the customer's name held at a credit institution or a foreign credit institution operating in the EU or EEA; and/or b) the customer shall submit to the entity a copy of a document verifying the existence of this account together with copies of the relevant parts of his identity card and at least one more identification document to validate the customer's identification data of this card i.e. the type, serial number, issuing country or institution and validity.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	To the Financial Analytical Department ("FAU") of the Police, the Ministry of Interior of the Slovak Republic: http://www.minv.sk/?financna-policia

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 3,928 GDP (in current prices): 2014 – USD100,248.6m (Source: data.worldbank.org) This results in a ratio of 1 SAR for every USD25.5m of GDP.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Suspicious transactions are identified based on various criteria such as unusual transactions, cash transactions above a certain threshold, international wire transfers etc. but no special report is required.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Potential cash penalties up to EUR332,000 (depending on the seriousness of the breach) or a suspension of business license for conscious non-compliance within a 12 month period.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No, however, transaction monitoring should be performed by using adequate means which assumes the use of some automated technology.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes, in general a transaction that is identified / reported as suspicious can be continued after 48 hours from when it has to be notified to the FAU, unless the FAU requires the transaction to be postponed further and the FAU has passed the notification to criminal police (in which case an additional 24 hour delay is anticipated by law).

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No. However, if the external auditor during performance of the regular audit procedures finds out facts which indicate a suspicion of committing economic crime, crime against property or crime of corruption, he is obliged to inform the FAU, statutory representatives and control body of the given bank thereof. Internal audit/control body of the bank is the body primarily responsible for AML procedures within the bank.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes. Slovak Act No. 122/2013 Coll. ("the Data Protection Act") governs the area of personal data protection. a) yes; b) the personal data used for corporate purposes are subject to the Data Protection Act. Rules for acquiring, processing, storing, and usage (jointly "processing") of personal data must be complied with in full extent. However, for the purpose of AML, processing of personal data is generally not subject to the consent of affected persons, if their eventual submission to the FAU as a part of SAR is required directly by the law; and c) yes, the Data Protection Act stipulates a separately protected category of personal data. It is forbidden to process personal data on racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in political parties or political movements, trade union membership and data concerning health or sex life. Personal data regarding mental identity, biometric personal data, and personal data on records of criminal and administrative offences may be processed only by persons designated by relevant laws, and only for specific purposes.

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	No. However, with regard to medical data, they are not very likely to be the subject of a SAR to the FAU.

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	In general, the AML data provided by the obliged subjects are exempt from any usual restrictions imposed on these types of data. However, each transfer would need to be considered carefully and provided strictly within the extent of the AML law and other applicable legislation, so that no rights or legal entities or natural persons are breached. Generally, transfers of personal data to countries without adequate protection measures (i.e. outside the EEA and EU and Safe Harbour Regime) require approval of the Slovak Personal Data Protection Office. Each case is considered separately.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes, the general business secrecy is stipulated in the Act No. 513/1991 Coll., the Commercial Code as amended, and specific bank secrecy is stipulated in the Act No. 483/2001 Coll. on banks. Trade secrets are all facts with a commercial, production or technical nature, related to the business, which have actual or at least potential material or immaterial value, which are not available in the relevant business circles, should be classified according to the will of the entrepreneur, and the entrepreneur adequately ensures their confidentiality. Bank secrecy means keeping confidential all the information and documents on matters relating to the client of the bank that is not publicly accessible. In particular, information on transactions, account balances and deposit balances. The bank is obliged to keep this information confidential and protected from disclosure, misuse, damage, destruction, loss or theft. Information and documents on matters that are protected by bank secrecy cannot be disclosed to third parties without the prior written consent of the client. There are also other types of confidentiality prescribed by the relevant laws, such as attorney-client confidentiality, medical confidentiality, auditor confidentiality and others.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Slovenia

Key contact: Oliver Currie
Email: oliver.currie@si.pwc.com
Tel: +386 30 606 654

Postal address: PwC SVETOVANJE d.o.o.
Cesta v Kleče 15,
SI-1000 Ljubljana

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1994. This has been amended several times and was completely replaced in 2007 with the Prevention of Money Laundering and Terrorist Financing Act which took effect on 21 Jul 2007 and was last amended in 2014. See: a) (http://www.uppd.gov.si/si/zakonodaja_in_dokumenti/zppdft_in_podzakonski_akti/); b) (http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/zakonodaja/ZPPDFT_ZPPDFT-A_B_ANG.pdf); c) (http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/zakonodaja/ZPPDFT-A_ANG.pdf); and d) (http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/zakonodaja/Slovenian_AML_CFT_law_2007.pdf).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) the Bank of Slovenia (https://www.bsi.si/en/) b) Securities Market Agency of the Republic of Slovenia (http://www.a-tvp.si/Eng/Default.aspx) and Insurance Supervision Agency (https://www.a-zn.si/Eng/); c) Office of the Republic of Slovenia for Gaming Supervision (casinos) (http://www.arhiv.unpis.gov.si/en/), Tax Administration of the Republic of Slovenia (http://www.fu.gov.si/en/businesses/), Market Inspectorate of the Republic of Slovenia (http://www.ti.gov.si/en/), and the Office for Money Laundering Prevention which is a constitutive part of the Ministry of Finance (http://www.mf.gov.si/angl/), performing duties referring to the prevention and detection of money laundering and terrorist financing, and other duties determined by the Act on the Prevention of Money Laundering and Terrorist Financing (Official Gazette of the Republic of Slovenia No. 60/2007): (http://www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/zakonodaja/ZPPDFT_ang_10_09.pdf)
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, forms for forwarding data to the Office for Money Laundering Prevention of the Republic of Slovenia: http://www.uppd.gov.si/en/legislation_and_documents/working_reports/ Links to available guidelines are published on the Office for Money Laundering Prevention's website: http://www.uppd.gov.si/si/zakonodaja_in_dokumenti/smernice/

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, the law differentiates between requirements for client identification based on the risk assessment.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The MONEYVAL assessment report was published in March 2010. A second regular follow-up report was published in April 2013: http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/follow-up%20report%204round/MONEYVAL(2013)6_SLV_4Follow-upRep.pdf

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes. Transactions for which the sum does not exceed EUR15,000 (whether the transaction is carried out in a single operation or in several operations which are evidently linked) unless: a) it is establishing a business relationship with a customer; b) there are doubts about the veracity and adequacy of previously obtained customer or beneficial owner information; c) there is a suspicion of money laundering or terrorist financing in respect of a transaction or customer, regardless of the transaction amount; d) an organisation enters into an additional business relationship with the customer or carries out the transactions referred to in point 2 on the basis of the existing business relationship; e) the transaction is with a concessionaire offering games of chance in a casino or gaming hall when the transaction is effected at the cashier's desk; f) the customer's registration is for participation in a system of organising games of chance with organisers and concessionaires who offer games of chance via the Internet or other telecommunications means shall be deemed an established business relationship; or g) the customer's accession to the fund rules of a mutual fund managed by a management company. Also in the case of life insurance, customer due diligence is not required when arranging life insurance contracts where the single premium or multiple premiums to be paid in a year do not exceed EUR1,000 or where the single premium does not exceed EUR2,500. In arranging pension insurance contracts there is no need to carry out customer due diligence, provided that: a) such insurance policies contain no surrender clause and cannot be used as security for a loan; or b) the collective insurance contract is entered into within a pension or other similar scheme guaranteeing the right to pension to the employees and provided the premiums are paid through salary deductions and the scheme rules contain no surrender clause. Electronic money undertakings from Member States and branches of electronic money undertakings from third countries need not apply customer due diligence measures in the following cases: a) when issuing electronic money, provided the amount of deposit made for the issue of electronic money stored on a medium does not exceed EUR250; or b) when issuing electronic money and in transactions via e-money, provided that the maximum amount for its issue in respect of the transaction stored on a medium does not exceed EUR2,500 in a calendar year, except when an amount of EUR1,000 or more is redeemed in that same calendar year by the bearer. Organisations referred to in paragraph (1) of Article 4 of the Prevention of Money Laundering and Terrorist Financing Act may not apply customer due diligence measures also in respect of other products or related transactions when such products and related transactions represent a low risk of money laundering or terrorist financing: a) products related to the financing of physical assets and for which the right of ownership and the right to dispose of property are not transferred to the customer before the termination of a contractual relationship (e.g. leasing of physical assets, leasing with purchase option, sale with retention of title) if the amount of down payment related to such product or the total of installments paid within one year do not exceed EUR15,000; b) savings products with characteristics similar to those of an insurance policy (e.g. gradual savings), provided that: a. individual down payments or several down payments payable together in one year do not exceed EUR1,000; b. in case of saving by a single down payment the amount of such down payment does not exceed EUR2,500; and c) other products (e.g. small-value consumer loans) if the maximum amount of the product and the related transactions does not exceed EUR15,000. For further details refer to 12.4 of the Prevention of Money Laundering and Terrorist Financing Act.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals, sole proprietors and individuals who conduct business: Name, surname, address, date of birth, place of birth, tax number, type of ID, ID number and name of issuing authority for ID inspected. This information would be verified by an identity card or passport (supporting evidence would have to be included). Legal entities: name of legal entity, type of legal entity, address of registered office, identification or registration number. The same principles for “individuals” apply for the identification of individuals in the company’s statutory body. Evidence of power of representation must also be provided (e.g. excerpt from court, certification of incorporation or another similar document). Civil law entities (institutions, associations, institutes, etc.): name of entity, name of member, member’s address, date and place of birth of member, member’s tax number. Documents evidencing certified power of representation must be attached. If these are members of a legal person, then the data required for the identification of legal entities must also be provided.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	These should be certified by an appropriate person (notary, local authorities, etc.).
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The beneficial owner of a corporate entity shall be any natural person who owns through direct or indirect ownership at least 25% of the business shares, stocks or voting or other rights, on the basis of which he/she participates in the management or in the capital of the legal entity with at least 25% share or has the controlling position in the management of the legal entity’s funds; or any natural person who indirectly provides or is providing funds to a legal entity and is on such grounds given the possibility of exercising control, guiding or otherwise substantially influencing the decisions of the management or other administrative body of the legal entity concerning financing and business operations. Name of the company for which the person is a beneficial owner, personal name and permanent or temporary address.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Provided that reasons for a suspicion of money laundering or terrorist financing do not exist in connection with the customer, simplified due diligence may be applied when the customer is: - an organisation referred to in points 1, 2, 4, 5, 6, 7 and 8 of paragraph 1 of Article 4 of the Prevention of Money Laundering and Terrorist Financing Act, or the insurance company, provided the organisation has its head office in a Member State or equivalent third country referred to in paragraph 5 of Article 25 of the Prevention of Money Laundering and Terrorist Financing Act; - a state body, self-governing local community body, public agency, public fund, public institution or chamber, established in the Republic of Slovenia; - a company whose securities are admitted to trading on a regulated market in one or more Member States in accordance with European Community legislation, or a company situated in a third country whose securities are admitted to trading on a regulated market; - in a Member State or in that country, provided that its disclosure requirements are consistent with European Community legislation; or - the other person referred to in paragraph 4 of Article 6 of this Act in connection with whom there is little risk of money laundering or terrorist financing. An auditing firm or independent auditor that establishes a business relationship of mandatory auditing of annual accounts of a legal entity pursuant to the Act governing its operations may apply simplified due diligence procedures, except when reasons for suspicion of money laundering or terrorist financing exist in connection with the customer or auditing circumstances.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence measures are required when: a) entering into a correspondent banking relationship with a respondent bank or similar credit institution situated in a third country; b) entering into a business relationship or carrying out a transaction referred to in point 2 of paragraph 1 of Article 8 of the Prevention of Money Laundering and Terrorist Financing Act with a customer who is a politically exposed person referred to in Article 31 of the Prevention of Money Laundering and Terrorist Financing Act; and c) when, within customer due diligence, a customer was not physically present for the purpose of determining and verifying his identity. The organisation shall apply, by analogy, a measure or measures of enhanced customer due diligence (corresponding banking relationships with credit institutions from third countries, foreign politically exposed persons and physical presence of a customer when determining and verifying identity) where it assesses that there is a high risk of money laundering or terrorist financing due to the nature of the business relationship, form or manner of executing the transaction, business profile of the customer, or other circumstances relating to the customer.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	When the customer entering into a business relationship with or effecting a transaction, or when the customer on whose behalf a business relationship is entered into or a transaction effected, is a politically exposed person or foreign politically exposed person.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The following additional data, information and documentation must be obtained: a) date of issue and period of validity of the authorisation to perform banking services, and name and head office of the competent authority from the third country that issued the authorisation; b) description of the performance of internal procedures relating to the detection and prevention of money laundering and terrorist financing, in particular to customer due diligence procedures, procedures for determining the beneficial owners, for reporting data on suspicious transactions to competent authorities, for keeping records, internal control and other procedures adopted by the bank or other similar credit institution with respect to detecting and preventing money laundering and terrorist financing; c) description of systemic arrangements in the field of detection and prevention of money laundering and terrorist financing applicable in the third country where the bank or other similar credit institution is established or registered; d) a written statement that the bank or other similar credit institution does not operate as a shell bank; e) a written statement that the bank or other similar credit institution has not established or does not enter into business relationships with shell banks; f) a written statement that the bank or similar credit institution is subject to administrative supervision in the country of its head office or registration and is, in accordance with the legislation of the country concerned, under the obligation to comply with laws and regulations governing the detection and prevention of money laundering and terrorist financing; and/or g) an employee of the organisation establishing the correspondent relationship and conducting the enhanced customer due diligence procedure shall obtain the written approval of his/her superior and the responsible person in the organisation prior to entering into such relationship. The organisation shall obtain the data referred to above by inspecting public or other accessible data records, or by inspecting documents and business records submitted by the bank or another similar credit institution situated in the third country.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In any case when a customer is not physically present in the organisation or in presence of the third person referred to in Article 25 of the Prevention of Money Laundering and Terrorist Financing Act when determining and verifying identity.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	To the Office for Money Laundering Prevention ("OMLP"): (http://www.uppd.gov.si/en/legislation_and_documents/working_reports/)

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 – 616 SARs. GDP (in current prices): 2013 – USD49.5m (Source: data.worldbank.org). This results in a ratio of 1 new SAR for every USD80.3m of GDP.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes. The law prescribes penalties up to EUR120,000 depending on the seriousness of the violation.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes. The Office may issue a written order temporarily suspending a transaction for a maximum of 72 hours if the Office considers that there are reasonable grounds to suspect money laundering or terrorist financing, and it shall inform the competent authorities thereof.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of “personal data” cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of “sensitive data”? How is it defined and what are the additional protections?
A29.	a) yes; b) client consent must be obtained; and c) yes. Sensitive personal data are data on racial, national or ethnic origin, political, religious or philosophical beliefs, trade-union membership, health status, sexual life, the entry in or removal from criminal record or records of minor offences that are kept on the basis of a statute that regulates minor offences (hereinafter: minor offence records); biometric characteristics are also sensitive personal data if their use makes it possible to identify an individual in connection with any of the aforementioned circumstances. There are special rules governing the processing of sensitive personal data and precautions to secure that only authorised persons have access to this data.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	There are restrictions for transferring data out of Slovenia to countries that do not ensure an adequate level of protection of personal data.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Personal Data Protection Act of Slovenia.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Article 214 of the Slovenian Banking Act (ZBan-1) indicates that banks shall treat as confidential and protect all information, facts and circumstances about individual clients notwithstanding the manner in which this information has been obtained. Article 215 of the same law continues to outline the obligation to protect confidential information and indicates that members of the bank's governing bodies, shareholders, employees or other persons who have access to the confidential information from article 214 of this Act in connection with their work at the bank or provision of services for the bank, may not disclose this information to third parties or use them by themselves or enable third parties to use them. The obligation to protect confidential information shall not apply in the following cases: a) if the client expressly agrees in writing with the disclosure of some confidential information; b) if this information is required by the Bank of Slovenia or another competent authority for the purposes of supervision carried out within its competencies; c) in cases of disclosure of information to parent undertakings in connection with supervision on a consolidated basis subject to the provisions of sub-section 7.9.3 of this Act or ZFK (Financial Conglomerates Act); d) exchange of information on credit rating of clients among banks or within a banking group for the purpose of credit risk management; and e) other measures stipulated by the law.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Spain

Key contacts: Javier Lopez Andreo / Francisco Javier Caro
Email: javier.lopez.andreo@es.pwc.com /
francisco.javier.caro@es.pwc.com
Tel: +34 915 684 352 / +34 915 685 130

Postal address: Torre PwC, Paseo de la Castellana,
259 B – 28046,
Madrid

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2010: Law 10/2010 2014: Royal Decree of Law 10/2010
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	Law 19/1993 regarding AML (in force until 30 Mar 2010).
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The Executive Service of the Commission for Monitoring Exchange Control Offences ("SEPBLAC"): www.sepblac.com
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	SEPBLAC Reports and Publications: http://www.sepblac.es/espanol/informes_y_publicaciones/otra_documentacion.htm
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Until the issuing of the new Royal Decree for Law 10/2010, the following guidance under the previous regime are still applicable: http://www.sepblac.es/espanol/legislacion/norma-blanqueo.htm
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, SEPBLAC has been leading work to embed a risk based approach into AML controls, both in terms of firms' legal obligations and their practical implementation. Law 10/2010 reinforces this approach by increasing the range of industries and activities affected by the updated regulation.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Last Mutual Report FATF/GAFI (2014): http://www.sepblac.es/espanol/informes_y_publicaciones/informe_eval_mutua_esp2014.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, one-off transactions (single or linked) under EUR1,000.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: firms should obtain a national identity document, permission of impeachment sent by the Ministry of Justice, passport or government issued document which includes the customer's full name and photograph. Additionally, firms must verify identification documents of all authorised persons of the account. Corporates: firms should obtain the following: full name, regulation form and number, business address and professional activity. Additionally, names and regulation documents of all Attorneys should be obtained.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Copies should be certified by an appropriate person, for example an employee of the commercial office.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The law determines that firms may consider it appropriate to verify the identity of appropriate beneficial owners. Where a principal owner is another corporate entity or trust, the firm should take measures to look behind that company or trust and establish the identities of its beneficial owners or trustees. The firm will then judge which of the beneficial owners exercise effective control, and whose identities should therefore be verified.

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence could be applied to some concrete clients and products. Detailed requirements for this are detailed in Law 10/2010, Section 2, Articles 9 and 10.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	The law determines that firms will require additional measures of identification for certain business transactions, including private banking, correspondent banking, online and telephone banking and currency exchanges. Enhanced due diligence must be applied for particular clients and products. Detailed requirements for these activities are detailed in Law 10/2010, Section 3, Article 11: in general terms, and Article 16: for products and transactions where anonymous activity is possible.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	Law 10/2010, Articles 14 and 15 detail the due diligence and monitoring requirements for PEPs.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Firms should take into account the greater potential for money laundering in a correspondent business relationship. Firms must send an AML questionnaire to their correspondent banks to verify that these banks have measures to control money laundering. Law 10/2010 Article 13 details the requirements for correspondent banking relationships.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Law 10/2010 Article 13 details the requirements for correspondent banking relationships. In particular, point 2 states that “financial entities do not set up relations or correspondent with shell banks”.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Firms should take account of the greater potential for money laundering in non face-to-face situations. Where a customer approaches a firm remotely (by post, telephone or over the internet), the firm should carry out non face-to-face verification, either electronically, or by reference to identification documents. Requirements for non face-to-face transactions and/or relationships are detailed in Law 10/2010, Article 12.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The SEPBLAC: www.sepblac.com

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 – 3,919 SARs GDP (in current prices): 2013 – USD1,369,261m (Source: data.worldbank.org) This results in a ratio of 1 SAR for every USD350m.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	There are two different types of reporting in Spain: Systematic Reporting and Suspicious Transaction Report.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Article 17 of Law 10/2010 states that, the subject will review transactions or operations regardless of the amount.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Penalties for non compliance with Law 10/2010 requirements are detailed on Chapter VIII, Articles 50, 51, 52, 53, 54 and 55, and Sanctions are detailed from article 56, 57 and 58.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Spanish Law 10/2010 has widened the scope of industries and activities to be monitored. All entities which have a large number of daily transactions are requested to use automated Suspicious Transaction monitoring technology. Article 17 of Law 10/2010 stated that accurate automated systems must be set up but adapted to the specific industry and Money Laundering risk. For these reasons, it was mandatory for industries such as finance, insurance and online gambling to have automated systems.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Law 10/2010 Article 19 details the requirement for injunctive enforcement.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Law 10/2010 Article 31 states the requirements for monitoring activity in branches and subsidiaries registered in other countries.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes, all banks have to be reviewed by an external auditor each year.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) every year: first year: complete review; next two years: following recommendation; b) to the Board of Directors; and c) no.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	All of the above are requirements.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes. All the files used by the Entity to manage the AML obligations have to be reported to the Data protection authorities.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Only for medical data. In this case is forbidden to transfer data without client approve.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Law 15/1999; Law 2/2011; Law 10/2010; RD 1720/2007; RD 3/2010.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Sweden

Key contact: Ulf Sandlund
Email: ulf.sandlund@se.pwc.com
Tel: +46 (0) 709 293 607

Postal address: Torsgatan 21, SE-113 21
Stockholm,
Sweden

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	In 2009, the 2009:62 Money Laundering and Terrorist Financing (Prevention) Act became effective. This law is based on the Third Anti-Money Laundering Directive. The legislation has been upgraded with extended criminal provisions and a penalty catalogue (see further information below). The law is called the Act on penalties for money laundering offences (2014:307) and became effective 01 Jul 2014. In addition, legislation updates based on FATF 40 revised standards from 2012 have been implemented in the Money Laundering and Terrorist Financing (Prevention) Act and became effective 01 Aug 2015. Furthermore updates of the Swedish FSA's regulatory code will be implemented on 01 Dec 2015.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The legislation upgrade of 01 Jul 2014 regards a wider scope of punishable acts, broader conspiracy provisions and extended asset freeze provisions. As regards to the upgrades of the Money Laundering and Terrorist Financing (Prevention) Act of 01 Aug 2015 (see above), the updates concern the extension of the PEP definition to domestic PEPs and international organization PEPs, requirements to establish routines for performing AML-risk assessments and a new chapter on data protection in the Money Laundering and Terrorist Financing (Prevention) Act. Furthermore, rules for more effective supervision by the county administration were implemented as well as extended record keeping periods, enhanced access to CDD-information from which third parties relied upon and rules on the risks associated with new products, business practices and technologies.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	For general information in English (http://www.fi.se/Folder-EN/Startpage/Regulations/Money-laundering-/): a) the Swedish Financial Supervisory Authority (Finansinspektionen) (http://www.fi.se/Regler/Penningtvatt/); b) the Swedish Financial Supervisory Authority only governs companies within the financial sector; and c) for other sectors, different regulators are in charge: a. casinos and lotteries: the Gaming Board for Sweden (Lotteriinspektionen) (www.lotteriinspektionen.se/en/); b. realtors: the Swedish Board of Supervision of Estate Agents (Fastighetsmäklarnämnden) (http://fastighetmaklarnamnden.se/); and c. other: the County Administrative Boards of Stockholm (http://www.lansstyrelsen.se/stockholm/En/Pages/default.aspx), Västra Götaland (http://www.lansstyrelsen.se/vastragotaland/En/Pages/default.aspx) and Skåne (http://www.lansstyrelsen.se/skane/En/Pages/default.aspx) (http://www.bolagsverket.se/om/oss/fler/penningtvatt).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes: a) by the Swedish Bankers' Association (http://www.penningtvatt.se/); and b) by the financial regulator (http://www.fi.se/Regler/Penningtvatt/).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	IMF Financial Sector Stability Assessment in 2011 (http://www.imf.org/external/pubs/ft/scr/2011/cr11172.pdf) and (http://www.fatf-gafi.org/media/fatf/documents/reports/mer/FoR%20Sweden.pdf). It can also be noted that Sweden is scheduled to be assessed by FATF in May/June 2016 (on site visit).

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes: a) when establishing a customer relationship; b) single transactions at EUR15,000 or more; c) serial transactions together totaling EUR15,000 or more; or d) any transaction, independent of value, if there is suspicion about terrorist financing.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Reliable and independent information sources must be used and controls signed off and documented independently whether the customer is a legal or physical entity. For example, evidence of identity can be in document or electronic form. The following information is required: Individuals: approved identification documents with name and social security number. Remote customers can be identified with an approved electronic identity card to verify name, social security number and address. Foreigners must be identified through a passport and a copy must be kept. Legal entities: official registration documents and the identity of representatives through approved identification documents.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Third parties can be used or the financial institution can choose to perform these controls in-house. However, the financial institution always has responsibility for identification procedures and ensuring compliance with laws and regulations.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Beneficial owners who control more than 25% of shares in a company or have significant influence over a company should be identified directly through an identification check, through official databases or through other documents received that can verify the identity of the beneficial owners.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	a) Swedish public authorities; b) firms within the European Union ("EU") / European Economic Area ("EEA") and specified countries that have similar AML/CFT legislation that conduct business as: a. banks (as defined by Swedish law); b. life insurance companies; c. securities firms (as defined by Swedish law); d. certain other financial firms that are registered with the Swedish Financial Services Agency ("FSA") (as defined by Swedish law); e. insurance brokers (as defined by Swedish law); f. firms that issue electronic money (as defined by Swedish law); g. mutual funds (as defined by Swedish law); and h. registered payment service providers and payment institutions (as defined by Swedish law); c) firms whose shares are listed on an exchange within the EU/EEA as defined by 2004/39/EU or listed on an exchange outside the EU/EEA where the requirements correspond to 2004/39/EU; d) life insurance products with an annual premium of maximum EUR 1,000 or a one off premium of maximum EUR2,500; e) certain occupational pensions; f) electronic money with certain thresholds as defined by Swedish law not exceeding EUR 250; and g) certain pooled accounts in the EU/EEA or in territories outside the EU/EEA provided that certain requirements are met.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	a) when a business relationship is established or an individual transaction is carried out with another at a distance; b) when establishing a business relationship or if executing a single transaction with a PEP; c) correspondent banking relationships with credit institutions outside the EU/EEA; and d) when the risk of money laundering or financing of terrorism is deemed to be high.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	a) at the establishment of a business relationship; and b) for single transactions.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Gather sufficient information about the bank in order to assess the reputation of the bank and the quality of supervision, assess the bank's AML/CFT controls, document the controls of each institution, obtain internal approval to establish a correspondent banking relationship and verify that the bank undertakes KYC procedures of its customers and can provide relevant information.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	When a business relationship is established or an individual transaction is carried out with another at a distance, such as opening bank accounts online.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Financial Intelligence Unit (Finanspolisen): http://www.imolin.org/imolin/amlid/data/swe/url/financial_intelligence_unit_of_sweden_-_finanspolisen_rikskriminalpolisen_fipo_.html

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 9,183 SARs (Financial Intelligence Unit - Finanspolisen) GDP (in current prices): 2014 – USD571.1b (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD 62.1m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Yes, non-compliance such as negligence / failure to report and a delay in reporting a suspicious transaction can result in significant penalties, director disqualification and/or loss of operating permit.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No. Financial institutions are however required to act instantly without delay.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No. In certain situations, the Police Authority can issue a temporary order to block transactions and funds from being executed or removed.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	The legislation does not prevent nor prohibit transaction monitoring outside the jurisdiction.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No, but if there is a lack of control the auditor is obliged to report to the board of directors.
Q27.	If an external report on the bank's AML systems and controls is required: - how frequently must the report be provided? - to whom should the report be submitted? - is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: - sample testing of KYC files? - sample testing of SAR reports? - examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: - does the definition of "personal data" cover material likely to be held for KYC purposes? - how do the laws apply to corporate data? - does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	- yes; - the Swedish Personal Data Act only covers information relating to individuals; and - yes, there are general restrictions in Sweden, but exemptions exist for institutions that are required to report suspicious transactions. These institutions can process the personal data of individuals provided they do not process data other than name, social security/organisation number, address and supporting data/documents constituting reason for suspicion. Restrictions also exist for how and when registers need to be cleansed. The upgrade of the Swedish Act on Combatting money laundering and terrorism on 01 Aug 2015 has introduced possibilities to process sensitive data when identifying PEPs and for the record keeping of such data or data related to the monitoring of PEPs.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes, criminal records and medical data are considered as sensitive information. Information typically contained in a credit report is possible to process according to the Swedish Act on Combatting money laundering and terrorism (SFS 2009:62).

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. Information about the relationship with a credit institute may not be revealed.



'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Switzerland

Key contact: Emmanuel Genequand
Email: emmanuel.genequand@ch.pwc.com
Tel: +41 58 792 95 75

Postal address: Avenue Giuseppe-Motta 50,
CH-1211 Geneva,
Switzerland

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	1977 (amended at various stages between 1982 and 2016).
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	Revised provisions of the Swiss Criminal Code, AML Act and AML Ordinance entered into force on 01 Jan 2016. Material changes are: a) qualified tax offences become predicate offences to money laundering (transactions in excess of CHF300 (approx. USD300) or equivalent per tax year by way of using forged documents); b) extension of the definition of PEP to national PEPs and PEPs related to inter-governmental organisations and international sportive federations; c) new concept of Beneficial Owner (can only be individuals) and requirement to identify controlling persons of operative legal entities (ultimate owners of >25% of votes or capital); and d) new procedure regarding communication to the Money Laundering Reporting Office Switzerland ("MROS") Financial Intelligence Unit ("FIU").
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) Swiss Financial Market Supervisory Authority ("FINMA") (http://www.finma.ch/e/pages/default.aspx); b) FINMA (http://www.finma.ch/e/pages/default.aspx) or various self-regulatory organisations ("SROs"), see a member list on (http://www.finma.ch/e/beaufsichtigte/sro/Pages/default.aspx); and c) please refer to b) above.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	For Banks, the Swiss Banking Association provides an Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB 16) including a commentary (http://www.swissbanking.ch/en/home/publikationen-link/shop.htm).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No, customer identification is not required. However, the financial intermediary must identify beneficial owners retrospectively.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	The AML Act provides for a risk based approach; auditing is also governed by a risk based approach according to "Circular 2013/3 - Auditing" from FINMA.

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The most recent report was undertaken in 2005 (http://www.fatf-gafi.org/countries/s-t/switzerland/documents/mutualevaluationofswitzerland.html), with follow up reports undertaken in 2009 (http://www.fatf-gafi.org/countries/s-t/switzerland/documents/follow-upreporttothemutualevaluationofswitzerland.html), and 2012 (http://www.fatf-gafi.org/countries/s-t/switzerland/documents/firstbiennialupdatetothewissmutualevaluationreport.html). The next FATF Mutual Evaluation will be in 2016.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, due diligence obligations can be waived if the business relationship only involves assets of a low value and there is no suspicion of money laundering or terrorist financing. The relevant thresholds are: - for electronic payments for services and goods, CHF1,000 (approx. USD995) per transaction and CHF5,000 (approx. USD4,970) per calendar year and per client; - for bilateral credit cards (including department store cards), CHF5,000 (approx. USD4,970) per month and CHF25,000 (approx. USD24,800) per year and per client; and - in the case of financial leasing, CHF5,000 (approx. USD4,970) per calendar year and per client.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: For face-to-face contact, the bank verifies identity via an official identification document with a photograph (passport, identity card, driving licence, etc.) and puts on record the individual's full name, date of birth, address and nationality. For non-face-to-face contact, the bank obtains a certified copy of an official identification document, as well as a confirmation of the domicile indicated, either through an exchange of correspondence or by any other appropriate method. Corporates: With a registered office in Switzerland the bank ascertains whether the firm's name is published in the official Swiss Commerce Gazette or listed on a public website for commercial register entries. Private directories / databases can also be used. Otherwise, identity must be established with an extract from the Commercial Register. Identity is verified with an extract from the Commercial Register or extracts from public websites for Commercial Register entries, or equivalent documents substantiating the existence of the legal entity or company (such as a Certificate of Incorporation). In addition, the identity of the individuals establishing the business relationship must also be checked and the bank must take note of and document the contracting partners' power of attorney arrangements. Further, the financial intermediary must acknowledge the provisions regulating the power to bind the legal entity, and verify the identity of the persons who enter into the business relationship on behalf of the legal entity.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Independent authentication of copies of official identification documents may be provided by branches, representative offices and subsidiaries of the bank, correspondent banks, other financial intermediaries recognised by the account opening bank as well as notaries, Swiss lawyers and public authorities who customarily issue such confirmations of authenticity. Additionally, authenticated copies are issued by Post Offices and SBB (Swiss Railway) stations.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	All due diligence which can reasonably be expected under the circumstances must be exercised in establishing the identity of the beneficial owner. If there is any doubt as to whether the contracting partner is himself the beneficial owner, the bank shall require by means of Form A, a written declaration setting forth the identity of the beneficial owner. Where the bank has no doubt regarding the fact that the contracting party and the beneficial owner are identical and thus does not require a Form A, it must document the rationale of its conclusion.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	It is not necessary to formally verify the identity of a contracting partner when: a) an account, securities account or passbook is opened in the name of a minor by an adult third party, provided that the assets deposited at the outset do not exceed CHF25,000 (approx. USD24,800); however, the identity of the adult opening the account must be verified; b) cash transactions and execution of transactions involving securities, currencies, precious metals or other commodities not exceeding CHF25,000 (approx. USD24,800); c) a rental surety account is opened for a rented property located in Switzerland; or d) the legal entity is listed on a stock exchange.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	In the case of higher risk, Swiss law requires financial intermediaries to define higher risk criteria and provides guidance and examples (domicile of the contracting party and beneficial owner, type of business, origin country of payment, volume of incoming funds, the complexity of the structures, notably in case of use of domicile companies and the absence of personal contact with the beneficial owner). PEPs and correspondent banking institutions are deemed higher risk relationships.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Business relationships with PEPs are regarded as higher risk and local regulations/guidance requires that enquiries should be made to ascertain whether the contracting partner/beneficial owner is a PEP. For national PEPs as well as PEPs related to inter-governmental organisations or international sporting federations, financial intermediaries may require another risk criteria to be met for the PEP to be considered as a higher risk relationship. The means of investigation for such higher risk business includes obtaining information in written or oral form from the contracting partner or beneficial owner, visits to the places of business of the contracting partner and beneficial owner, consultation of publicly accessible sources and databases, and information from trustworthy individuals where necessary.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	For cross-border banking relationships with foreign banks, the following due diligence procedures are to be performed in addition to the standard clarifications for high risk relationships: ensuring that the foreign bank is prohibited from entering into business relationships with shell banks, clarifying the AML and CFT controls implemented by the foreign bank and examining whether the foreign bank is subject to an equivalent regulation and supervision in the anti-money laundering and counter financing of terrorism domain. Furthermore, a risk-based procedure has to be established concerning the processing of repeated wire transfer instructions which lack the required sender information.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	For business relationships entered into through correspondence or via the internet, banks must verify the identity of the contracting partner by obtaining a certified copy of an official identification document as well as a confirmation of the domicile indicated, either through correspondence exchange or by any other appropriate method. Identification based on an official identification document at delivery or receipt of mail is also deemed as sufficient proof of identity, provided that personal delivery to the recipient is thus warranted. In addition, beneficial ownership according to Form A must invariably be provided by individuals entering into a business relationship with a bank through correspondence. For business relationships established by electronic means, the bank shall identify, mitigate and control the risk associated with the use of new technologies. The lack of personal contact with the contracting party and the beneficial owner is considered higher risk, according to the domain of activity of the bank.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Money Laundering Reporting Office ("MROS") (https://www.fedpol.admin.ch/fedpol/en/home/kriminalitaet/geldwaescherei.html).

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 1,753 SARs (Source: MROS) GDP (in current prices): 2014 – USD701,037m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD399.9m of GDP.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Anyone who fails to comply with the duty to report shall be liable to a fine of up to CHF500,000 (approx. USD497,000), or in the case of negligence, up to CHF150,000 (approx. USD149,200).

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	The AML Ordinance requires banks, fund managers, investment companies and its asset managers and security dealers to operate an IT-based system for transaction monitoring.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	With the exception of filing regarding terrorism financing lists, where freezing of assets by the financial intermediary is required upon filing, transactions can be processed pending the decision to freeze (or not to freeze) by the competent authority. In such cases, the financial intermediary is required to process the transaction in a way that maintains the paper trail.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Transaction monitoring may be outsourced to persons outside Switzerland, provided that the respective information is still available in Switzerland and provided that the results are subject to a plausibility check in Switzerland. However, the Swiss financial intermediary remains responsible. Furthermore, the client needs to be informed in case of a transfer of client information outside Switzerland.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	Yes, according to FINMA’s standard audit strategy on a yearly basis.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) annually. b) FINMA; and c) no, it is part of the regulatory audit.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) yes; b) yes; and c) yes.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	a) yes, the definition of art. 3 lit. a DPA includes all data that refers to a specific person or can be used to identify a person; b) yes, according to art. 2 para 1 DPA the law is also applicable to corporate data; and c) yes, the law differentiates between "personal data", "sensitive personal data" and "personality profile". The primary laws and regulations governing data protection in Switzerland are the Swiss Federal Data Protection Act ("DPA"), the Swiss Federal Data Protection Ordinance ("DPO"), the Swiss Federal Ordinance on Data Protection Certification ("DPCO") and Guidelines of the Federal Data Protection and Information Commissioner on the minimum requirements for a data protection management system (DPMS-Guidelines). The latest revisions of the DPA and the DPO as well as the DPCO came into force on 01 Jan 2008. The DPMS-Guidelines came into force on 01 Sept 2008 and were revised in 2014. Sensitive personal data is defined as "data on religious, ideological, political or trade union-related views or activities; health, the intimate sphere or the racial origin; social security measures, and; administrative or criminal proceedings and sanctions". Personality profile is defined as a collection of data that permits an assessment of essential characteristics of the personality of a natural person. The additional protections of sensitive personal data and personality profiles include additional requirements regarding consent of the data subject, requirements of declaration of the existence of data files, prohibition of disclosure without justification and duty to inform the data subject of the data collection. Furthermore, the disclosure is subject to fines.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Criminal records and medical data are considered sensitive personal data. The transfer of such information is only possible with justification (consent of the data subject, overriding public or private interest or law). Credit reports, depending on their content, might also be part of sensitive personal data or even personality profiles.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No, see A32 below. Furthermore, the Swiss Law has taken over large parts of the European Union ("EU") data protection law. Therefore, interpretation within the EU is interesting for the Swiss interpretation as well.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes, Switzerland has bank secrecy laws (art. 47 Banking Act). All secrets that a representative of a bank (a person active for the bank including Board of Directors, Management Board, employees, auditors, liquidators) learns in his/her function.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Turkey

Key contact: Bekir Özdemir /
Emre Haykir

Email: bekir.ozdemir@tr.pwc.com / emre.haykir@tr.pwc.com

Tel: +90 212 376 5946 / +90 212 326 6813

Postal address: BJK Plaza, Süleyman Seba Caddesi No:48 B
Blok Kat 9 Akaretler
Beşiktaş 34357 İstanbul, Turkey

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Law on Preventing Money Laundering (Law No: 4208), enacted on 19 Nov 1996, is the primary AML law in Turkey. The AML legal framework established by this law has been updated and strengthened by the passing of the Prevention of Laundering the Proceeds of Crime (Law No: 5549) on 18 Oct 2006 and by subsequent amendments on 1 Apr 2008, 07 Jul 2011, 26 Sep 2011, 11 Oct 2011 and 18 Jun 2014. In addition, the government of Turkey enacted on 7 Feb 2013 and amended on 18 Jun 2014 the Law on the Prevention of the Financing of Terrorism (Law No: 6415) which further defines terrorist financing offenses and provides new powers to the authorities to take action against suspected terrorist financing. Overarching these laws are the provisions of the Turkish Criminal Code (Law No. 5237, 12 Oct 2004) and its subsequent amendments (Law No. 5377, 8 Jul 2005) and the Criminal Procedure Law (Law No. 5271, 12 Dec 2004) which also contains provisions in relation to the prosecution of financial crime. AML regulations have also been issued to supplement the provisions of these laws. The key regulations are: a) Regulation on the Measures regarding Prevention of Laundering the Proceeds of Crime and Financing of Terrorism, published in the Official Gazette No. 26751 of 9 Jan 2008, amended on 26 Jun 2010 and 10 Jun 2014; b) Regulation on the Examination of Money Laundering Offence, published in the Official Gazette No. 26603 of 4 Aug 2007, amended on 5 Feb 2010 and 10 Jun 2014; and c) Program of Compliance with Obligations of Anti-Money Laundering and Combating Financing of Terrorism, published in the Official Gazette No. 26999 of 16 Sep 2008, amended on 2 Jan 2010 and 11 Jun 2014. Mali Suclari Arastirma Kurulu ("MASAK"), the Turkish Financial Crimes Investigation Board has provided guidance on specific AML issues through the publishing of several Communiqués. These have included, amongst other things, guidance on suspicious transaction reporting and customer due diligence.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	While the previous AML requirement remains in force, the passing of the Prevention of the Financing of Terrorism law (Law No.6415) on 7 Feb 2013 adds an additional facet to the existing regime by establishing new definitions of terrorist financing and creating new asset freezing powers for the regulatory authorities.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non-financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The central authority for suspicious transaction reporting in Turkey is the Mali Suclari Arastirma Kurulu ("MASAK"), the Turkish Financial Crimes Investigation Board, which is a service unit instituted within the Ministry of Finance (http://www.masak.gov.tr/en/default.aspx). Other regulators for the AML controls for (a) Banking; (b) Other financial Services; (c) Non- financial sector are: a) Bankacilik Düzenleme ve Denetleme Kurumu ("BDDK") / The Banking Regulation and Supervision Agency ("BRSA") (http://www.bddk.org.tr/websitesi/English.aspx); b) Sermaye Piyasasi Kurulu ("SPK") / The Capital Markets Board ("CMB") (http://www.cmb.gov.tr/index.aspx), and c) The Undersecretariat of Treasury (http://www.treasury.gov.tr/) including the Ministry of Customs and Trade (Turkish: Gümrük ve Ticaret Bakanlığı) ("TMCT"), a government ministry office of the Republic of Turkey, responsible for the non-financial sector, with respect to control of the cash flow in the customs. TMCT has issued a Circular (2015/1) within the framework of Decree No. 32 on The Protection of the Value of Turkish Currency to govern the cash flow principles at the Turkish Customs (http://hukuk.gtb.gov.tr/data/5440c4d7f293704d6c39e7c5/GumNakKont.pdf).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes. As listed above, a series of regulation documents and guidance communiqués have been issued by MASAK to supplement the legal code: http://www.masak.gov.tr/en/content/l-p-c-national-legislation/159
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Article 19 of the "Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism" provides that "The obliged parties shall be required to follow up permanently the transactions conducted by their customers whether they are in compliance with the information regarding the customer's profession, commercial activities, business history, financial status, risk profile and sources of funds within the scope of permanent business relationships and keep up-to-date information, documents and records regarding the customer. Furthermore, the accuracy of information regarding the telephone and fax number and e-mail address of customers received for customer identification shall be verified, if necessary, within the scope of risk-based approach using these means by contacting the relevant person. Financial institutions shall also take the necessary measures in order to follow up the transactions conducted out of permanent business relationship in the risk-based approach. Financial institutions shall establish, with this purpose, appropriate risk-management systems." Separately, the Ministry of Finance has the authority to determine obliged parties and specify the implementation of principles and procedures, including measures to assign an officer with necessary authority at an administrative level for ensuring compliance with this Law and to establish training, internal control and risk management systems regarding the size of business and business volumes.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The latest FATF Mutual Evaluation Report is dated Oct 2014: http://www.fatf-gafi.org/countries/s-t/turkey/documents/mutualevaluationofturkey.html The latest IMF Financial System Stability Assessment is dated Sep 2012: https://www.imf.org/external/pubs/ft/scr/2012/cr12261.pdf

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes. Obligated parties shall identify their customers or those who act on behalf or for the benefit of their customers by receiving their identification information and verifying it: a) regardless of the monetary amount when establishing permanent business relationships. Customer identification shall be completed before the business relationship is established or the transaction is conducted. When establishing permanent business relationship, information on the purpose and intended nature of the business relationship shall be obtained; b) when the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than TRY 20,000 (approx. USD6,630); c) when the amount of a single transaction or the total amount of multiple linked transactions is equal to or more than TRY 2,000 (approx. USD660) in wire transfers; d) regardless of the monetary amount in cases requiring Suspicious Activity Report; and e) regardless of the monetary amounts in cases where there is suspicion about the adequacy and the accuracy of previously acquired identification information.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Turkish national real persons: National identification card, driving licence or passport. In the case of a continuous transaction relationship: any utility bill (water, electricity, gas etc.) issued within the last three months of the date of transaction for address verification. Foreign national real persons: Passport, residence permit or other identification cards determined to be valid by the Ministry of Finance. Address verification is the same as stated above. Legal persons registered under Chambers of Commerce: Trade gazettes, national identification card, driving licence or passport for Turkish national real persons and passport, residence permit or other identification cards determined by the Ministry of Finance for foreign national real persons authorised to represent the company, signature circulars, list of authorised company representatives and their signature circulars. The verification of the updated information is done through the Chamber of Commerce Databases and telephone, fax and email verification through using the same channels. Other detailed regulations exist for associations and foundations, unions and confederations, political parties, non-resident legal persons, unincorporated organisations, public institutions, and those acting on behalf of others. See: http://www.masak.gov.tr/userfiles/file/ROM_amended_10_June_2014.pdf
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Submitted national identification cards, passports, driving licences and residency permits should be originals or copies stamped by the public notary. Trade Gazettes and signature circulars should be stamped by the Chambers of Commerce and public notaries, respectively. Customer identification of non-resident legal persons should be carried out using copies of the types of documents which have been approved by the Turkey government and which correspond to the documents required for legal persons in Turkey. Alternatively, copies of documents attached, notarized by an authority of a country which is a party to the "Convention on Abolishing the Requirement of Legislation for Foreign Public Documents" may be used. Also, in the framework of a risk-based approach, when necessary, identity information should be verified through notarized Turkish translations of copies of the documents.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	On behalf of real persons: National identification card, driving licence or passport of the person performing the transaction and the beneficiary and proxy document stamped by the public notary. Legal persons: Trade gazettes, signature circulars, list of authorised company representatives and their signature circulars of the beneficiary, national identification card, driving licence or passport of the person performing the transaction. If the person performing the transaction is not listed as an authorised company representative of the beneficiary, then a proxy document stamped by the public notary is required. The definition of beneficial owner was amended in Jun 2014. The amendment requires legal persons to take necessary measures to identify the beneficial owner of entities by checking the shareholding structure and company from the relevant trade registry. If there is any doubt about the identification of the beneficial owner, then the real persons who exercise control over the management of a legal entity are deemed to be the beneficial owner. Under the regulation, when establishing a permanent business relationship with legal persons registered within the trade registry, obliged parties should identify the natural person partners holding more than 25% of the legal person's shares as the beneficial owner. In cases where there is a suspicion that the natural person partner holding more than 25% of the legal person's shares is not the beneficial owner, or where there is no natural person holding a share at this rate, necessary measures should be taken in order to detect the natural person(s) who is/are ultimately controlling the legal person. Any natural person(s) detected shall be considered as beneficial owner. In cases where the beneficial owner is still not detected, the natural person(s) holding the position of senior managing official, whose authorisation to represent the legal person is/are registered to trade registry, shall be considered as beneficial owner.
Q12.	In what circumstances are reduced/ simplified due diligence arrangements available?
A12.	Simplified measures in terms of customer due diligence may be applied in the following situations: a) transactions carried out between financial institutions on behalf of themselves (in the event that the financial institution is located abroad, it must be in a country which is subject to regulations and supervision in accordance with international standards in combating money laundering and terrorist financing for simplified measures to be permitted); b) transactions in which the customers of the obliged parties excluding financial institutions are banks; c) in transactions where the customer is a public administration or quasi-public professional organisation in the scope of general administration in accordance with the Public Financial Management and Control Law No. 5018; d) in transactions where the customer is an International Organisation or an Embassy or a Consulate Located in Turkey. Obligated parties shall register the information specified in Article 6 of the Regulation about the natural persons who carry out the transaction on behalf of these organisations and shall verify their authorisation status through a document reflecting the authorisation; e) in establishing a business relationship relating to salary payments when accepting a batch of customers; f) in transactions related to pension schemes and Life Insurance Contracts that provide retirement benefits to employees by way of deduction from their salaries and of pension agreements; g) in transactions where the customer is a public company and its shares are listed on the stock exchange; h) transactions relating to prepaid cards where defined thresholds are not met; and i) obliged parties conducting transactions particularly in electronic environments. Simplified measures are amended: a) to decrease the frequency of monitoring customer profile (periodic reviews) in the framework of permanent business relationship; and b) to keep information, documents and records regarding the customer given in the articles 5 to 14, 17/A and 19 of the Regulation up-to-date.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	For complex and unusually high volume transactions, enhanced customer due diligence measures is required. There is a recommendation by MASAK stating that banks should utilise enhanced due diligence procedures for high-risk transactions. The risk is determined on the basis of various factors such as the background of the customer, country of residence, related bank accounts and commercial activities. Additional enhanced measures are included in relation to groups with high risk to be assessed in line with risk based approach.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	There is no additional requirement in relation to Politically Exposed Persons under MASAK regulations.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Financial institutions shall take necessary measures in foreign correspondent relationships in order to: a) obtain, by making use of publicly available resources, reliable information on whether the respondent financial institution has been subject to a money laundering and terrorist financing investigation and been punished as well as information on its business field, reputation and the adequacy of inspection on it; b) assess anti-money laundering and terrorist financing system of the respondent financial institution and to ascertain that the system is appropriate and effective; c) obtain approval from a senior manager before establishing new correspondent relationships; d) clearly determine their and the respondent financial institution's responsibilities by a contract in a way that meets the obligations in Chapter 3 of Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing Terrorism; and e) in cases where the correspondent relationship includes the use of payables - through accounts, be satisfied that the correspondent financial institution has taken adequate measures pursuant to principles in the Chapter 3 of the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing Terrorism and will be able to provide the identification information of the relevant customers when requested.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes. Financial institutions are prohibited to have respondent institution relationships with shell banks or with banks which are not confirmed not to be shell banks.

Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	Financial institutions are required to take appropriate and effective measures including paying special attention to operations such as depositing, withdrawing and wire transfers which are carried out by using systems enabling the institutions to conduct non face-to-face transactions, closely monitoring the transactions that are not consistent with financial profile or activities of the customer or do not have connection with their activities, and establishing a limit to amounts and number of transactions. As to the subsequent transactions conducted by using the systems allowing non-face-to-face transactions, necessary measures shall be taken for authentication of the customer and updating the information for customer identification.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Suspicious Activity Reports are made to MASAK: http://www.masak.gov.tr/en/content/suspicious-transactions-reporting/1322

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Reporting obligations are as follows: a) the obliged parties shall report to MASAK any transactions exceeding the amount determined by the Ministry of Finance to which they are party or intermediaries. (For this purpose, transactions which are linked to each other as to their natures shall be considered as a single transaction. Transactions carried out at weekends, on holidays and during night shall be considered as the transaction of the first workday following the date when the transactions were carried out); b) transaction types subject to periodic reporting, reporting procedure and periods, excluded obliged parties and other implementation principles and procedures shall be determined by the Ministry of Finance. The Ministry is authorised to determine, separately for each obliged party, the principles and procedures of filling the periodical reporting forms, submitting them to MASAK through all types of electronic means and communication forms and using electronic signature in the reports. Application dates for electronic reporting shall be determined by the Ministry of Finance; and c) TMCT has issued a Circular (2015/1) based on the Decree No. 32 On the Protection of the Value of Turkish Currency to govern the cash flow principles at the Turkish Customs. The transfer of cash outside of Turkey through customs in an amount equivalent or over USD5,000 is subject to disclosure obligation: http://hukuk.gtb.gov.tr/data/5440c4d7f293704d6c39e7c5/GumNakKont.pdf
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for noncompliance with reporting requirements e.g. tipping off?
A22.	Yes. MASAK states that: "According to Article 13 of Law No. 5549; The obliged parties violating any obligation shall be punished with administrative fine of TRY 9,685 (approx. USD3,000) for 2015 by the Presidency. If the obliged party is a bank, finance company, factoring company, money lender, financial leasing company, insurance and reinsurance company, pension company, capital market institution or bureau de change, administrative fine shall be applied two-fold."
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Article 5 of Law 5549 states that: "In the scope of necessary measures, the Ministry of Finance has the authority to determine obliged parties and implementation principles and procedures, including measures to assign an officer with necessary authority at administrative level for ensuring compliance with this Law and to establish training, internal control and risk management systems by regarding size of business and business volumes." According to Masak General Communiqué 13, suspicious transaction reporting shall be done by filling in STR forms attached to the general or sector-specific suspicious transaction reporting guidelines prepared for the obliged parties. Electronic suspicious transaction reporting shall be done by using MASAK.ONLINE system. Obligated parties who are required to submit STRs electronically and the starting dates of the application shall be determined by MASAK. Guidelines to be published by MASAK shall include procedures and principles related to the accession to and the using of MASAK.ONLINE system by obliged parties. Obligated parties who are deemed appropriate by MASAK, other than those who are required, may also submit suspicious transaction reports electronically. Guidelines to be published by MASAK shall include information on the form, period and contents related to the application for submission of electronic STRs and on filling in STR forms using MASAK.ONLINE system by obliged parties willing to submit STRs electronically. Obligated parties allowed to submit STR forms electronically shall be required to report suspicious transactions through MASAK.ONLINE system as of the date of authorisation. They shall not submit STRs, any more, in paper form.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Article 4(2) of Law No.5549 prohibits institutions and individuals from disclosing to other parties that they have reported a suspicious transaction to MASAK in relation to one of their customers. Article 29 of the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism covers the persons and the institutions who report suspicious transactions as well as any members of the institution who carry out and manage the transaction, their legal representatives and any other personnel that knows that the suspicious transaction has been reported. This regulation prohibits disclosing the fact that a suspicious transaction has been reported to MASAK to parent companies, branches, agencies and affiliated businesses abroad. In addition, internal reports relating to the suspicious transaction may also not be disclosed to these parties. There is also a requirement that access to systems and other information should be restricted to ensure that information regarding suspicious transaction reports remains confidential. Masak General Communiqué No.13 sets forth that in order to categorize an international transaction as a suspicious transaction which may be monitored outside the jurisdiction, obliged parties should determine whether such transaction constitutes a part of customers' business transaction. While there is no specific prohibition, these requirements in combination with the restrictions around the transfer of customer information to other parties, make monitoring of transactions outside of the jurisdiction problematic.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes. The Banking Regulation and Supervisory Agency ("BRSA") requires banks to conduct an independent "Information Systems and Banking Processes Audit" on an annual basis. Although this is not specifically AML related it does include requirements to review the deposits process, new customer creation, customer data entry and change management and money transfer controls.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	Audits are carried out on a yearly basis and the reports are submitted to BRSA with the release of financial statements.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	The information systems audit covers system and controls generally. While testing must be performed as part of this, there is no requirement for this to include AML processes specifically.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Currently, there is no all-encompassing data protection law in Turkey and there is no specific definition of personal data or sensitive data. Likewise, there are no specific laws in relation to the protection of corporate data. A draft data protection law was submitted to Parliament for review on 24 Apr 2008. However, it has not yet received approval from the Turkish parliament. It is envisaged that the new law will govern the protection of personal data, the use of personal data, reliability for the accuracy of data, renewal and erasure requirements, information security and additional requirements about confidential personal data. In the absence of a specific data protection law, there is currently a fragmented set of laws that govern data privacy. The key applicable laws and articles are set out below: a) as per Article 20, titled Privacy of Private Life, of the Constitution of the Republic of Turkey; everyone has the right to demand respect for his/her private and family life; b) as per Article 73 of the Banking Law (No. 5411), staff of Banking Regulation and Supervision Agency and Savings Deposit Insurance Fund shall not disclose the confidential information that they acquire as part of their duties. Besides, those who, by virtue of their positions or in the course of performance of their duties, have access to confidential information about banks or clients are not permitted to disclose such confidential information to any person or entity other than the authorities expressly authorised by law; c) as per Articles 113 and 135 of the Capital Markets Law (No. 4902); the chairman and members of the Capital Markets Board as well as the staff shall not disclose the secrets they have learned during their services to anyone, except the persons authorised according to this Law and their special laws and they cannot use them for the benefit of themselves or others. Persons and institutions from which the Board has outsourced support services as well as their employees shall also be subject to this provision. This obligation shall also continue after retiring from office; d) as per Article 25 of the Civil Law (No. 4721); the person subject to assault on his/her personal rights may claim protection from the judge against the individuals who made the assault. Each assault against personal rights is considered contrary to the laws unless the assent of the person whose personal right is damaged is based on any one of the reasons related to private or public interest and use of authorisation conferred upon by the laws; and e) as per Article 136 of Turkish Criminal Law (No. 5237), any person who unlawfully delivers data to another person, or publishes or acquires the same through illegal means is punished with imprisonment from one year to four years.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	A credit centre has been established within the Banks Association of Turkey for the purpose of collecting credit risk data relating to customers. Credit risk information is shared between eligible member financial institutions (as defined by the BRSA). General data privacy restrictions, outlined above, prohibit the transfer of other private information.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	As there is no all-encompassing law, data protection principles are set out in a patch work of constitutional and other laws.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. The Banking Law and Criminal Code contain secrecy provisions which limit the transfer of information. A criminal offence is in place for banks and bank employees who breach customer confidentiality. All persons or legal entities to which a bank provides services can be regarded as bank customer according to the Article 76 of Banking Law. Accordingly, even customers who makes a one-off payment to the bank counter is regarded as a bank customer even though he/she does not have an account in related bank. It is an offense when the customer secrets are shared with unauthorised persons or used for responsible individual's own or other's benefit. A verbal transfer of customer secrets is also regarded as an offense. Occurrence of damage is not required. The offense cannot occur if a bank employee declares a customer secret negligently. For example, a bank employee may not be sentenced in cases where the transfer of information is unintentional, for example if conversations or documental evidence are heard or seen by third parties incidentally. Furthermore, the aggrieved party may file a suit for damages against the bank, since the bank is also liable as employer for the tortuous acts of its employees within the scope of Obligations Law Article 49, 66 and 116. In this case, the bank may recourse to the responsible employee which declared the customer secret. Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions numbered 6493 ("Law 6493") requires the system operator and payment service provider to use personal information by taking the necessary precautions for protecting personal data. However, according to the Article 90 of the Capital Markets Law numbered 6362, ("CML") the obliged parties shall not refrain from providing information by claiming the confidentiality and secrecy provisions related to existing in CML and special Laws. Recently, Prime Ministry Circular No. 2014/10 on Financial Access, Financial Education and Financial Consumer Protection Strategy and Action Plans which includes principles on protection of consumer data and privacy was adopted and published in the Official Gazette No. 29021 dated 05 Jun 2014.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



United Kingdom

Key contact: Andrew P. Clark
Email: andrew.p.clark@uk.pwc.com
Tel: +44 (0)207 804 5761

Postal address: 1 Embankment Place,
London,
WC2N 6RH

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	A general legal obligation on the part of financial institutions in the UK to identify its customers was first introduced in 1994. The Money Laundering Regulations ("ML Regulations") came into force in the UK on 15 Dec 2007. The Money Laundering (Amendment) Regulations 2012 extended the scope of the Regulations to include all estate agents, included a power for professional supervisory bodies to share information with each other and particularised HMRC's criteria that may be used to determine whether an individual is "fit and proper" in connection with money service businesses and trust and company service providers.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) banks are regulated for AML controls by the Financial Conduct Authority ("FCA") (http://www.fca.org.uk/); b) other financial services are also regulated for AML controls by the FCA; and c) there are a number of AML controls supervisory authorities for the non-financial sector (additional details below). HM Revenue & Customs ("HMRC") (http://www.hmrc.gov.uk) is the supervisory authority for: a) money services businesses not supervised by the FCA; b) high value dealers; c) trust or company service providers not supervised by the FCA or a professional body; d) accountancy service providers not supervised by a professional body; and e) estate agency businesses. The Gambling Commission is the supervisory authority for commercial gambling: http://www.gamblingcommission.gov.uk/ Some designated professional bodies also act as supervisory authorities. These are listed in Schedule 3 to the Money Laundering Regulations 2007: http://www.legislation.gov.uk/ukSI/2007/2157/schedule/3/made Solicitors in England and Wales are regulated for AML controls by the Solicitors Regulation Authority ("SRA") (https://www.sra.org.uk/home/home.page). The SRA is an independent regulatory arm of the Law Society. Barristers in England and Wales are regulated for AML controls by the Bar Standards Board ("BSB") (https://www.barstandardsboard.org.uk/). The BSB is an independent regulatory arm of the Bar Council.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Key sources of practical guidance with regard to AML requirements include: a) the FCA's Financial Crime Guide for Firms Part 1 (Apr 2015) (https://www.handbook.fca.org.uk/handbook/document/FC1_FCA_20150427.pdf) and the FCA's Financial Crime Guide for Firms Part 2 (Apr 2015) (https://www.handbook.fca.org.uk/handbook/document/FC2_FCA_20150427.pdf); b) Joint Money Laundering Steering Group ("JMLSG") Guidance Parts 1 and 2 (http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current); c) Gambling Commission: Money Laundering: the prevention of money laundering and combating the financing of terrorism – Guidance for remote and non-remote casinos, second edition (July 2013) (http://www.gamblingcommission.gov.uk/pdf/prevention%20of%20money%20laundering%20and%20combating%20the%20financing%20of%20terrorism%20-%20july%202013.pdf); d) ICAEW (http://www.icaew.com/en/technical/legal-and-regulatory/money-laundering/uk-law-and-guidance); e) HMRC (http://www.hmrc.gov.uk/MLR/); and f) The Law Society (http://www.lawsociety.org.uk/support-services/risk-compliance/anti-money-laundering/).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, with the FCA leading the work in terms of relevant persons' legal obligations and their practical implementation.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The most recent mutual evaluation follow-up report was conducted in Oct 2009 and can be found at: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/FoR%20UK.pdf This was a follow-up from the Mutual Evaluation conducted in June 2007 which can be found at: http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20UK%20FULL.pdf The IMF United Kingdom 2013 Article IV Consultation Report was issued in July 2013: http://www.imf.org/external/pubs/ft/scr/2013/cr13210.pdf The IMF United Kingdom 2014 Article IV Consultation Staff Report, Press Release and Statement by the Executive Director was issued in Jul 2014: http://www.imf.org/external/pubs/ft/scr/2014/cr14233.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Evidence of identity can be in documentary or electronic form. Individuals: full name, residential address and date of birth ideally from a government issued document which includes the customer's full name and photo, and either residential address or date of birth e.g. valid passport, valid photo card driving licence etc.; or a government issued document (without a photograph) which includes the customer's full name, supported by a second document, either government-issued, or issued by a judicial authority, a public sector body or authority, a regulated utility company, or another FCA-regulated firm in the UK financial services sector or in an equivalent jurisdiction, which includes the customer's full name and either residential address or date of birth. Corporates (other than regulated firms): full name, registration number, registered office in country of incorporation and business address. Additionally, for private / unlisted companies: names of all directors (or equivalent), names of individuals who own or control over 25% of its shares or voting rights and names of any individual(s) who otherwise exercise control over the management of the company. The firm should verify the existence of the corporate from either confirming the company's listing on a regulated market, conducting a search of the relevant company registry or obtaining a copy of the company's Certificate of Incorporation. For private / unlisted companies, the firm may decide, following a risk assessment, to verify one or more of the directors as appropriate in line with the CDD requirements for individuals. In respect of beneficial owners, the relevant person must take risk based and adequate measures to verify the identity of the beneficial owner(s).
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	UK AML Guidance states that where identity is verified electronically, or copy documents are used, the firm should apply an additional verification check to manage the risk of impersonation fraud. For example, one of these checks may be to require copy documents to be certified by an appropriate person.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The ML Regulations define beneficial owners as individuals either owning or controlling more than 25% of bodies corporate or partnerships (or at least 25% of trusts) or otherwise owning or controlling the customer. The JMLSG Guidance stipulates that the firm must know the names of all individual beneficial owners owning or controlling more than 25% of the company's shares or voting rights (even where these interests are held indirectly) or who otherwise exercise control over the management of the company. The firm must take risk based and adequate measures to verify the identity of those individuals.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence may be applied to: a) certain regulated firms in the financial sector; b) companies listed on a regulated market subject to specified disclosure obligations; c) beneficial owners of pooled accounts held by notaries or independent legal professionals; d) UK public authorities; e) European Community institutions; f) certain life assurance and e-Money products; g) certain pension funds; h) certain low risk products; and i) child trust funds and junior ISAs.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	A firm must apply, on a risk-sensitive basis, enhanced customer due diligence measures and enhanced ongoing monitoring in any situation which by its nature can present a higher risk of money laundering or terrorist financing. The three specific types of relationship in respect of which enhanced due diligence measures must be applied are: a) where the customer has not been physically present for identification purposes; b) in respect of a correspondent banking relationship with Respondents from non-European Economic Area ("EEA") states; or c) in respect of a business relationship or an occasional transaction with a PEP.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Where a firm proposes to establish a business relationship or carry out a one off transaction with a PEP the relevant person must: a) have appropriate risk based procedures to determine whether a customer is a PEP; b) obtain appropriate senior management approval for establishing the business relationship with that customer; c) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or occasional transaction; and d) conduct enhanced ongoing monitoring of the relationship.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Enhanced customer due diligence must be undertaken by Correspondents on Respondents using a risk based approach. The following risk indicators should be considered both when initiating a relationship, and on a continuing basis thereafter, to determine the levels of risk-based due diligence that should be undertaken: a) the Respondent's domicile; b) the Respondent's ownership and management structures; c) the Respondent's business and customer base; and d) downstream Correspondent Clearing. Where a Correspondent bank is outside the EEA, the UK bank should thoroughly understand its correspondent's business, reputation, and the quality of its defences against money laundering and terrorist financing. Senior management must give approval to each new correspondent banking relationship.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.
Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	Where a customer has not been physically present for identification purposes, a firm must take specific and adequate measures to compensate for this higher risk by applying one or more of the following measures: a) ensuring that the customer's identity is established by additional documents, data or information; b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the Money Laundering Directive; or c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	National Crime Agency ("NCA"): http://www.nationalcrimeagency.gov.uk/
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: Oct 2013 - Sept 2014 - 354,186 SARs (Source: NCA Suspicious Activity Reports (SARs) Annual Report 2014: http://www.nationalcrimeagency.gov.uk/publications/suspicious-activity-reports-sars/464-2014-sars-annual-report/file) Comparative GDP data is not available for this specific period.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Where firms believe that they hold funds or assets for a sanctioned party, this must always be reported to the Asset Freezing Unit at HM Treasury as soon as practicable. There are no other specific reporting obligations outside of suspicious transactions.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Yes, the Proceeds of Crime Act 2002 ("POCA") outlines the following penalties with regard to reporting requirements: a) Failure to report: up to five years imprisonment and/or an unlimited fine; and/or b) Tipping off: up to five years imprisonment and/or unlimited fine. Changes to the Money Laundering Regulations 2007 which came into force on 01 Oct 2012, included the power to impose penalties for failure to provide information required by notice.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No, however, the transaction monitoring should be performed by using adequate means which assumes use of some automated technology for larger organisations.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Consent is required from the NCA (the UK FIU) to proceed with a current/ongoing transaction that is identified as suspicious.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes. The processing or retaining of personal data in the UK is governed by the Data Protection Act 1998 (DPA): a) the DPA regulates the processing of 'personal data'. The information obtained/retained by a relevant person for the purposes of customer due diligence would fall within the definition of personal data; b) the DPA only applies to individuals and not legal persons. It therefore does not extend protection to corporate data; and c) yes. Section 2 of the DPA provides a separate definition of "sensitive personal data" which relates to personal data consisting of information as to the racial or ethnic origin of the data subject, their political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union, their physical or mental health or condition, their sexual life, their commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings. In addition to meeting one of the conditions for processing in Schedule 2 of the DPA, at least one of several other conditions listed in Schedule 3 of the DPA must be met in the case of processing of sensitive personal data. Additional regulations such as the Data Protection (Processing of Sensitive Personal Data) Order 2000 and subsequent orders also provide that sensitive personal data can be processed where there is substantial public interest, such as the prevention or detection of crime, and protecting the public against malpractice or maladministration. For further information see 'The Guide to Data Protection' published by the Information Commissioner's Office: http://ico.org.uk/for_organisations/data_protection/~media/documents/library/Data_Protection/Practical_application/the_guide_to_data_protection.pdf
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Credit reports are personal data and the processing and transmission of this category of information is governed by the DPA. Both criminal records and medical data fall within the definition of sensitive personal data and therefore in order to process such data, the data controller must meet at least one of the additional conditions identified in Schedule 3 of the DPA.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	The DPA regulates the sending of personal data outside of the EEA. The Act contains a prohibition on data being sent to countries that do not ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. No corresponding provisions exist governing the receipt of personal data from countries outside the EEA. Once received by an entity or individual within the United Kingdom, the data is subject to the requirements of the DPA.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	The UK does not have bank secrecy laws. The case of <i>Tournier v National Provincial and Union Bank of England</i> [1924] determined that it is an implied term of the contract between customers and a bank that the bank will keep the customers’ information confidential. The scope of confidentiality extends to all information held on a customer. However, a bank’s duty of confidentiality is not absolute. The case established the conditions under which banks owed confidentiality to their clients and circumstances allowing banks to legally disclose information about their customer. These principles include: a) where the financial institution is compelled by law to disclose the information; b) if a financial institution has a public duty to disclose the information; c) if the financial institution’s own interests require disclosure; and d) Where the customer has consented, even implicitly, to disclosure.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Ukraine

Key contact: Gennadiy Chuprykov / Victoriya Tsytzak
Email: gennadiy.chuprykov@ua.pwc.com / victoriya.tsytzak@ua.pwc.com
Tel: +38 044 490 6777

Postal address: Eurasia Business Center,
10th floor, 75 Zhylyanska,
Kyiv 01032, Ukraine

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The new edition of the AML law was adopted on 14 Oct 2014 and became effective on 06 Feb 2015. This replaced the 28 Nov 2002 Law of Ukraine on Prevention and Counteraction to Legalisation (Laundering) of the Proceeds of Crime or Terrorist Financing.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	The new law introduces several substantial changes to the current legislative regime, namely: a) strengthens the requirements towards subjects' internal monitoring procedures by imposing a risk based assessment approach to all the subjects of the law and shorter reporting terms; b) extends the subjects of the law by introducing audit firms precisely; c) introduces national politically exposed persons as a risk trigger for extensive internal identification of the transaction; and d) strengthens the administrative and criminal sanctions for violations thereof.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) banking: a. The National Bank of Ukraine (http://www.bank.gov.ua/control/en/); and b. State Committee for Financial Monitoring of Ukraine ("SCFM") (http://www.sdfm.gov.ua/); b) other financial services: a. SCFM (http://www.sdfm.gov.ua/); b. National Securities and Stock Market Commission (www.nssmc.gov.ua); and c) non-financial sector: a. Ministry of Justice of Ukraine (http://www.minjust.gov.ua/); and b. SCFM (http://www.sdfm.gov.ua/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	All authorities listed in A3 provide regulations and clarifications as to the application of the AML law in the form of regulatory legal acts which can be found on the websites of relevant authorities.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. According to the Law of Ukraine on Prevention and Counteraction to Legalisation (Laundering) of the Proceeds of Crime or Terrorist Financing, the subject of primary financial monitoring shall proceed with the classification of its clients taking into account risk criteria. The risk criterion was approved by the Decree of State Committee for Financial Monitoring of Ukraine #126 on 03 Aug 2010. Starting from the effective date of the new edition of the law, all subjects of the law shall apply a risk based approach to identification of their clients and performing internal monitoring procedures. The risk criteria are still to be adopted.

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The last mutual evaluation report was conducted in Mar 2009: http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round3/MONEYVAL(2009)4Rep-UKR3_en.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Financial operations / customers are not subject to financial monitoring / due diligence if the transaction amount is less than UAH150,000 (approx. USD6,410).

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: name, date of birth, personal identity document details, residential (registration) address and actual address, taxpayer identification number and source of funds. Private Entrepreneur: name, date of birth, personal identity document details, residential (registration) address and actual address, bank account details (if any) and source of funds. Legal entities: the full name, registration address, information about management and controllers of the company, shareholder structure, registration number ("EDRPOU") and bank account details.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Legal entities accepting the identification documentation should be sure that the copies of such documentation correspond to the originals, i.e. either a contractor's internal verification or external authentication (notary, apostille) will be needed.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Beneficial owners need to be known in all cases, but the level of requirements for identification depends on the type of transaction and risk involved.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence can be applied if: a) the client is either a state body, a state company, or an international organisation Ukraine is a member of; b) the financial transaction takes place at the organised securities market; c) the client is an official organisation, office or agency of European Union; d) the client is an embassy of another state accredited in Ukraine; or e) the client is listed on a regulated stock exchange which reveals the beneficial owners of the participants.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	a) the client originates from FATF blacklist countries; and b) PEPs are involved in the transaction.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	In all cases where PEPs are the beneficial owners of a potential client or the direct client of the law subject.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Correspondent banking relationships with non-resident banks (except for the banks registered in EU countries and FATF member countries) are high risk relationships and are subject to enhanced identification requirements and additional documentation review: a) information regarding the client's identification and client's owners should be checked; b) enhanced monitoring of all of the client's financial transactions should be performed; and c) other measures stipulated in the internal procedures should be taken.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	The concept of shell banks is not specified in Ukrainian legislation. Generally fictitious business is considered a criminal offence under the Criminal Code of Ukraine.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	In all cases of providing services using the latest technology, including support of operations without direct contact with the client.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	SFMS: http://www.sdfm.gov.ua/
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 - 1,297,324 SARs GDP (in current prices): 2014 - USD 131,805m (Source: data.worldbank.org) This results in a ratio of 1 SAR for every USD101,593 of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	A transaction must be reported if it exceeds or is equal to UAH150,000 (approx.USD6,410); for gambling industry UAH13,000 (approx. USD560) and has one or more of the following features: a) the transfer of money is to an anonymous bank account or an account in the offshore zone; b) buying and selling cheques, travellers' cheques or other similar payments for cash; c) any transaction in which the receiver or sender is located in a country which does not have AML legislation and which does not cooperate with other countries in the area of AML; d) the transfer of the money is to a third party the day after the transaction; e) the transfer of money is to the account of a private entrepreneur or legal entity that was opened less than three months or in the case where there were no transactions to/from the bank account of the private entrepreneur or legal entity from the registration date; f) the transfer of money to a foreign company without contract; and/or g) payment in cash, etc.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Below the thresholds as stipulated in A20, transactions do not need to be reported according to the AML law. However, the threshold should be applied by taking into consideration all other qualitative characteristics of transactions and customers as stipulated by the AML law.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, the applied penalties may be either of financial nature (the fine is calculated on a case by case basis) or of regulatory nature (e.g. withdrawal of a licence). The type and severity of sanctions depend on the specific case.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Generally there are no such requirements. Such requirements are stipulated only for banks by the National Bank of Ukraine.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	There is a requirement to report suspicious transactions. If after a certain period of time the authority does not prohibit the transaction, the law subject can proceed with the transaction.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank’s AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, Data Protection Law (Jun 2010): a) yes; b) corporate data for legal entities is covered. However, according to the Ukrainian "Data Protection Law" corporates cannot gather, analyse or provide any information on individuals that may be considered as personal since it is confidential information by Law. This information can be gathered and analysed only based on an individual's written consent, otherwise the violation is subject to criminal liability; and c) yes. Personal data regarding racial or ethnic origin, political, religious or ideological beliefs, membership in political parties and trade unions, charge with a crime or criminal sanction application, as well as data concerning health or sex life is considered as "sensitive data". Such information can be processed only upon the relevant person's consent or in order to protect the relevant person's rights. Otherwise the processing of sensitive personal data is prohibited.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	The gathering, processing and transferring of such data is possible with the consent of the person whose data is transferred.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes, Ukrainian Data Protection Law and International Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data approved by Ukraine (1981) (transfer of information from / to countries that did not ratify this Convention requires enhanced regulation by parties).
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. Data that was obtained by the bank in the process of providing the services to its clients and data defined by its owner as confidential is the subject of regulation of the Law On Banks and Banking Activity and the Law On Information.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Bahrain

Key contact: Madhukar Shenoy
Email: madhukar.shenoy@ac.pwc.com
Tel: +973 1 711 8800

Postal address: Jeera I Tower,
13th Floor, Seef District,
Manama, Bahrain

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2001 (amended 2006). The Anti Money Laundering & Terrorist Financing Unit ("AMLTU") was established in Jul 2002, under the direct control of the Ministry of the Interior. The AMLTFU is the money laundering enforcement unit in the Kingdom of Bahrain responsible for receiving, requesting, analysing and disseminating disclosures of financial information to the investigatory and supervisory authorities concerning suspected proceeds of crime and alleged money laundering.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	Central Bank of Bahrain ("CBB") is responsible for enforcing AML controls for CBB licensed institutions including banks and other institutions in the financial services sector: http://www.cbb.gov.bh The Ministry of Industry and Commerce ("MOIC") is responsible for enforcing AML controls for the non-financial sector: http://www.moic.gov.bh/En/Pages/Home.aspx
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes. CBB website for information on AML & Combating the Financing of Terrorism ("CFT") (http://www.cbb.gov.bh/page.php?p=aml_cft) and The Ministerial Order No. 23 of 2002.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No. However banks are required to review and update their records at least every three years.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, the CBB uses a risk based approach to customer due diligence and ongoing monitoring through its rulebooks. The CBB requires banks to have effective anti-money laundering policies and procedures in addition to measures for combating the financing of terrorism.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No, Bahrain's compliance with international AML/CFT standards was assessed by the International Monetary Fund in 2005, as part of a financial sector assessment programme review. The report was approved by the IMF in Jan 2006. The same report was subsequently discussed and endorsed by the MENA-FATF in Nov 2006: http://www.cbb.gov.bh/assets/pdf/Bahrain_FSAP%20Report_2006.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes. Financial institutions: The Financial Crime module of CBB Rulebook Volume 1 (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) states that a bank must implement customer due diligence measures when: a) establishing business relations with a new or existing customer; b) a change to the signatory or beneficiary of an existing account or business relationship is made; c) a significant transaction takes place; d) there is a material change in the way that the bank account is operated or in the manner in which the business relationship is conducted; e) customer documentation standards change substantially; f) the bank has doubts about the veracity or adequacy of previously obtained customer due diligence information; g) carrying-out one-off or occasional transactions above BHD6,000 (approx. USD15,980), or where several smaller transactions that appear to be linked fall above this threshold; h) carrying out wire transfers irrespective of amount; or i) there is a suspicion of money laundering or terrorist financing. Non financial institutions: Article 4 of Ministerial Order No.23 of 2002 exempts the following transactions from customer due diligence: a) the transaction or transactions which total less than BHD10,000 (approx. USD26,630); b) transactions related to life insurance if the premiums are paid through an account opened for the customer in a local bank; and c) transactions related to a retirement scheme if they arise from the Insured's occupation or contract of employment or if the amount of subscriptions is paid through an account opened for the customer in a local bank.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Financial institutions: The Financial Crime module (FC – 1.2) of CBB Rulebook Volume 1 (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) states that banks must obtain and record the following information, where applicable: In the case of natural person: Full legal name and any other names used/Full permanent address/Date and place of birth/Nationality/Passport number/CPR or residency number/Telephone/Fax number/Email address/Occupation or public position held/Employer's name and address (if self-employed, the nature of the self-employment)/Type of account and nature and volume of anticipated business dealings with the conventional bank licensee/Signature of the customer(s)/Source of funds. Confirmation of the date of birth and legal name should be carried out by obtaining a copy of a current valid official original identification document (e.g. birth certificate, passport, CPR or Iqama). As for the permanent residential address, a copy of a recent utility bill, bank statement or similar statement from another bank or financial institution, or some form of official correspondence or official documentation card, such as CPR, from a public/governmental authority, or a tenancy agreement or record of home visit by an official of the bank should be considered. In the case of legal entities: The entity's full name and other trading names used/Registration number (or equivalent)/Legal form/Registered address and trading address/Type of business activity/Date and place of incorporation or establishment/Telephone, fax number and email address/Regulatory body or listing body (for regulated activities such as financial services and listed companies)/Name of external auditor/Type of account, and nature and volume of anticipated business dealings with conventional bank licensees/Source of funds. The information obtained must be verified in accordance with CBB requirements as per FC – 1.2.4 to FC – 1.2.6 and FC – 1.2.8. Non-financial institutions: Article 4 of Ministerial Order No.23 of 2002 identifies details to be established and kept on record for non-financial institutions where applicable: In the case of natural persons: Customer's full name/Date of birth/Nationality/Full details of the identity card or passport/Central Population Register (CPR) Card number (if any)/Occupation/Usual residence address/Employer's name and address. In the case of a corporate client: Customer's full name/Legal status/Registration number and place/Address of the head office and branches (if any)/Names of board members/Legal representative of the corporate person and his identification. The Memorandum and Articles of Association and the Power of Attorney must also be verified for incorporated activities.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Financial institutions: The Financial Crime module (FC – 1.2.4 and FC - 1.2.5) of CBB Rulebook Volume 1 (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) states that an authorised official of the licensee must certify copy documents, by viewing the original and writing on the copy the words 'original sighted', together with the date and a signature. Equivalent measures must be taken for electronic copies. Identification documents which are not obtained by an authorised official of the licensee in original form must instead be certified by one of the following from a Gulf Cooperation Council ("GCC") or FATF member state: a lawyer; a notary; a chartered/certified accountant; an official of a government ministry; an official of an embassy or consulate; or an official of another licensed financial institution or of an associate company of the licensee. The individual making the certification under FC-1.2.5 must give clear contact details (e.g. by attaching a business card or company stamp). The bank must verify the identity of the person providing the certification through checking membership of a professional organisation (for lawyers or accountants), or through checking against databases/websites, or by direct phone or email contact. Non-financial institutions: Article 4 of Ministerial Order No.23 of 2002 details that before establishing any business relationship, registered persons shall establish the identities of their customers, representatives and beneficiaries from the transaction by using all the reasonable methods and adopt all the possible precautions to ascertain the validity of documents or details concerning their identities.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Financial institutions: The Financial Crime module (FC – 1.1.5 to FC - 1.1.7 and FC - 1.6.1) of CBB Rulebook Volume 1 (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) states that banks must obtain a signed statement from all new customers confirming whether or not the customer is acting on their own behalf. This undertaking must be obtained prior to conducting any transactions with the customer concerned. Where a customer is acting on behalf of a third party, the bank must also obtain a signed statement from the third party, confirming they have given authority to the customer to act on their behalf. Where the third party is a legal person, the bank must have sight of the original board resolution (or other applicable document) authorising the customer to act on the third party's behalf, and retain a certified copy. Banks must establish and verify the identity of the customer and (where applicable) the party/parties on whose behalf the customer is acting, including the beneficial owner of the funds. In the case of minors, banks must additionally verify the identity of the parent(s) or legal guardian(s). Where a third party on behalf of a person lacking full legal capacity wishes to open an account, the bank must establish the identity of that third party as well as the intended account holder. Financial services must not be provided to charitable funds and religious, sporting, social, cooperative and professional societies, until an original certificate authenticated by the relevant Ministry confirming the identities of those purporting to act on their behalf (and authorising them to obtain the said service) has been obtained. For clubs and societies registered with the General Organisation for Youth & Sports (GOYS), banks must contact GOYS to clarify whether the account may be opened in accordance with the rules of GOYS. In addition, in the case of sports organisations registered with the Bahrain Olympic Committee (BOC), banks must contact BOC to clarify whether the account may be opened in accordance with the rules of BOC. Non-financial institutions: Ministerial Order No.7 of 2001 requires each institution to verify a customer's identity and his source of funds and obtain proof that: - establishes the customer's identity; - establishes that the source of funds is as claimed by the customer; and - determines the customer's address, date of birth and nationality. If the customer is an agent of a business or firm subject to the supervision of a controlling authority and resides in a country that has similar laws for prohibition and combating money laundering, it may be sufficient evidence to receive written confirmation from the customer of the availability of proof of the principal's identity, its registration and maintenance thereof.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Financial institutions: The Financial Crime module (FC – 1.11) of CBB Rulebook Volume 1 (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) states that banks may apply simplified due diligence if: a) the customer is the CBB, the Bahrain Bourse ("BHB") or a licensee of the CBB; b) the customer is a Ministry of a GCC or FATF member state government, a company in which a GCC or FATF government is a majority shareholder, or a company established by decree in the GCC; c) the customer is a company listed on a GCC or FATF member state stock exchange (where the FATF state stock exchange has equivalent disclosure standards to those of the BSE); d) the customer is a financial institution whose entire operations are subject to AML/CFT requirements consistent with the FATF recommendations/special recommendations and it is supervised by a financial services supervisor in a FATF or GCC member state for compliance with those requirements; e) the customer is a financial institution which is a subsidiary of a financial institution located in a FATF or GCC member state, and the AML/CFT requirements applied to its parent also apply to the subsidiary; f) the customer is a borrower in a syndicated transaction where the agent bank is a financial institution whose entire operations are subject to AML/CFT requirements consistent with the FATF recommendations/special recommendations and it is supervised by a financial services supervisor in a FATF or GCC member state for compliance with those requirements; and g) the transaction is a one-off or occasional transaction not exceeding BHD6,000 (or equivalent in other currencies), or one of a number of transactions which are related and, when taken together, do not exceed BHD6,000 per year (or equivalent in other currencies). Non-financial institutions: Article 4.7 of Ministerial Order No.7 of 2001 specifies that procedures for proving a customer's identity and sources of funds of the following shall not be applicable if: a) the customer is an organisation affiliated to or under the supervision of the Ministry of Commerce and Industry, the Bahrain Stock Exchange, the Ministry of Justice or if it is a company in which the government has a majority stake, or if it is a company incorporated by virtue of a law or decree; b) the subject matter of the transaction is the payment of sums by the customer or on his behalf through another organisation; c) a separate significant transaction takes place with or for the account of a third party with the intervention of a person who is subject to a supervisory authority, who has provided confirmation that the identity of the third party has been established and registered according to the custody procedures of such person; and d) the customer purchases a stake in a collective investment venture.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	The CBB Rulebook Volume 1, Financial Crime module FC – 1.3 to FC 10A (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) states that enhanced customer due diligence must be performed on those customers identified as having a higher risk profile and additional enquiries made or information obtained in respect of those customers. Specific conditions that give rise to a higher risk profile include: instances where there is non-face-to-face business; dealing with PEPs; dealing with charities, clubs and other societies; dealing with a professional intermediary who manages pooled funds; and dealing with a correspondent bank and cross border cash transactions equal to and above BHD6,000 (approx. USD15,980) by courier.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	The Financial Crime module (FC – 1.5) of CBB Rulebook Volume 1 (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) states that Banks must have appropriate risk management systems to determine whether a customer is a PEP, both at the time of establishing business relations and thereafter on a periodic basis. Banks must utilise publicly available databases and information to establish whether a customer is a PEP. Banks must establish a client acceptance policy with regard to PEPs, taking into account the reputational and other risks involved. Senior management approval must be obtained before a PEP is accepted as a customer. Where an existing customer is a PEP, or subsequently becomes a PEP, enhanced monitoring and customer due diligence measures must include: a) analysis of complex financial structures, including trusts, foundations or international business corporations; b) a written record in the customer file to evidence that reasonable measures have been taken to establish both the source of wealth and the source of funds; c) development of a profile of anticipated customer activity, to be used in ongoing monitoring; d) approval of senior management for allowing the customer relationship to continue; and e) on-going account monitoring of the PEP's account by senior management such as the MLRO.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The Financial Crime module (FC – 1.8) of CBB Rulebook Volume 1 (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) states that Banks must implement the following additional measures, prior to opening a correspondent banking relationship: - complete a signed statement that outlines the respective responsibilities of each institution in relation to money laundering detection and monitoring responsibilities; and - ensure that the correspondent banking relationship has the approval of senior management. Banks which intend to act as correspondent banks must gather sufficient additional information (e.g. through a questionnaire) about their respondent banks to understand the nature of the respondent's business. Factors to consider include: - information about the respondent bank's ownership, structure and management; - major business activities of the respondent and its location (i.e. whether it is located in a FATF compliant jurisdiction) as well as the location of its parent (where applicable); - where the customers of the respondent bank are located; - the respondent's AML and CFT controls; - the purpose for which the account will be opened; - confirmation that the respondent bank has verified the identity of any third party entities that will have direct access to the correspondent banking services without reference to the respondent bank; (e.g. in the case of 'payable through accounts') - the extent to which the respondent bank performs on-going due diligence on customers with direct access to the account, and the condition of bank regulation and supervision in the respondent's country (e.g. from published FATF reports). Banks should take into account the country where the respondent bank is located and whether that country abides by the FATF 40+ 9 recommendations when establishing correspondent relationships with foreign banks. Banks should obtain where possible copies of the relevant laws and regulations concerning AML/CFT and satisfy themselves that respondent banks have effective customer due diligence measures consistent with the FATF 40+ 9 recommendations; - confirmation that the respondent bank is able to provide relevant customer identification data on request to the correspondent bank; and - whether the respondent bank has been subject to a money laundering or terrorist financing investigation.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes. The Financial Crime module (FC – 1.10) of CBB Rulebook Volume 1 (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) states that Banks must not establish business relations with banks which have no physical presence or "mind and management" in the jurisdiction in which they are licensed and which is unaffiliated with a regulated financial group. Banks must not knowingly establish relations with banks that have relations with shell banks. Banks must make a suspicious transaction report to the Anti-Money Laundering unit & the Compliance Directorate if they are approached by a shell bank or an institution they suspect of being a shell bank.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	The Financial Crime module (FC - 1.4) of CBB Rulebook Volume 1 (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) states that where no face-to-face contact takes place, banks must take additional measures in order to mitigate the potentially higher risk associated with such business. In particular, banks must take measures to ensure that the customer is the person they claim to be and that the address provided is genuinely that of the customer. There are multiple checks that can provide a bank with a reasonable degree of assurance as to the authenticity of the applicant: - telephone contact with the applicant on an independently verified home or business number; - with the customer's consent, contacting an employer to confirm employment, via phone through a listed number or in writing; and - salary details appearing on recent bank statements.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	For licensees registered under the CBB, SARs must be simultaneously sent to both the CBB (www.cbb.gov.bh) and the AMLTFU. For licensees registered under the Ministry of Industry and Commerce, SARs must be simultaneously sent to both the MOIC (http://www.moic.gov.bh/En/Pages/Home.aspx) and the AMLTFU.
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Financial Institutions: The Financial Crime module (FC – 5.1.1) of CBB Rulebook Volume 1 (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) specifies that banks must implement procedures to ensure that staff who handle customer business (or are managerially responsible for such staff) make a report promptly to the MLRO if they know or suspect that a customer (or a person on whose behalf a customer may be acting) is engaged in money laundering or terrorism financing, or if the transaction or the customer's conduct otherwise appears unusual or suspicious. These procedures must include arrangements for disciplining any member of staff who fails, without reasonable excuse, to make such a report. Non-financial institutions: Ministerial Order No.7 of 2001 Article 4.9 specifies that all institutions shall report to the Anti Money Laundering Unit any suspicious or extraordinary transactions regardless of the value of amounts subject to the transaction.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No. A transaction is considered significant if it is above BHD6,000 (approx. USD15,980) or where several smaller transactions that appear to be linked fall above this threshold.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Article 3.4 and Article 3.5 of Law No. (4) of 2001 (http://cbb.complinet.com/file_store/pdf/rulebooks/AppendixFC1.pdf) specifies that: a) any person who commits any of the offences related to money laundering shall be liable to imprisonment for a period not exceeding two years and/or a fine not exceeding BHD50,000 (approx. USD133,140) or both; and b) any person who contravenes the provisions of Regulations and Ministerial Regulations issued under this law shall be liable to imprisonment for a period not exceeding three months or a fine not exceeding BHD20,000 (approx. USD53,250) or both.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	The Financial Crime module (FC – 2.1 and FC – 2.2) of CBB Rulebook Volume 1 (http://cbb.complinet.com/cbb/display/display.html?rbid=1820&element_id=5272) specifies that banks must take reasonable care to establish and maintain appropriate systems and controls to limit their vulnerability to financial crime. These systems and controls must be documented, approved and reviewed annually by the Board of the bank. The documentation and the Board's review and approval, must be made available upon request to the CBB. Banks must develop risk-based monitoring systems appropriate to the complexity of their business, their number of clients and types of transactions. These systems must be configured to identify significant or abnormal transactions or patterns of activity. Such systems must include limits on the number, types or size of transactions undertaken outside expected norms; and must include limits for cash and non-cash transactions. The banks' risk-based monitoring systems should therefore be configured to help identify: a) transactions which do not appear to have a clear purpose or which make no obvious economic sense; b) significant or large transactions not consistent with the normal or expected behaviour of a customer; and c) unusual patterns of activity (relative to other customers of the same profile or of similar types of transactions, for instance because of differences in terms of volumes, transaction type, or flows to or from certain countries), or activity outside the expected or regular pattern of a customer's account activity. Banks must consider the need to include automated transaction monitoring as part of their risk-based monitoring systems to spot abnormal or unusual flows of funds. In the absence of automated transaction monitoring systems, all transactions above BHD6,000 (approx. USD15,980) must be viewed as significant and be captured in a daily transactions report for monitoring by the MLRO or a relevant delegated official, and records to be retained by the bank for five years after the date of the transaction. CBB would expect larger banks to include automated transaction monitoring as part of their risk-based monitoring system.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No, unless the bank is specifically requested by the CBB to do so.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Article 8 of Law No. (4) of 2001 (http://cbb.complinet.com/file_store/pdf/rulebooks/AppendixFC1.pdf) states that where a foreign state makes a request for specific information relating to suspicious transactions, persons and corporations involved in those transactions or the investigation or prosecution of a money laundering offence, the AMLTFU shall execute the request or inform the foreign state of any delay in or the reason for not executing the request.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes. The licensee must instruct their external auditors to produce the report referred to in Paragraph FC-4.3.1(d). (http://www.complinet.com/cbb/display/display_viewall.html?rbid=1820&element_id=3371).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) at least once each calendar year; b) the report must be submitted to CBB by the 30 April of the following year. The report and its findings must be received and acted upon by the bank; and c) it is a separate report and not part of the financial statement audit.
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	The scope of the review must include: a) a report, containing the number of internal reports made in accordance with Section FC-5.1, a breakdown of all the results of those internal reports and their outcomes for each segment of the licensee's business, and an analysis of whether controls or training need to be enhanced; b) a report, indicating the number of external reports made in accordance with Section FC-5.2 and, where a licensee has made an internal report but not made an external report, noting why no external report was made; c) a sample test of compliance with this Module's customer due diligence requirements; and d) a report as to the quality of the licensee's anti-money laundering procedures, systems and controls, and compliance with the AML Law and this Module. (http://www.complinet.com/cbb/display/display_viewall.html?rbid=1820&element_id=3371).

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	In accordance with Article 117 of the CBB Law, banks must not publish or release information to third parties concerning the accounts or activities of their individual customers, unless: a) such information is requested by the CBB or by an order from the Courts; b) the release of such information is approved by the customer concerned; or c) it is in compliance with the provision of the law or any international agreements to which the Kingdom is a signatory. (http://cbb.complinet.com/cbb/display/display.html?rbid=1820).
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Bahrain recently (2015) amended the CBB Law of 2006. One of the amendments expands the definition of confidential information to cover credit information and credit reports.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	In accordance with Article (1) of Law (7) of the Year 2003 on The Trade Secrets, any natural or legal person is prohibited from disclosing information in his possession if such an information contains the following features: a) if the information is confidential. Confidentiality is thereto fulfilled if the information in its final form or its specifics are unknown nor circulated and is not accessible for those who usually deal with such type of information; b) if it was of a commercial value due to its confidentiality; and c) if its confidentiality was dependable on the effective measures undertaken by its legal holder to preserve it. (http://www.wipo.int/wipolex/en/text.jsp?file_id=198907). Within the course of implementing provisions of this law, the information stipulated in the features hereinabove are thereto regarded as trade secrets.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	In accordance with Article (2) of Law No. (7) for the Year 2003 on The Trade Secrets, disclosure prohibition of the previously prescribed trade secrets in the above Article extends to include confidential tests and data that were the outcome of notable efforts, and which are submitted to the competent authorities at their request for approval of promoting pharmaceutical or agrichemical products in which new chemical components are used. The competent authorities shall be obliged not to disclose received data or tests of those mentioned in the previous paragraph until the same is no longer confidential, and prohibit unfair commercial use of the said data or tests by means of not permitting any person without the consent of the owner from depending on it to market his own products or pharmaceutical products until after five years consecutive to the date of marketing approval in the Kingdom of Bahrain. (http://www.wipo.int/wipolex/en/text.jsp?file_id=198907).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Iraq

Key contact: Bashar Akroush
Email: bashar.akroush@iq.pwc.com
Tel: +964 (0) 7719945688

Postal address: Golan Street,
English Village,
Villa 252, Erbil, Iraq

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Iraqi AML law became effective in 2004.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) Central Bank of Iraq ("CBI") http://www.cbi.iq; b) N/A; and c) real estate agents, accountants, lawyers, notaries and trust and company service providers are not subject to the AML law. While the AML Law applies to dealers in precious metals, stones and jewels, no supervision of this sector exists.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	N/A
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Article 15(5) of the AML Law requires financial institutions to apply CDD/KYC measures to accounts which existed prior to effectiveness of the AML Law, "unless the financial institution reasonably believes that it knows the true identity of the customer." This provision allows application of a risk based approach to accounts which existed prior to enactment of the AML Law.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Article 15 of the AML Law permits a financial institution to determine the extent of due diligence obtained on a risk sensitive basis depending on the type of customer, business relationship or transaction.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise since 2003? If yes, please find a link to a relevant report (if publicly available).
A7.	Iraq was subject to a MENAFATF Mutual Evaluation Report published on 28 Nov 2012 which can be accessed here: http://www.menafatf.org/MER/MER_Iraq_English.pdf In October 2013, Iraq made a high-level political commitment to work with the FATF and MENAFATF to address its strategic AML/CFT deficiencies. Iraq will work on implementing its action plan to address these deficiencies, including by: a) adequately criminalising money laundering and terrorist financing; b) establishing and implementing an adequate legal framework for identifying, tracing and freezing terrorist assets; c) establishing effective customer due diligence measures; d) establishing a fully operational and effectively functioning Financial Intelligence Unit; e) establishing suspicious transaction reporting requirements; and f) establishing and implementing an adequate AML/CFT supervisory and oversight programme for all financial sectors. The FATF Public Statement issued on 18 Oct 2013 can be accessed here: http://www.fatf-gafi.org/countries/d-i/iraq/documents/fatf-compliance-oct-2013.html#Iraq

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Transactions below IQD5m (approx. USD4,520) for non-account holders only require the collection and verification of customer name and address unless the transaction is deemed suspicious in which case the dispensation does not apply.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Article 15 of the AML Law requires a financial institution to obtain the following information when opening an account for a customer: Individuals: Legal name and any other names used, correct permanent address including the full street address, telephone number, fax number, email address, date and place of birth. Corporates: Charter or other establishing document, nationality, occupation, public position held and/or name of employer, an official personal identification number or other unique identified contained in an unexpired official document (e.g. passport, identification card, residence permit, driving license) that bears a photograph of the individual customer, type of account and nature of the business relationship and signature. All information that is obtained should be verified. The requirement to understand the purpose and intended nature of the business relationship only arises if there is reason to suspect money laundering.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Article 15 of the AML Law requires that all information obtained is verified.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Article 17 of the AML Law obligates financial institutions to "undertake such verification as is necessary in order to form a reasonable belief that it knows the true identity of the customer and/or any beneficial owner of the funds." It further requires financial institutions to have procedures in place "including escalation protocols" to resolve discrepancies and decline or cease to do business with a customer when it cannot form a reasonable belief that it knows the true identity of the customer and/or beneficial owner of the funds. There is, however, no requirement that financial institutions understand the ownership or control structure of the customer or determine who are the natural persons that ultimately own, control or exercise ultimate effective control over the legal person or arrangement or control the customer. Financial institutions should require from customers a statement of ownership when it is clear the client is not the beneficial owner.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Article 15(2) of the AML Law allows for simplified CDD measures when a transaction is being executed by a non-account holder and the value of the transactions is (or a series of transactions are) less than IQD5m (approx. USD4,520).
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	N/A
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	There is no requirement to conduct enhanced due diligence measures in respect of PEPs or to designate those accounts as high risk.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	There are no laws, regulation or prudential requirements which require financial institutions to implement AML/CFT controls in regard to correspondent relationships, nor gather information about any respondent businesses to determine the reputation, quality of supervision or whether it has been subject to a money laundering or terrorist financing investigation or regulatory action. There are no requirements in law, regulation or other enforceable means requiring that financial institutions obtain a copy of any respondent institution's internal AML/CFT controls or assess them for effectiveness. There are no requirements in law, regulation or other enforceable means requiring internal management approval prior to the establishment of new correspondent relationships. Cross border transactions above IQD15m (approx. USD13,560) require the submission of a report to the Money Laundering Reporting Office and/or Iraq Customs Services. The report shall contain: - the legal capacity of the person filing the report; - the origin, destination and route of the currency; - the amount and type of monetary instruments; and - any other additional information.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	The Law is silent in this regard.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	N/A

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	SARs should be made to the Money Laundering Reporting Office at CBI: www.cbi.iq

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes. Article 20 of the AML Law provides that the CBI may require each financial institution to file a report with the MLRO of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through or to such financial institution which involves a transaction in currency or other monetary instrument of more than IQD15m (approx. USD13,560). Article 21 of the AML Law provides that the CBI is authorised to require all persons to submit a report of currency and monetary instruments with the Money Laundering Reporting Office when transporting currency or other monetary instruments greater than IQD15m (approx. USD13,560) from a place within Iraq to a place outside of Iraq or from a place outside Iraq to a place within Iraq. The report should contain the following information to the extent prescribed by the MLRO: a) the legal capacity in which the person filing the report is acting; b) the origin, destination, and route of the currency and/or monetary instrument; c) the amount and kind of monetary instruments and/or currency transported; and d) other additional information as required.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	The obligation to report suspicious transactions only applies to transactions above IQD4m (approx. USD3,610). Article 19 of the AML Law provides that where a financial institution has reason to know that a suspicious transaction has occurred, whether effected by a customer or other person, where the total value of the transaction or series of potentially related transactions is equal to or greater than IQD4m (approx. USD3,610) the financial institution must notify the MLRO. However, in the case of suspected structuring transactions for the purpose of circumventing reporting requirements, a financial institution should report such transactions irrespective of the amount.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	The CBI may impose the following if a financial institution violates the law: a) issue an order to cease the activity resulting in the violation; b) assess a monetary penalty; c) publish the results of any enforcement action; or d) issue an order to prohibit the violating party from being involved in the affairs of financial institution either permanently or temporary.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	The Law is silent in this regard.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	The Law is silent in this regard.

AML Audits

Q26.	Is there a legal requirement for a bank’s external auditor/other external organisation to report on the bank’s AML systems and controls?
A26.	No, but Article 8 of the AML Law states that the CBI is authorized to request from Banks’ auditors all information and documents needed for the performance of the CBI's duties.

Q27.	If an external report on the bank’s AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	No, but Article 22 of AML Law states that all financial institutions have to maintain all records related to AML for a period 5 years, and that this data has to be protected and well preserved.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Not to our knowledge.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Not to our knowledge.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Bank information secrecy is mentioned in the Iraqi Banks Law number 94 of year 2004 (Section 8 of the Law – articles 49, 50, 51 and 52).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Israel

Key contact: Eyal Ben-Avi
Email: eyal.ben-avi@il.pwc.com
Tel: +972 3 7954940

Postal address: 25 Hamered Street,
Tel Aviv 68125,
Israel

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2002.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) Banking: Bank of Israel (http://www.boi.org.il/en/Pages/Default.aspx); b) other financial services: a. Israel securities authority (http://www.isa.gov.il/); b. Ministry of finance (http://www.financeisrael.mof.gov.il/FinanceIsrael/Pages/En/Home.aspx); and c. Ministry of communication (http://www.moc.gov.il/130-en/MOC.aspx); and c) non-financial sector: a. Ministry of Economy: Dealers in precious stones (http://www.economy.gov.il/English/Pages/default.aspx); and b. Ministry of Justice: Lawyers and accountants (http://www.justice.gov.il/Units/FBPS/Obligations/Pages/default.aspx).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, by the Israel Money Laundering and Terror Financing Prohibition Authority "IMPA" (the Israeli Financial Intelligence Unit): http://index.justice.gov.il/En/Units/IMPA/AboutImpa/Pages/default.aspx With regard to lawyers and accountants, guidance is provided by the regulator: http://www.justice.gov.il/Units/FBPS/Obligations/Pages/default.aspx
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, Israel was evaluated in 2008 and 2013 by Moneyval. The report is available at: http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Israel_en.asp Also, see: http://www.coe.int/t/dghl/monitoring/moneyval/Publications/Archive_MONEYVAL_en.asp

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No. For occasional customers of money services businesses ("MSBs") CDD is not required under NIS25,000 (approx. USD6,500).

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: should obtain name, address, identification number, date of birth and gender. Passports and identity cards are suitable for verification purposes. Corporates: should obtain name, address, identification number, date of incorporation. For controlling shareholders the same information as for individuals should be obtained. Memorandum and Articles of Association and Certificates of Incorporation are suitable for verification purposes.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Document copies should be certified by an appropriate person, for example a notary, lawyer or accountant. In addition, verification in accordance with the Population Registry should be performed.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Financial institutions and obliged DNFBPs should require the applicants to declare whether they are acting for themselves or on behalf of another. If an applicant declares that he/she is acting on behalf of another, the declaration should include the particulars as set out in the guidance notes in respect of each of the beneficiaries. Financial institutions and obliged DNFBPs shall take reasonable measures, in reference to the risk of money laundering and financing of terrorism, to verify the identity of the beneficiaries and the controlling share owners by using relevant information or data received from a reliable source.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Reduced/simplified CDD apply in certain law-risk circumstances specified in the AML/CFT orders.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced CDD is required in high-risk situations as specified in the orders (e.g. high-risk countries, PEPs etc.)
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons (‘PEPs’)?
A14.	Foreign PEPs are automatically considered high risk clients and are subject to additional procedures.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The banking corporation should obtain the following: a) name; b) name of the country and supervisory authority; c) general information (address and telephone number of the corporation and names of persons to contact, according to the Banking Order); d) name and address of all shareholders above 20%; and e) last annual report and ‘request letter’ (letter requesting the opening of an account to be retained for at least seven years after the account closed). When the correspondent is not from the OECD, the bank should obtain a licence from the supervisory authority, the incorporation documents and letters of reference from banks in OECD member countries that manage accounts of the corporation wishing to open an account. In addition, Israeli banks should examine the efforts taken by the correspondent bank to defend against money laundering and terrorist financing.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Every non face-to-face transaction requires additional due diligence.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Reporting	
Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The IMPA: the Israeli FIU (http://index.justice.gov.il/En/Units/IMPA/AboutImpa/Pages/default.aspx).
Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014/2015: 48,116 SARs (Referred to as Unusual Activity Reports "UAR's" in Israel) Comparative GDP data is not available for this specific period.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Obligated entities are required to report unusual activity reports and currency transactions reports (of specified thresholds; e.g. cash transactions above NIS50,000 (approx. USD13,000)).
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	Generally, transactions under NIS50,000 (approx. USD13,000) do not need to be reported (with the exception of high-risk countries, which require a report from a sum of NIS 5,000 (approx. USD1,300)).
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, the regulators can sanction the supervised institutions. The maximum fine that supervised institutions can face is NIS2.26m (approx. USD580,000) for each violation.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No, although several institutions use automated suspicious transaction monitoring technology.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	The obligation is to report the transaction to the FIU, there is no requirement to obtain the authority to proceed (with the exemption of TF suspected transactions).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, Israel established Privacy Law (from 1981): a) yes, the definition includes financial data and other personal data; b) unknown; and c) there are two definitions: a. "Information" - Data on personality, personal status, intimate affairs, state of health, economic, professional qualifications, opinions and beliefs; and b. "Sensitive information" - Data on the personality, intimate affairs, state of health, economic, opinions and beliefs.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	a) credit reports are used for credit risk analysis. Banks are allowed to transfer credit related information to two authorized service providers, and search for such information for credit risk management, as applicable; b) criminal records are allowed to be transferred by the person himself; and c) medical data transfer is prohibited.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Unknown.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. See above. Additionally, bank's secrecy and confidentiality obligations are set under the Banking Law.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Jordan

Key contact: Fadi Fakhouri
Email: fadi.fakhouri@jo.pwc.com
Tel: +962 (6) 500 1300

Postal address: PricewaterhouseCoopers 'Jordan'
Third Circle, Jabal Amman, 14 Hazza' Al-Majali Street,
PO Box 5175, Amman 11183, Jordan

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Anti-Money Laundering and Counter Terrorist Financing Law ("AMLCTFL") came into force in 2007. The date the law became effective is different across the industry. For further information see: http://www.amlu.gov.jo/ar-jo/legislation/instructionsguidelinesforantimoneylaunderin.aspx
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) Central Bank of Jordan: http://www.cbj.gov.jo/; b) Jordan Securities Commission regulates financial services companies, custodians, mutual investment companies, mutual funds and has issued the Anti-Money Laundering Instructions In Securities Activities For The Year 2008: http://www.jsc.gov.jo/Public/English.aspx?Lang=3&Page_ID=1784; Jordan Insurance Commission regulates the insurance sector: http://www.captiveinternational.com/company/insurance-commission-of-jordan; Central Bank of Jordan supervises money exchange companies; Company Control Department of the Ministry of Industry and Trade control financial leasing companies save for those affiliated to banks which come within the purview of the Central Bank of Jordan; and c) while real estate companies and dealers in precious metals and stones are subject to the AMLCTFL and instructions have been issued, monitoring of compliance with implementation has to date required their accountants to verify the extent of adequacy of relevant policies and procedures and include information in the annual report. There are no casinos in Jordan.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes, please refer to the following link which provides guidance on AML requirements: http://www.amlu.gov.jo/ar-jo/legislation/instructionsguidelinesforantimoneylaunderin.aspx
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Guidance issued by the Central Bank approves the adoption of a risk based approach for customer due diligence.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	As a result of the Middle East and North Africa FATF Mutual Evaluation Report on Jordan published on 19 May 2009, Jordan was placed under the regular follow-up process. The report can be accessed here: http://www.menafatf.org/images/UploadFiles/MER_Hashemite_Kingdom_of_Jordan.pdf Most recently the Third Follow-Up Report for Jordan was published on 30 Apr 2013 and can be accessed here: http://www.menafatf.org/MER/JordanFUR3_E.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes, if the value of a transaction does not exceed JOD10,000 (approx. USD14,090) or the equivalent in foreign currency.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Banking Natural Persons: Identification data shall include the full name of the customer, nationality, permanent address, phone number, work address, type of activity, purpose of business relationship and its intended nature, names and nationalities of persons authorised to manage the account and any other information the bank deems necessary. With regard to legally unqualified persons, such as minors, documents of their legal representatives who manage such accounts shall be obtained and in case a person deals with the bank on behalf of the customer, a notarised power of attorney or a bank authorisation shall be obtained and kept in addition to verifying the identity of the proxy. Legal persons: Identification data shall include the name of the legal person, legal status, name of owners and their shares, the authorised signatories, domicile of the legal person, line of business, capital, registration date and number, tax number, national identity number of the organisation, names and nationalities of signatories authorised to run the account, phone numbers, purpose of the business relationship and its nature so the bank is aware of the ownership structure and the provisions governing the powers to take binding decisions for the legal person and any other information the bank deems necessary. The bank should obtain the required documents indicating an authorisation by the legal person to natural persons to run the account as well as identifying the authorised persons. Public shareholding companies are excluded for the request for names of owners and their shares; instead it is adequate to obtain a list of shareholders whose shares exceed 10% of the capital. Insurance Natural persons: Identification data shall include the full name of the customer, nationality, date and place of birth, national number for Jordanian nationals and the passport number for non-nationals, current permanent residential address, purpose of the business relationship and its nature and any other information the company considers necessary. Regarding persons without mental capacity, the company shall have the documents relating to them and to the persons who represent them legally, as the case may be. Legal persons: Identity data shall include the name of the legal person, legal status, location address, type of activity, capital, date and number of registration with the competent entities including tax number, phone numbers, purpose of the business relationship and its nature, names and addresses of owners and their shares, the authorised signatories, binding authority of the legal person or legal arrangement so that the company is aware of the ownership structure and the provisions governing the powers to take binding decisions for the legal person and any other information the company deems necessary. Companies should obtain the required documents indicating an authorisation by the legal person to the natural persons to represent it, the nature of their relation with the legal person, and identify their identity and their activities according to the procedures of identifying the identity and the activities of the customer. The company shall be sure that there is no legal bar that prevents transacting with them and obtain their signatures. For other industries please refer to the attached documents at the following link: http://www.amlu.gov.jo/ar-jo/legislation/instructionsguidelinesforantimoneylaunderin.aspx
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Banking: A bank shall preview the official identification documents of the customer and obtain a copy of the same documents signed by a competent employee declaring that it is an original copy and take the necessary procedures to verify the validity of the information and data obtained from the customer from reliable and neutral sources, including contacting the competent entities that issued such official documents, and refer to the database of the Civil Status which is available to the banks and the website of the Companies Control Department. In the case of legal persons, the existence, legal form, names of the owners and the authorised signatories of the legal person shall be verified by virtue of necessary documents and information contained therein, such as, memorandum and articles of association, and the certificates issued by the Ministry of Industry and Trade and certificates issued by the commercial and industrial chambers in addition to obtaining the required official certificate from the competent authority in case the company is registered abroad. Insurance: Verify the existence of the legal person and its legal form, as well as the names of owners and signatories of the legal person through the necessary documents and the information they include, such as memorandum of association, articles of association, and certificates issued by the Ministry of Industry and Trade, Chambers of Industry and Trade and Company Control Department, in addition to the necessity to obtain a registration certificate of the legal person at the competent authorities in case the company is registered outside of Jordan. The company shall view the official documents to identify the customer and their activities and have a copy of this documentation signed by the competent company employee or authorised person declaring that it is an original copy. The validity of the information should be verified using neutral and reliable sources, including contacting the competent entities that issued the official documents, and referring to the website of the Company Control Department.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Banking: Banks are required to request each customer to provide a written declaration in which he/she determines the identity of the beneficial owner of the intended transaction. Such declarations shall contain the identification data of the customer. The bank shall verify the identity of the beneficial owner by using data or information obtained from official documents to verify the identity of the beneficial owner. Where the beneficial owner is a legal person, reasonable procedures shall be taken to verify the ownership structure and the controlling management of the legal person by using data or information obtained from official documents to verify the identity of the beneficial owner. Insurance: Procedures for identifying the identity of the beneficial owner shall take into consideration the following: a) taking appropriate procedures for verifying the identity of the beneficial owner. This includes viewing data and information obtained from official documents and data until the company is satisfied that it knows who the beneficial owner is; b) requesting the customer to submit a written declaration to specify the identity of the beneficial owner. The declaration shall contain at least the identification data of the customers identity; and c) obtaining information about provisions regulating the business of the legal person including its ownership structure and the controlling management of it.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Banking: The Central Bank of Jordan has the right to determine the transactions or customers who may be subject to simplified customer due diligence procedures when identifying and verifying the identity of the customer and the beneficial owner. This should be limited by international standards, recommendations and best practices that determine customers or transactions of low risk and any international controls or local requirements in this respect. Simplified customer due diligence procedures are prohibited whenever there are suspicions of money laundering or terrorist financing transactions, or whenever high risk circumstances occur. Insurance: The company may simplify the procedures of identifying and verifying the customer, his activity and the beneficial owner in the following cases: a) dealing with financial institutions which are subject to certain procedures for anti-money laundering and counter terrorist financing similar to the procedures mentioned in these Instructions and the decisions issued by virtue thereof, including FATF recommendations, where implementation is subject to supervision; b) dealing with public shareholding companies that are subject to regulatory disclosure requirements; c) dealing with ministries and government departments and institutions; d) dealing with customers residing in another country if such country is sufficiently applying the international standards for anti-money laundering and counter terrorist financing, including the FATF recommendations; e) insurance policies for pension schemes if the policy cannot be used as collateral and there is no surrender clause; f) life insurance policies where the annual premium is no more than JOD1,000 (approx. USD1,410) or a single premium of no more than JOD2,000 (approx. USD2,820); and g) general insurance business where a single premium or total annual premiums do not exceed the amount of JOD3,000 (approx. USD4,230).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Banking: The company shall apply enhanced procedures for identifying the customer and his activity in the following cases: a) customers that are considered high risk, which includes Politically Exposed Persons ("PEPs"), non-resident customers, private banking customers and customers who are associated with countries that do not apply or insufficiently apply the FATF recommendations; b) correspondent banking relationships; c) non-face-to-face relationships; d) unusual transactions; e) requesting facilities against deposits; f) leasing safe deposit boxes; and g) depositing cash amounts or travellers cheques in an existing account by a person(s) that does not represent the owner of the account under a power of attorney or authorisation approved by the bank. Insurance: The company shall apply enhanced procedures for identifying the customer and his activity in the following cases: a) large insurance transactions and those which have no apparent economic or visible lawful purpose; the company shall put the necessary procedures to examine the background and surrounding circumstances of such transactions and their purpose, and shall keep the results of such examination in its records; b) insurance transactions with persons residing in or coming from countries which do not have appropriate anti-money laundering and counter terrorist financing systems or which do not apply or insufficiently apply the international standards related to anti-money laundering and counter terrorist financing, including the FATF recommendations; c) any transaction that the company believes by its own estimation forms a high level of money laundering and terrorist financing risk; and d) dealing with PEPs.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Banking: In the case of PEPs the following enhanced due diligence should be performed: a) the approval of the bank's general manager, regional manager, or the person authorised thereby shall be obtained when commencing a relationship with these customers. Such approval shall also be obtained when a customer or a beneficial owner is discovered to be a PEP; b) the bank shall take all necessary procedures to verify the source of the wealth of customers and beneficial owners; and c) the bank shall accurately and continuously monitor the transactions with such customers and give special attention to business relationships and transactions that occur with any of them. Insurance: In the case of PEPs the following enhanced due diligence should be performed: a) the approval of the company general manager, authorised manger, or the person authorised thereby shall be obtained when commencing a relation with these customers. Such approval shall also be obtained when a customer or a beneficial owner is discovered to be a PEP; b) take sufficient procedures to identify the source of wealth of customers and beneficial owners who fall under such categories; and c) conduct enhanced ongoing monitoring on the company's dealings with politically exposed persons.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	When establishing correspondent banking relationships the correspondent bank shall: a) verify the nature of the external bank's business activity and reputation thereof in the field of anti-money laundering and counter terrorist financing transactions; b) obtain the approval of the bank's general manager or regional manager before the commencement of the relationship; c) ensure that the external bank is subject to effective supervision by a supervisory authority in the bank's home country; d) anti-money laundering and counter terrorist financing systems shall be verified by the bank and applied by the respondent bank; and e) ensure that the respondent bank has exerted due diligence regarding its customers who have authority to use (payable-through accounts) and that the respondent bank is able to provide information related to such customers and transactions made to such accounts when needed.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	The bank shall apply the necessary policies and procedures to avoid risks related to non face-to-face dealings with customers, taking into consideration the instructions of the Central Bank.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The Anti-Money Laundering & Counter Terrorist Financing Unit: http://www.amlu.gov.jo/ar-jo/forms.aspx

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2012 – 168 SARs (by entities obliged to report) and 17 notifications (SARs) received from supervisory authorities GDP (in current prices): 2012 – USD30,937.3m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD184.2m of GDP.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes. Article 15 of the Anti-Money Laundering and Countering Terrorist Financing Law 2007 prohibits tipping off.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes. They should be reported to the Anti-Money Laundering and Counter Terrorist Financing Unit which will recommend whether to proceed or not.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	The law is not explicit in this regard.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	a) annually; b) the Anti-Money Laundering and Terrorist Financing Unit in Jordan; and c) yes.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	a) yes; b) yes; and c) yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Jordan has no Data Protection Laws, however the Jordanian Constitution specifically recognises a limited right to privacy but these rights must be circumscribed by laws to be claimable. Furthermore, there are a number of laws which already provide some level of privacy protection such as the Law of Securing Information Obtaining Rights.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	See A29.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	See A29.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	See A29.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Kuwait

Key contact: Khalid AlShatti
Email: khalid.alshatti@kwt.pwc.com
Tel: +965 2227 5701

Postal address: Arraya Tower II, 23rd - 24th Floor,
Al-Shuhada St. P. O. Box 1753, Safat
Sharq, 13018. Kuwait

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Law #106/2013 came into effect in May 2013, replacing law #35/2002.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	Prior to law #106/2013, law #35/2002 was in effect, which did not cover international treaties in relation to terrorist financing. The update to the law reflects the recent developments in AML across the world.
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) law #24/2012 relates to the establishment of Anti-Corruption Authority that looks after all the AML related activities for Kuwait as a whole. In addition, the Central Bank of Kuwait plays a role in monitoring the financial sector (http://www.cbk.gov.kw/) alongside the Capital Markets Authority (http://www.kuwaitcma.org/); b) as above; and c) commercial goods are monitored by CBK and Ministry of Commerce and Industry (http://www.moci.gov.kw/). As part of law #106/2013, an investigation unit was established under ministerial order #1532/2013 to undertake the role of taking in any reported suspicious activities.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	None other than what is covered in the law and regulations above.
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, all financial institutions are required to update their records by requesting all their customers provide new KYC information.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes, the IMF did a report on Kuwait in 2011, which resulted in the issuance of the mentioned laws above. A full report is not available, however extracts that were reported in the local media can be obtained.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	For banking transactions (i.e. a cash deposit or transfer), no thresholds are in place. In the event of purchasing jewellery, it is required that photo identification is presented in addition to the source of funds.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Identification documentation and source of funds.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	None.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	None.

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	With respect to foreigners (i.e. those whose identification and documents are not issued locally), attestation from the Kuwaiti embassy in that particular country and the ministry of foreign affairs is usually required.

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	As stated above in A12.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Always.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	As stated in A12.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	No.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	As stated in A12.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	As stated in A3.

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, all of the above are considered.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, it is covered under the relevant laws.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	Yes.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	Yes, it is performed annually and is reported to the Central Bank of Kuwait. It does not form part of the financial statement audit.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	Sample testing of all the above is required. The report itself is referred to as the Internal Controls Review ("ICR").

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes: a) yes; b) the same as for individuals; and c) there is no separate definition of sensitive data.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes, information can only be shared with the Central Bank of Kuwait. It cannot be shared with any other party.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	Yes, banking law #32/1968.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation?) If so, what data is subject to regulation?
A32.	Yes, under banking law #32/1968, all customer data is considered confidential.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Lebanon

Key contact: Camille C. Sifri
Email: camille.sifri@lb.pwc.com
Tel: +961 (5) 428600

Postal address: Saba House bldg, Block B & C,
Said Freiha Street,
Hazmieh, Lebanon

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Law 318 Fighting Money Laundering became effective in 2001 and was amended twice; firstly in 2003 to criminalise terrorist financing and then recently in 2015 to include tax evasion.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	a) banks and financial institutions are regulated by the Central Bank of Lebanon ("BDL") (www.bdl.gov.lb). However In 2001, the Special Investigation Commission ("SIC") was established <i>inter alia</i> to monitor compliance with the rules and procedures stipulated by Law 318. The Head of SIC is the Governor of the Central Bank of Lebanon (www.sic.gov.lb); b) as above; and c) there is no defined regulator for the non-financial sector. Banks are required to monitor these clients closely and identify any potential suspicious transactions.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Money Laundering is of the utmost importance for the Central Bank of Lebanon. Accordingly, periodical updates are performed on all the circulars related to money laundering (http://www.bdl.gov.lb/circulars/index/5/33/0/Basic-Circulars.html). In addition, the SIC performs missions every 18 months to check that Banks are following its directives and abide by the regulator requirements. For SIC directives issued to the financial sector, refer to: http://www.sic.gov.lb
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	Yes, as required by Article 6 of Basic Circular no.83.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes. Article 9 of Basic Circular no.83 requires the adoption of a risk based approach.

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No evaluation has been performed in the last 3 years. The last evaluation dates back to 2009: http://www.menafatf.org/topiclist.asp?ctype=reg&id=470

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No. Due diligence is required for cash/cheque transactions below USD10,000 or equivalent in a foreign currency. However, it should be noted that any new client opening an account in any bank is required to submit a detailed KYC form.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: a copy of a passport, identity card, individual civil registration or residence permit and KYC form showing residential/work addresses, profession and average monthly income. Legal entities: Articles of incorporation, certificate of registration at the Chamber of Commerce, ownership structure, a list showing the stocks or shares, a list of the authorised signatories, in addition to a copy of the identify of its legal representative and the directors and persons who hold, whether directly or indirectly a percentage of shares enabling them to have effective control of the company. Banks are required to obtain legal documents pertaining to the ultimate beneficiary. In the case of an authorised agent, the power of attorney or a certified copy of the power of attorney in addition to documents regarding the identity of the agent (i.e. a copy of a passport, identity card, individual civil registration or residence permit).

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Clients are requested to provide original copies prior the opening of any new accounts with the Bank/Financial Institution. Copies of these documents are then taken by the Banks/Financial Institution for archiving and in some cases copies are certified by Public Notaries to assert validity of the copies to be archived.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The customer should fill out a form detailing the identity of beneficial owners by providing the individual(s) name, family name, residential address, profession and information about his/her financial situation.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	As stipulated by BDL basic circular no.83, several cases might be limited to simplified due diligence, of which: a) as long as transactions are below USD10,000 and the frequency of transactions is in line with the client's profile then no additional due diligence procedures are performed; and b) exempted clients i.e. clients with a high volume of cash transactions in line with their volume of business and type of business.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Enhanced due diligence measures are required if customers are classified as high risk as per the Central Bank's guidelines. Article 9 of Basic Circular no.83 identifies the following customer risk factors but falls short of classifying these as high risk: a) customers whose occupation relies mainly on cash (money exchange, gold and precious stones dealers, restaurants and night clubs, real estate agents and car dealers); b) foreign PEPs, their family members and close associates; c) offshore companies; d) companies established in countries known to be tax havens; e) non face-to-face customers; f) customers dealing only through intermediaries; g) customers dealing through fiduciary contracts or trusts; h) companies with a capital totally or partly constituted of bearer shares; and i) customers who are nationals or resident in countries that do not or insufficiently apply the FATF recommendations.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Article 9 of Basic Circular no.83 requires the establishment of an adequate system in order to determine whether a foreign customer is a PEP and the adoption of risk based controls to include: a) obtaining more detailed information about customers, notably the source of their wealth; b) obtaining, according to risk levels, the necessary administrative approvals, in order to deal or continue to deal with customers and to execute operations; c) periodically review the relationship; and d) continuous peer comparisons.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	Article 2 of Basic Circular no. 83 provides that when establishing a relationship with a foreign correspondent bank, the bank must ascertain the following: a) the respondent bank is not a shell bank and that it actually exists based on submitted documentary evidence; b) it does not deal with shell banks; c) it has a good reputation and is subject to effective controls; d) it implements sufficient and effective procedures to fight money laundering and terrorist financing; e) the nature of the respondent bank's business; f) the approval of senior executive management must be obtained; and g) determine the responsibility of both parties particularly for payable through accounts and make sure that the respondent is capable of providing relevant customer identification data if requested.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	a) transactions in writing - the Bank should verify the client's identity and the authenticity of the signature; and b) transactions done via an agent - the Bank should obtain an official procuration and the identity cards of the agent and the client.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The Bank should report suspicious activities to the Governor of the Central Bank in his capacity as chairman of the SIC and to the Special Investigation Committee (SIC): http://www.sic.gov.lb

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No, unless it is specifically requested by the Central Bank of Lebanon.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No. All suspicious transactions, regardless of materiality, need to be reported.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Any person who does not comply with the reporting requirements could be imprisoned and subject to a fine as stipulated by Law no. 318.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	As stipulated by Basic Circular no. 83, banks are required to use specialised software to monitor accounts and transactions for any of the mentioned risk indicators.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Banks should inform the SIC of suspicious transactions and are permitted to process the transactions unless objected to by the SIC. In addition, Banks are not allowed to close suspicious clients' accounts before consulting with the SIC. It should be noted that in case the client account was frozen at the request of the SIC, banks are not allowed to process any transaction for the client.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	The law is silent in that regard.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	As stipulated by the Central Bank of Lebanon Basic Circular no. 83, external auditors are required to assess the Bank's AML function and issue a "gap analysis" report in that regard.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	External auditors are required to report on yearly basis. The report should be addressed to the following parties: The Governor of the Central Bank, the SIC and the Management of the Bank.

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	The external auditor is required to check the Bank's compliance with the requirements of Basic Circular no. 83, of which: a) Section I: Relations with foreign correspondent banks abroad; b) Section II: Relations with customers and due diligence measures; c) Section III: Controlling certain operations and customers; and d) Section IV: Committees and administrative units in charge of the control of operations for fighting money laundering and terrorist financing, and their tasks. Accordingly, we are required to check a sample of KYC files related to new clients operating with the Bank, the Bank's monitoring of its correspondent banks and the Bank's monitoring framework set at the branches level, etc.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	Yes, in Lebanon we operate under the Banking Secrecy Law. Accordingly any information pertaining to any depositor cannot be revealed to any party except the SIC, or if the client is subject to a court case. As for clients who have facilities with banks, their information can be shared between banks and this is done to help banks better assess the credit risk of facilities provided or to be provided.
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Please refer to A28.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	Yes. The Banking Secrecy Law was promulgated on 03 Sept 1956. Article 2 provides that managers and employees of banking establishments are bound to absolute secrecy in favour of the bank's clients and may not disclose to anyone, whether a private individual or an administrative, military or judicial authority, the names of clients, their assets and facts concerning them. Banks are authorised to open code number deposit accounts for their clients. The following exceptions apply: Banking secrecy terminates in the case of bankruptcy or in the case of debtor accounts, SIC is exempt so as to provide for the lifting of confidentiality in favour of competent judicial authorities where it has reason to suspect suspicious activity and additionally, records are required to be kept by financial institutions of cash transactions that exceed USD10,000 which are not subject to the Bank Secrecy Law.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Oman

Key contact: Pushpa Malani
Email: pushpa.malani@om.pwc.com
Tel: +968 24559142

Postal address: Hatat House,
Suites 205-210,
Wadi Adai, Muscat, Oman

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The first AML law in Oman, the Law of Money Laundering, was issued through Royal Decree No. 34/2002 and published in the Official Gazette No. 716 dated 01 April 2002. The law was notified by the Central Bank of Oman ("CBO") circular BM 936 dated 07 April 2002. Executive regulations for the law were issued in 2004 through Royal Decree No.72/2004. Royal Decree 79/2010 issued on 28 June 2010 promulgated the Law of Combating Money Laundering and Terrorism Financing. The Executive Regulations of the previous law is still effective until the time the Executive Regulation under the new law will be issued.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The Financial Intelligence Unit ("FIU"), an independent unit under Royal Oman Police, is the regulator for AML controls for all financial and non-financial sectors (http://www.fiu.gov.om/).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Practical guidance in the form of the Manual of Suspicious Transaction Reports is available on the website of the FIU - Royal Oman Police ("FIU-ROP") (http://www.fiu.gov.om/files/English.pdf).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	The executive regulations describe transactions that may pose a potential threat for money laundering. These follow a risk based approach by focusing on customers and transactions that pose a larger money laundering threat to financial institutions.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The most recent FATF evaluation was conducted in 2011. See: http://www.fatf-gafi.org/countries/n-r/oman/documents/mutualevaluationofthesultanateofoman.html

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	The regulations do not define any such threshold. However, each company/bank, as a matter of policy, has defined its own threshold.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Individuals: For Omani natural persons: a) full name; b) current address; and c) copy of passport or ID or driving license. For non-Omani natural persons: a) full name; b) current address; c) copy of passport; and d) copy of residence permit or labour card for residences. Juristic persons: a) copy of a valid commercial registration; b) specimen signature form of the authorized signatories; c) copies of identification of authorised signatories; d) memorandum and Articles of Association; and a) other identification documents as deemed necessary.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	There is no compulsory requirement with regard to independent verification.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The high level requirements for beneficial ownership are similar to those required for any customer.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Politically Exposed Persons ("PEPs"), NRI and privileged customers are high risk clients and exposed to higher due diligence when compared to normal individuals. Each customer is subject to similar customer due diligence requirements.

Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	High risk customers and suspicious transactions require enhanced due diligence.

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Additional due diligence is always required. PEPs also require approval from senior management.

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	An AML questionnaire developed by each bank is sent to the correspondent bank before entering into a relationship. Licenses are requested and efforts are made to ensure they are not shell companies.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Non face-to-face transactions are avoided in most cases. Enhanced due diligence is always required for such relationships.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	SARs are reported directly to FIU-ROP (http://www.fiu.gov.om/). Also, Article 4 of the Executive Regulations requires that institutions appoint a competence officer who should be responsible for reporting any suspicious activities after he receives them from any individual in the institution. The officer shall then review the suspected documents to ascertain whether the suspicions raised are justified. He shall then make sure that the report is received by the competent authority, the Central Bank and the supervisory competent authority.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2013 – 254 SARs (Source: FIU-ROP) GDP (in current prices): 2013 – USD78,183m (Source: data.worldbank.org[*]) This results in a ratio of 1 SAR for every USD307.8m of GDP.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No, however FIU-ROP can investigate any transaction based on its discretion.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.
Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Article 4 of Anti-Money Laundering and Combating the Financing of Terrorism states that a person shall be guilty of a crime related to money laundering if they do not report or disclose any information or suspicion related to money laundering. The penalty is set out under Article 28, which consists of imprisonment for a term not longer than 3 years and/or a fine not greater than OMR3,000 (approx. USD7,800).
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Article 5, paragraph d of the AML regulations require companies to use AML software to monitor all electronic banking transactions, including a set of minimum requirements.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	No, however, if the competent authority investigates a report from a compliance officer and finds evidence of money laundering or attempted money laundering, then the competent authority shall submit a written application to the Public Prosecution to consider stopping the transaction in accordance with Article 12 of the Law. This measure is regulated under Article 6 of the AML Executive Regulations.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No.

^{*} GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	No.
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	AML is not part of a financial statement audit. Banks are not required to get their AML systems and controls reviewed independently. Accordingly, no such reports are available.
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	There are no external reports available on AML systems and controls.

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	There is an Electronic Transactions Law issued under Royal Decree No. (69/2008). There is no clear definition of "personal" or "sensitive" data. The law generally regulates electronic transactions between parties. Article 45 of the Electronic Transactions Law sets out a general guideline on the protection of personal data. Additionally, Article 70 of banking law issued by CBO discusses certain aspects of confidentially required by banks in respect of the information gathered during KYC (http://www.cbo-oman.org/).
Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	The information cannot be shared without prior approval of CBO.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	The Banking Law of Oman. The law does not allow any customer related information to be shared with anyone without prior approval of CBO (http://www.cbo-oman.org/).



'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Qatar

Key contact: James Tebbs
Email: james.tebbs@qa.pwc.com
Tel: +974 4419 2715

Postal address: 41st Floor Tornado Tower,
West Bay, Doha, State of Qatar,
P.O. Box 6689

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	The Combating Money Laundering and Terrorism Financing Law No (4) of Year 2010 was made effective in 2010. Additionally, the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Markets Authority were also made effective in 2010. The Anti-Money Laundering and Combating Terrorist Financing Rules 2010 were issued by the Qatar Financial Centre Regulatory in 2010 and were last amended in 2015. The Anti-Money Laundering and Combating Terrorist Financing (General Insurance) Rules 2012 were issued by the Qatar Financial Centre Regulatory in 2012 and were last amended in 2015.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The Qatar Financial Centre Regulatory Authority (www.qfcra.com), Qatar Financial Markets Authority (www.qfma.org.qa) and The Qatar Central Bank (www.qcb.gov.qa) are the financial services regulators in Qatar.
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Yes. The Combating Money Laundering and Terrorism Financing Law No (4) of Year 2010 provides guidance on the relevant rules to firms in Qatar: http://www.qfcra.com/en-us/legislation/Laws/Anti-Money%20Laundering%20Law%20No.%20(4)%20of%202010.pdf Additionally, the Qatar Financial Centre Regulatory Authority has issued the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 giving practical AML/CFT guidance to firms within its jurisdiction: http://www.complinet.com/net_file_store/new_rulebooks/q/f/QFCRA_6883_VER6.pdf Furthermore, the Qatar Financial Centre Regulatory Authority has also issued the Anti-Money Laundering and Combating Terrorist Financing (General Insurance) Rules 2012 (AMLG): http://www.complinet.com/net_file_store/new_rulebooks/q/f/QFCRA_8999_VER2.pdf Firms regulated by the Qatar Financial Markets Authority are subject to the Anti-Money Laundering and Combating Terrorist Financing Rules 2010: http://www.qfma.org.qa/EnglishPdf/rul1.pdf

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	Yes: http://www.menafatf.org/images/uploadfiles/4th_fyr_of_qatar_removal.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No.
Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Article 24 of the Combating Money Laundering and Terrorism Financing Law No (4) of Year 2010 states the following: "For the purposes of implementation of the requirements provided for in the preceding article, identification of natural persons and verification of their identity shall include the full name, as well as national identification number for Qatari citizens and residents and the passport number for expatriates. Identification of legal persons shall include obtaining and verifying information concerning the corporate name, registered office business address, proof of incorporation or similar evidence of their legal status, legal form, the names of executives, and articles of association, as well as verifying that the person purporting to act on behalf of the customer is so authorised, and to identify and verify the identity of that person. Identification of legal arrangements that are express trusts shall include identifying and verifying the identities of the trustees, the settlers, and major beneficiaries." Further detailed requirements can be found in Division 4.6C of the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Centre Regulatory Authority and Division 4.4C of the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Markets Regulatory Authority.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	There are no explicitly stated requirements for independent verification.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Guidance on the requirements for identification and verification of beneficial ownership are included within the following: a) Articles 22, 23, 26, 31 and 34 of the Combating Money Laundering and Terrorism Financing Law No (4) of Year 2010; b) Article 4.1.2 of Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Centre Regulatory Authority; and c) Article 4.1.2 of the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Markets Regulatory Authority.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Detailed guidance on reduced and simplified CDD is contained within the relevant regulations as follows: a) Article 31 of the Combating Money Laundering and Terrorism Financing Law No (4) of Year 2010; b) Section 4.5 of the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Centre Regulatory Authority; and c) Section 4.6 of the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Markets Regulatory Authority.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	Details on enhanced CDD is contained within the relevant regulations as follows: a) Section 4.4 of the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Centre Regulatory Authority; b) Section 4.5 of the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Markets Regulatory Authority; and c) Section 4.3 of the Anti-Money Laundering and Combating Terrorist Financing (General Insurance) Rules 2012 (AMLG).
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	The following sections of the legislation and rules provide guidance on PEPs: a) Article 26 of the Combating Money Laundering and Terrorism Financing Law No (4) of Year 2010; b) Article 3.2.5 of the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Centre Regulatory Authority; and c) Article 3.2.5 of the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Markets Regulatory Authority.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The due diligence requirements for correspondent banks can be found in the following: a) Article 27 of the Combating Money Laundering and Terrorism Financing Law No (4) of Year 2010; and b) Article 3.3.5 of the Anti-Money Laundering and Combating Terrorist Financing Rules 2010.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes. This is stated in Article 3 of the Combating Money Laundering and Terrorism Financing Law No (4) of Year 2010. Article 3.3.6 of Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Centre Regulatory Authority also states that relationships with shells bank are prohibited. Additionally, Article 3.3.6 of the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Markets Regulatory Authority also states the same.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	There is no explicitly stated requirement for additional due diligence for non-face-to-face relationships.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	Qatar Financial Information Unit: www.qfiu.gov.qa

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Volume of SARs: 2014 – 516 SARs (Source: QFIU Annual Report 2014: http://www.qfiu.gov.qa/files/QFIU_Annual_ENG_2014.pdf) GDP (in current prices): 2014 - USD210,109m (Source: data.worldbank.org*) This results in a ratio of 1 SAR for every USD407.18m of GDP.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No.

* GDP at purchaser's prices is the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. It is calculated without making deductions for depreciation of fabricated assets or for depletion and degradation of natural resources. Data are in current U.S. dollars. Dollar figures for GDP are converted from domestic currencies using single year official exchange rates. For a few countries where the official exchange rate does not reflect the rate effectively applied to actual foreign exchange transactions, an alternative conversion factor is used.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	In the event of non-compliance with the reporting requirements, Article 44 of the Combating Money Laundering and Terrorism Financing Law No (4) of Year 2010 shall apply: "A supervisory authority, in case of a violation of the obligations established under this law by a financial institution, NPO, or DNFBP, made intentionally or by gross negligence, is evidenced, may impose one or more of the following measures and sanctions: a) ordering regular reports on the measures it is taking; b) ordering compliance with specific instructions; c) sending written warnings; d) replacing or restricting the powers of managers, board members, or controlling owners, including the appointing of ad hoc administrator; e) barring individuals from employment within a business, profession or activity , either permanently or for a provisional period; f) imposing supervision, suspending license, restricting or withdrawing any other form of permission and prohibiting the continuation of a business, profession or activity; g) imposing financial penalty in an amount no greater than IRR10m (approx. USD332); or h) any other measures. The supervisory authority shall inform the Unit of the measures and sanctions imposed."
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	No.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	The Financial Information Unit Guide to Money Laundering and Terrorist Financing Suspicious Transaction Reporting (http://www.qfcra.com/en-us/legislation/Guides/FIU%20STR%20Guide.pdf) states the following under the section entitled Impact on Reported Transactions: "The law does not stipulate any provisions requiring Reporting Entities who have filed an STR to end or terminate their financial relationships with the reported entity or person. Reporting Entities should be aware that the decision to continue the business relationship after filing a STR should be based on commercial or risk containment reasons. However, a decision to terminate the business relationship must also ensure that the customer is not alerted to the filing of the STR which would constitute the offence of tipping off under Article (39) AML/CFT Law. It is recommended that in circumstances where Reporting Entities decide to terminate a business relationship, the Reporting Entity liaise directly with the FIU to ensure the termination does not tip off the entity or person or prejudice an investigation in any way. However, it is preferable that the Reporting Entity acts in coordination with the FIU, upon deciding to terminate its relationship with the suspected entity or person." Article 5.1.9 of Anti-Money Laundering and Combating Terrorist Financing (General Insurance) Rules 2012 (AMLG) issued by the Qatar Financial Centre Regulatory Authority Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Centre Regulatory Authority and the Anti-Money Laundering and Combating Terrorist Financing Rules 2010 issued by the Qatar Financial Markets Regulatory Authority rules all state that regulated entities can terminate relationships with customers for which they have issued SARs, however, regulated entities must ensure that restricting or terminating the business relationship does not inadvertently result in tipping off the customer.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	The laws and regulations do not expressly state that transactions should be monitored outside Qatar for regulated entities.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	There is no specific requirement for external auditors or other external organisations to report on the bank's AML systems and controls.
Q27.	If an external report on the bank's AML systems and controls is required: - how frequently must the report be provided? - to whom should the report be submitted? - is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: - sample testing of KYC files? - sample testing of SAR reports? - examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: - does the definition of "personal data" cover material likely to be held for KYC purposes? - how do the laws apply to corporate data? - does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	There are a number of laws which contain provisions relating to data privacy in Qatar such as the Constitution of Qatar (http://portal.www.gov.qa/wps/wcm/connect/5a5512804665e3afa54fb5fd2b4ab27a/Constitution+of+Qatar+EN.pdf?MOD=AJPERES), Law Number 13 of 2012 (the Qatar Central Bank Law) and the Qatar Financial Centre Data Protection Regulations 2005 (http://www.complinet.com/net_file_store/new_rulebooks/q/f/QFCRA_1559_VER1.pdf): - yes; - corporate data is regarded as confidential information and it is generally prohibited for this information to be shared except without the consent of the customer. Article 25 (G) of the Qatar Financial Centre Data Protection Regulations 2005 states that the data protection regulations cover "references to a person includes any natural or legal person, Body Corporate, or body unincorporated, including a branch, company, partnership, unincorporated association, government or state". Additionally, we understand from publications by lawyers based in Qatar that Law Number 13 of 2012 (the Qatar Central Bank Law) contains provisions stating that corporate data is confidential. The aforementioned law has not been published in the English language yet; and - Article 26 of the Qatar Financial Centre Data Protection Regulations 2005 define sensitive data as "Personal Data revealing or relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and health or sex life." Furthermore, Article 37 of the Qatari Constitution states that "the sanctity of human privacy shall be inviolable, and therefore interference into privacy of a person, family affairs, home of residence, correspondence, or any other act of interference that may demean or defame a person may not be allowed".

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	We understand that there are restrictions on the transfer of the above mentioned information. Article 7 (1) of the Qatar Financial Centre Data Protection Regulations 2005 states that "a Data Controller may only Process Personal Data if: (1) the Data Subject has unambiguously given his consent." The definition in Article 26 of processing data in the aforementioned regulations is "any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Additionally, our understanding of Law Number 13 of 2012 (the Qatar Central Bank Law), based on the publications issued by lawyers reviewing the Arabic text of the Law, is that customer data cannot be transferred, except with the consent of the customer. Article 37 of the Qatari Constitution (quoted above) indicates that it is imperative that the confidentiality of private information is maintained.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	We understand that the following will apply to information transferred within Qatar: a) The Constitution of Qatar; b) Law Number 13 of 2012 (the Qatar Central Bank Law); and c) Qatar Financial Centre Data Protection Regulations 2005.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	We understand that Law Number 13 of 2012 (the Qatar Central Bank Law) states that it is not permissible to disclose customer information to third parties, without the prior consent of the customers. Customer information includes personal data provided by the customer for KYC purposes and the information on the value of the customer's assets.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information



Saudi Arabia

Key contact: Tareq Haddad
Email: tareq.haddad@sa.pwc.com
Tel: +966 560911113

Postal address: Kingdom Tower
21st Floor
Riyadh, Saudi Arabia

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	Saudi Arabia passed the Anti-Money Laundering Law and Supplementary Guidance, under Royal Decree referenced M/39 dated 25/6/1424H corresponding to (24 Aug 2003) ratifying the Council of Ministers Decision #167 dated 20/6/1424H (corresponding to 19 Aug 2003). This Law provides a statutory basis for criminalising money laundering and terrorist financing activities.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non-financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	Saudi Arabia Monetary Agency (SAMA): For all commercial banks, money exchangers, branches of foreign banks operating in the Kingdom of Saudi Arabia, insurance companies and financing companies (http://www.sama.gov.sa/en-us/pages/default.aspx). Capital Market Authority (CMA): For Capital Banks (Investment Banks) and listed company excluding commercial banks and entities mentioned above (http://www.cma.org.sa/en/Pages/home.aspx).
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Saudi Arabia Monetary Agency (SAMA); a) for all banks, money exchangers and branches of foreign banks operating in the Kingdom of Saudi Arabia: http://www.sama.gov.sa/en-US/Laws/BankingRules/B%20and%20E%20AML%20CTF%20Rules%20Final%203rd%20Update.pdf; b) for financing companies: http://www.sama.gov.sa/en-US/Laws/BankingRules/Anti-Money_Laundering_and_Counter-Terrorism_Financing_Rules_For_Financing_Companies.pdf; and c) for insurance companies: http://www.sama.gov.sa/en-US/Laws/InsuranceRulesAndRegulations/IIR_4600_AML_Regulations_Updated.pdf. Capital Market Authority (CMA): For capital banks (Investment Banks) and listed company excluding the entities mentioned above: http://www.cma.org.sa/En/Documents/AML%20%20amended%20Final.pdf
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	The AML Law was ratified in 2003. It requires subject entities to update their customers' profiles at least once every five years.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	Yes, related guidance is provided in the AML law and supplementary guidance.

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	No, the latest FATF review was conducted in 2010: http://www.sama.gov.sa/en-US/AntiMoney/AntiDocuments/Report%20the%20FATF's%20final%20Kingdom%20John%2025,%202010.pdf

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	No.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	Saudi Nationals: Originals of either Personal Status Card; National Identity Card; Family Registration Book; Certified Family Record; Diplomatic passport; Special Passport; Hafithat Nofos; Certified Civil Record for Women; Certificate of Birth Expatriate legally residing in the Kingdom - Residence Book (Iqama); Five Year Resident Book; GCC Passport or Diplomatic Card Entities / Juristic persons: Copies of Commercial registration; entity's license; Articles of Association and appendices ID of the owner of the licensed business; List of the owners of the business entity; List of persons authorized by the owner to operate the accounts.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Individual: the original identification card (ID) has to be viewed by the bank's employee. A copy is taken and sealed with the bank's seal signifying its verification against the original. The purpose of obtaining a copy of the original ID should be documented and the customer must sign on the photocopy certifying its authenticity against the original. Legal entities: commercial register and/ or license and copy of the ID cards of the owners of the company whose names are included in the Articles of Association and its amendments. The customer must sign on the photocopy certifying its authenticity against the original.

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	Legal entities should verify the beneficiaries owner of all accounts and relationships and should conduct due diligence on all final beneficial owners. Legal persons should establish the identity of all shareholders or beneficial owner who own 5% and more of the company's shares.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	Simplified due diligence procedures are allowed for customers that are not considered high risk.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	For high risk accounts, including self-employed individuals, high net worth individuals, private banking accounts, insurance companies account, and PEPs. Subject entities are also required to apply enhanced due diligence procedures if they become aware that another subject entity has refused to deal with a particular customer on AML/ CTF grounds.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	No specific guidance is provided however all PEPs are to be considered high risk and subject to enhanced due diligence measures. Opening an account for a PEP requires an approval of a general manager, managing director, or CEO.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	a) banks should not open a correspondent account for or deal with a shell bank; b) correspondent bank accounts shall not be opened before the approval of the compliance officer in addition to that of the chief executive officer/director; c) banks should immediately inform SAMA of opening correspondent bank account in Saudi Riyal; d) third parties are prohibited from operating correspondent bank accounts; e) local cash deposits should not be allowed. This arrangement, known as "Payable-Through Accounts" should not be accepted; f) the correspondent bank should not be under sanctions by the UN or Saudi Arabia; g) banks should also determine from any available information (e.g., the internet) whether the correspondent bank has been subject to any money laundering, terrorist financing investigations or regulatory action; h) banks should obtain certification of AML/CTF compliance for all correspondent relationships, which should include the following information: a. the location, major business activities, and management; b. that they are under jurisdiction of their central bank or a similar monetary authority and are committed to the FATF recommendations; c. that they are governed by and committed to AML/CTF and KYC policies and procedures; d. that they have procedures in place for reporting suspicious transactions; e. that they are not dealing with any shell bank; f. any other pertinent information that can reassure the bank that sufficient focus is being directed to combating money laundering and terrorist financing; and g. the certification should be either renewed or confirmed by the correspondent bank every three years; and i) banks and money exchangers should apply satisfactory due diligence on a continuous basis regarding the banking correspondence relationships, document the responsibilities of AML/CTF, which are the correspondent and receiving banks responsibilities and apply due diligence regarding all banking correspondence relationships, including correspondence relationships that already exist.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q17.	In what circumstances is additional due diligence required for non-face-to-face transactions and/or relationships?
A17.	It is forbidden to open accounts or establish relationships for other than face-to-face customers. All account holders are subject to interview and identity verification.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	To the Saudi Financial Intelligence Unit – Ministry of Interior: https://www.moi.gov.sa/wps/portal/Home/sectors/safiu/contents!/ut/p/z1/tZLPT8lwHMX_FS4eSb9bu607VoLrhIDTDFkvpPsB1rAyWAX9790WPXhgSKK9Nf28I76XhwRaIqHIUW2kUTstt809Ee4KQkK4RexJ4MS3wKJosvDtsQWWH547wl-CEectYDEXWOjZcwgdKwhtJH6jHwWME28KQKeBAyHj8aMfYQwM9-rHLoggUSmTWVeULJWWupMye1A6WNRm68cN3D24VBUu4NRejOo3-gqyEyRD8xB6lpmLVC37IWmcpRgnFNcUCA5SVNsgyS-u3bSlvcySbFLO7L-tajwzv_4O3FPJV3iM4dBoxcd0tfZJQ_xs1Zg9A4YwwwOvcieUwslvSm4i56uaOaCGf5DM59cZXZ_aZ7N_tXrfi9YM7KdNsW7Qct_WFIVxnFJcTlcnnooy9VsNpQp_Th9Alhvgzw!/dz/d5/L2dBISevZ0FBIS9nQSEh/

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information about the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	No.

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	No thresholds are set.

Q22.	Are there any penalties for non compliance with reporting requirements e.g. tipping off?
A22.	Yes, though not specified.

Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	Yes. The Law mentions that the appropriateness and sophistication of the automated monitoring system will depend on the relevance of the parameters to the nature of business undertaken by each bank or money exchanger.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	Yes.

Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	No specific guidance is mentioned in the Law.

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	External auditors do not report on AML systems and controls. However, SAMA performs regular reviews and solicits external assistance. Subject entities are not required to engage independent parties to report on their AML compliance.

Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A

Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	No.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	No.
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No clear requirements in Saudi Laws.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

United Arab Emirates

Key contact: Tania Fabiani / Helen Brewster

Email: tania.fabiani@ae.pwc.com / helen.brewster@ae.pwc.com

Tel: +971 2 694 6991 x 2991 / +971 4 304 3374

Postal address: Emaar Square, Building 4,

Level 8, Dubai, United Arab Emirates

P.O. Box 11987

Last updated:

January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	With effect from 2000, the Central Bank of UAE ("CBUAE") issued the initial AML regulations under Circular 24/2000 ("the CB Regulations"). In addition, the Dubai Financial Services Authority ("DFSA") AML Module became effective from 2004 onwards. In Jul 2013, the DFSA AML Module was revised to the Anti-Money Laundering, Counter Terrorist Financing and Sanctions Module ("the DFSA AML Rules") while the UAE Securities and Commodities Authority ("SCA") issued its Anti-Money Laundering and Terrorism Finance Combating Procedures in Mar 2010 ("the SCA Regulations").
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	The three primary regulators for AML controls in respect of UAE are (i) the CBUAE (ii) the DFSA, in respect of the Dubai International Financial Centre ("DIFC") free-zone area and (iii) the SCA. The CBUAE licenses and regulates all banks, moneychangers, finance companies and other financial institutions operating in the United Arab Emirates. The DFSA is the regulator of Authorised Firms, (which include banks, insurance companies, investment banks, asset managers and fund administrators) Authorised Market Institutions, Designated Non-Financial Businesses and Professions providing financial services in the DIFC. The SCA is the regulator for all companies and securities licensed by the SCA to operate in the field of securities. The links to the respective websites and regulations are as follows: http://www.centralbank.ae/en/index.php?option=com_content&view=article&id=75&Itemid=95 http://www.dfsa.ae/Pages/DoingBusinesswithDFSA/Anti-MoneyLaundering/Anti_MoneyLaundering.aspx https://www.sca.gov.ae/English/legalaffairs/New%20Laws/056.pdf
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	In respect of the CBUAE and the SCA, no practical guidance is provided while in respect of the DFSA, guidance and supporting commentary is provided for each regulation as part of the DFSA AML Rules (see link provided in A3).

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	An addendum to the CB Regulations ("the Addendum") states that where accounts have been opened prior to 2000, customer due diligence procedures must be undertaken to ensure that there are no risks in continuing such relationships (http://www.centralbank.ae/en/pdf/amlscu/Central%20Bank%20Notice%20No.2922-2008.pdf).
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	The CB Regulations do not appear to apply a risk based approach to the application of the preventive measures, and no sectors have been specifically exempted from the provisions under the AML/CFT legislation and regulations. In addition, the CB Regulations have not been structured so as to recognise the possibility of a risk-based approach to the implementation of the preventive measures at an institutional level. This is in contrast to the approach adopted by the DFSA, which applies an overriding principle that institutions should have systems and controls that recognise and mitigate their specific risks. The DFSA AML Rules place greater emphasis on firms adopting a Risk Based Approach ("RBA") to AML compliance. Firms now have to undertake a risk assessment of its business and of every customer, and assign a risk rating proportionate to the money laundering risk, which will dictate the extent of Customer Due Diligence ("CDD") required. Where the risk of money laundering is high, firms are required to conduct Enhanced CDD. Alternatively, where the money laundering risks are deemed low, firms are permitted to adopt Simplified CDD measures. The SCA outlines a risk based approach by stating that customers should be classified in various categories according to the rates of potential risks they might pose.
Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The country had been subject to the mutual evaluation by IMF followed by a discussion with the MENA FATF and FATF in 2008. See: http://www.menafatf.org/TopicList.asp?cType=train

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	Yes – payment of cash for transfers and drafts above AED2,000 (approx. USD540) for money changers and AED3,500 (approx. USD950) for banks, and also for receipt of transfers and drafts above AED40,000 (approx. USD10,880) to be paid in cash or in the form of travellers cheques. A circular issued by the UAE Ministry of Economy and Commerce sets out thresholds for insurance transactions.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	With respect to the CB Regulations: Individuals: The standard customer identification information specified in the regulations includes the name, address and place of work. In the case of natural persons, institutions are required to check the applicant's passport and retain a copy, which must be annotated by the account officer as a true copy. Passports are considered a universal and reliable form of verification in the UAE. Corporates: The regulations specify that the institution must take the name and address of the entity and, in the case of a partnership, must record similar information for each of the partners. In addition, it must "obtain all information and documents with regard to juridical persons", but specifies, in particular, the government-issued trade licence required by all businesses registered in the UAE. Institutions have typically interpreted "all documents" to mean the Memorandum and Articles of Association (or equivalent) and any documents that support the legal status of the company to conduct business in the jurisdiction. The DFSA AML Rules require all entities to establish and verify the identity of the customers and any beneficial owners on the basis of original or properly certified documents, data or information issued by or obtained from a reliable and independent source. In addition to the above requirements for individuals and corporate, the DFSA AML Rules require all entities to understand the customer's source of wealth or income and undertake on-going due diligence of the customer business relationship. The SCA Regulations outline the verification and identification requirements for both natural and nominal persons in Article 3. These requirements are similar to the requirements outlined for individuals and corporates in the CB Regulations.
Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	For individuals, a copy of the passport is required. For corporates, a copy of the trade licence, stamped and initialled by the concerned employee as "a true copy of the original" is required. There is no information in the regulations or guidance issued by the CBUAE or the SCA as to whether copies can or must be certified by external third parties such as notaries, lawyers and accountants. However, the DFSA AML Rules provide guidance for the identification documents to be certified as a true copy by the specified authorities such as registered lawyer, notary, chartered accountant, government ministry, post office, police officer, embassy or consulate.
Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	The Addendum states that, when opening accounts or remitting money, banks or financial institutions must obtain satisfactory evidence of the identities of the beneficial owners of companies and businesses and clearly understand the ownership and control structure of all legal entities. In addition to the above, the CB Regulations state that, when opening an account for a public shareholding company, a bank must obtain the name and address of the shareholders with holdings of 5% or more. The DFSA AML Rules require establishing and verifying the identity of the beneficial owners and obtaining sufficient and satisfactory evidence of their identities, which includes verifying information on the source of funds and wealth. In addition, the enhanced CDD measures requires the firm to update more regularly the customer CDD information which it holds on the customer and any beneficial owners, increase the degree and nature of monitoring of the business relationship in order to determine whether the customer's transactions or activities appear unusual or suspicious and obtain the approval of the senior management to commence a business relationship with a customer. However, in certain cases, the DFSA AML Rules permit a firm to decide not to verify the beneficial owners and apply simplified CDD measures. The SCA Regulations require verifying the "real beneficiary" of nominal persons (i.e. corporates), where a real beneficiary is defined as a natural person who has and practices actual control over the customer or the legal person, or over the legal arrangements.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	The one exception by the CB Regulations for simplified due diligence relates to transactions falling below the cash transaction thresholds specified for banks (AED40,000 (approx. USD10,880) or AED3,500 (approx. USD950) – see A8) and money changers (AED2,000 (approx. USD540)). The DFSA AML Rules permit simplified CDD measures where the customer is rated as “low risk”. Under the DFSA AML Rules, examples of “Prescribed Low Risk Customers” include: a) an Authorised Firm; b) an Authorised Market Institution; c) a Financial Institution whose entire operations are subject to regulation, including AML, by a Financial Services Regulator or other competent authority in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF Recommendations and it is supervised for compliance with such regulations; d) a Subsidiary of a Financial Institution referred to in c), provided that the law that applies to the parent company ensures that the Subsidiary also observes the same AML standards as its Parent; e) a law firm, notary firm, or other independent legal business or an equivalent person in another jurisdiction whose entire operations are subject to AML regulation and supervision by a competent authority in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF Recommendations; f) an accounting firm, Auditor or other audit firm or insolvency firm or an equivalent person in another jurisdiction whose entire operations are subject to AML regulation and supervision by a competent authority in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF Recommendations; g) a company whose Securities are listed on a Regulated Exchange and which is subject to disclosure obligations broadly equivalent to those set out in the Markets Rules; and h) a government body or a non-commercial government entity in the UAE or a FATF member country. The SCA Regulations do not outline any circumstances for performing reduced/simplified due diligence.
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	The Addendum states that enhanced due diligence processes should be applied with respect to high risk customers which includes foreign PEPs, correspondent banks and specific businesses and individuals dealing in precious metals and stones, real estate, luxury goods, auction houses, private banking customers and non-resident account holders. In addition, the indicators provided in Articles 8 to 14 of the regulations make reference to certain high risk scenarios (e.g. customers from drug producing countries or from countries that do not adequately apply the FATF standards), that should be considered as heightening the money laundering risk. The DFSA AML Rules require enhanced CDD measures in respect of any customer the firm has assigned a rating of “high risk”. Examples of such customers include: a) business relationships conducted in unusual circumstances; b) legal persons or arrangements that are personal investment vehicles; c) companies that have nominee shareholders or directors or shares in bearer form; d) businesses that are cash-intensive; e) the ownership structure of the legal person that appears unusual or excessively complex given the nature of the legal person's business or activities; f) countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML systems; g) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations Security Council or identified by credible sources as having significant levels of corruption or other criminal activity; h) countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country; i) a person not meeting the definition of a PEP but whose high profile or influence poses an elevated risk of corruption; j) anonymous transactions (which may include cash); and k) non-face-to-face business relationships or transactions. The SCA Regulations require companies to take preventative and precautionary measures for high risk customers by performing repeated, periodical and careful examination of the latest positions and transactions of the customer.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	The Addendum requires banks and financial institutions to have systems and controls in place to identify whether a potential or existing customer or a beneficial owner is a foreign PEP. Banks and financial institutions are required to obtain written approval from senior management to open accounts for a foreign PEP. The SCA Regulations are similar in respect of the identification and approval requirements for customers of political significance in a foreign country. The DFSA AML Rules provide detailed guidance on PEPs. A customer falling into this category is considered "high risk" and therefore, enhanced CDD measures are applicable.
Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	The Addendum and the DFSA AML Rules require banks, exchange houses and other financial institutions to carry out due diligence measures when entering into a cross-border correspondent banking relationship. In addition, research must be conducted from publicly available information on the correspondent bank's business activities, their reputation and the quality of supervision and whether the institution has been subject to any regulatory action. Senior management written approval is required to be obtained prior to such relationships being established. The SCA Regulations do not outline enhanced due diligence requirements for correspondent banking relationships.
Q16.	Are relationships with shell banks specifically prohibited?
A16.	The Addendum and the DFSA AML Rules strictly prohibit any relationship, directly or indirectly, with institutions that have no physical presence (shell banks and companies). Although the issue of shell banks is not explicitly addressed in the SCA Regulations, Article 4 prohibits the opening of account or conducting transactions using pseudonyms for natural or nominal persons or for customer acting on behalf of other customers.
Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	Article 3.1 of the CB Regulations requires institutions to take possession of the passport at the time of opening an account. This is understood by institutions (and reinforced by the UAE Central Bank) to mean that the process must be completed in the presence of the customer and that non-face-to-face account opening is not permitted in any circumstances. Similarly, the SCA Regulations require companies to review the original passport of the customer at the time of opening an account. Investors in securities can place their orders through a broker by telephone or in person, but the majority of orders are currently placed by telephone. Trading on the Dubai Financial Market ("DFM") and Abu Dhabi Securities Market ("ADSM") occurs on an electronic trading system, which automatically lists, matches, and executes trades. Securities brokers in the UAE provide investors with direct access to several trading platforms. There are no specific requirements in the DFSA AML Rules that seek to address the risks posed in this area. However, the guidance to the DFSA AML Rules specifies non face-to-face transactions and/or relationships as "high risk". For such business relationships, firms should adopt the enhanced CDD measures to AML compliance.

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	The Suspicious Transactions Reports ("STRs") are required to be reported to the Anti-Money Laundering and Suspicious Cases Unit ("AMLSCU") of the CBUAE and a copy to the DFSA (for entities regulated by the DFSA). See: http://www.dfsa.ae/Pages/DoingBusinesswithDFSA/Anti-MoneyLaundering/STR.aspx

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.
Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes, all three regulations stipulate an obligation to report unusual transactions. Fines are imposed in case of non-compliance with these requirements.
Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	As per the regulation 26/1/2002 issued by the CBUAE regarding declaration when importing cash money into the UAE, any amount not exceeding AED40,000 (approx. USD10,890) can be brought into the country without declaration.
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	Yes, Article 15 of UAE Federal Law No 4 of 2002 sets out the penalties for failure to report any act related to a Money Laundering offence (imprisonment and/or a fine ranging from AED10,000 (approx. USD2,720) to AED100,000 (approx. USD27,230)). In addition, Article 16 sets out the penalties for tipping off any person subject to investigation (imprisonment for a maximum of one year and/or a fine ranging from AED5,000 (approx. USD1,360) to AED50,000 (approx. USD13,600)).
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	There is no such mandatory requirement for use of automated monitoring technology.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	In case a transaction is identified as suspicious, the AMLSCU of the CBUAE shall give instructions to the institutions on how to proceed with the transaction. If the customer in question expresses his wish to proceed with the transaction before the institution receives the instruction from the AMLSCU, the institution shall immediately contact the AMLSCU for further instructions.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	There is no specific guidance on monitoring transactions outside UAE. However, Article 21 and 22 of Federal Law No 4 of 2002 issued by the CBUAE permits cooperation with countries with which the UAE has a ratified treaty.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	There is no specific legal requirement for an external auditor to provide a report on the bank's AML systems and controls. However, the DFSA AML Rules require a firm to undertake regular reviews and assessment of the effectiveness of its money laundering policies, procedures, systems and controls including compliance with its obligations under the DFSA AML Rules. The review and assessment may be undertaken by the firm's internal audit function or by a competent firm of independent auditors or compliance professionals. Similarly, the SCA Regulations stipulate that companies must conduct independent audits on at least an annual basis to measure the effectiveness of their policies and procedures.
Q27.	If an external report on the bank's AML systems and controls is required: a) how frequently must the report be provided? b) to whom should the report be submitted? c) is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	The UAE does not have specific federal laws on data privacy, but various pieces of legislation may have an impact on businesses that engage in data processing activities. These include Federal Law No. 9 of 1987 as amended (Penal Code) which is the primary source of criminal law in the UAE. Specifically, Articles 378 and 379 set out statutory offences and punishment for publication of private matters or the unauthorised disclosure of private information. However, data privacy provisions do exist in the DIFC under the Data Protection Law 2007, as amended by the Data Protection Amendment Law 2012 ("the Law") a) to the extent that "personal data" is defined essentially as "any data referring to an identifiable natural person", this is likely to cover material held for KYC purposes; b) the Law does not apply to corporate data; c) yes. Sensitive personal data is defined in the Law as personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade union membership and health or sex life. The additional protections are captured under Article 10 of the Law with respect to "processing of sensitive personal data." https://www.difc.ae/sites/default/files/Data%20Protection%20Law%20Amendment%20Law_DIFC%20Law%20No.%205%20of%202012%20mark%20up_enacted_16%20Dec%202012.-v3doc_0.pdf

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	Yes, there are a number of limitations and prohibitions on processing sensitive personal data pursuant to Article 10 of the Law: https://www.difc.ae/sites/default/files/Data%20Protection%20Law%20Amendment%20Law_DIFC%20Law%20No.%205%20of%202012%20mark%20up_enacted_16%20Dec%202012.-v3doc_0.pdf
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	No.
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation)? If so, what data is subject to regulation?
A32.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

West Bank & Gaza

Key contact: James Tebbs
Email: james.tebbs@qa.pwc.com
Tel: +974 4419 2715

Postal address: Tornado Tower, 41st Floor
West Bay, Doha, PO Box 6689,
Qatar

Last updated:
January 2016

Regulatory Environment

Q1.	In what year did the relevant AML laws and regulations become effective?
A1.	2007.
Q2.	If the AML laws and/or regulations became effective in the last 2 years, what were the requirements of the previous AML regime?
A2.	N/A
Q3.	Who is the regulator for AML controls for: (a) Banking; (b) Other financial Services; (c) Non financial sector (e.g. casinos, high value goods etc.). Please include link to the regulator(s) website.
A3.	For AML purposes, a national committee has been created to oversee powers at a national level. Members of the committee include representatives from various agencies, which include the Palestine Monetary Authority (http://www.pma.ps/); the Ministries of Finance (http://www.mof.gov.ps/); the Ministry of Justice (http://www.moj.pna.ps/); the Ministry of Interior (http://www.moi.gov.ps/En/); the Ministry of National Economy (http://www.mne.gov.ps/DesktopDefault.aspx?lng=2); the Capital Market Authority (http://www.pcma.ps/portal/english/Pages/Home.aspx); and professional experts in law enforcement and finance. The committee oversees the Financial Follow-Up Unit ("FFU").
Q4.	Is there any practical guidance provided to firms by public authorities regarding AML requirements, beyond the FATF recommendations and local legislation? Please include link to website, where available.
A4.	Palestine Monetary Authority: Money Changers Guideline to Combat Money Laundering (http://www.pma.ps/Portals/1/Users/002/02/2/Legislation/Regulations/Sarrafeen_final_web.pdf); and Financial Follow-up Unit ("FFU") Instructions and Guidelines (http://www.ffu.ps/ar_page.php?id=37b9y14265Y37b9).
Q5.	Is there a requirement to retrospectively verify the identity of customers before the date the new AML regime was introduced?
A5.	No. However, article 6 of the Anti-Money Laundering Decree Law No. (9) of 2007 establishes the requirement to identify and verify the identities of customers when there is doubt about the accuracy or adequacy of previously obtained data concerning the identity of a customer.
Q6.	Is a risk based approach approved by the local regulator(s)?
A6.	No.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q7.	Has the country been the subject of a FATF (or FATF-style) Mutual Evaluation or IMF assessment exercise in the last three years? If yes, please find a link to a relevant report (if publicly available).
A7.	The West Bank/Gaza Strip is not a Member of the Financial Action Task Force ("FATF") and is not on the FATF List of Countries that have been identified as having strategic AML deficiencies. A Mutual Evaluation Report relating to the implementation of anti-money laundering and counter-terrorist financing standards has not yet been undertaken for the West Bank/Gaza Strip.

Customer Due Diligence

Q8.	Are there minimum transaction thresholds, under which customer due diligence is not required? If Yes, what are the various thresholds in place?
A8.	The FFU Instructions for AML for Banks Operating in Palestine (2009/1) article 2 states that a bank must implement customer due diligence measures when: a) establishing business relations with a new or existing customer; b) a customer presents intentions to proceed with financial transactions or money transfers (domestic or international) greater than USD10,000; or c) a natural person or legal entity presents intentions to carry out occasional financial transactions or money transfers equal to or greater than USD10,000.

Q9.	What are the high level requirements for verification of customer identification information (individuals and legal entities)?
A9.	The natural person shall be required to present his/her ID, passport or any legally accepted official document to verify his/her full name, ID number, address, residence location, date and place of birth and his/her work address on the document. Additionally, it is required to have his/her permanent address in his/her country for those who are Non-Palestinians. All the information related to the legal person shall be verified including his/her name, address, head office, and his/ her mangers' legal IDs. Additionally, he/she shall be required to submit the following officially certified documents: a) registration certificate; b) Articles of Association; c) bylaw; d) authorized signatories; and e) his/her agent identity. Moreover, the names of partners or stockholders whose ownership exceeds 10% of the company capital in addition to owner beneficiaries shall be verified. Relevant documents corroborating such information shall be attached. For <u>charitable organisations</u>: a) registration certificate and authorized signatories; b) bylaw; and c) his/her agent identity.

Q10.	Where copies of identification documentation are provided, what are the requirements around independent verification or authentication?
A10.	Not explicitly addressed.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q11.	What are the high level requirements around beneficial ownership (identification and verification)?
A11.	When a party is representing a customer, a copy of the agency agreement or power of attorney certified by a notary is required, in addition to documents confirming the identity of the agent and the principal. The bank must verify the identity of the depositor when depositing cash or travellers cheques into an account by an individual or individuals whose names do not appear on the agency agreement or power of attorney for that account, or if any of these individuals are not legally authorised by the account holder to deposit funds into the account. In the case of minors or a person lacking full legal capacity, the bank must perform the verification of customer identification information for the person lacking full legal capacity as well as their representative opening the account.
Q12.	In what circumstances are reduced/simplified due diligence arrangements available?
A12.	N/A
Q13.	In what circumstances are enhanced customer due diligence measures required?
A13.	The FFU Instructions for AML for Banks Operating in Palestine (2009/1) article 3 requires that banks ensure enhanced due diligence for PEPs as they are considered high risk as follows: - by accurately verifying the identity of partners or stockholders whose ownership exceeds 10% of the company capital in addition to owner beneficiaries; - obtaining the approval of upper management before initiating any dealing with the party; and - confirming the sources of funds to be deposited and the sources of wealth. The FFU Instructions for AML for Banks Operating in Palestine (2009/1) article 4 requires that banks ensure enhanced due diligence measures for the following cases: - when renting safety deposit boxes; - when collecting checks from external unknown third parties; - when a request for operations or deals which are complex or significant, or unusual deals or transactions which do not have clear financial objectives, and those connect with offshore activities, as well as operations connected with juristic individuals not legally present or unregistered; - significant foreign exchange operations, or recurring foreign cash outlays; - exchanges of significant amounts of smaller coins for larger coins; - deposit of significant amounts, or recurring deposits which are significant when aggregated, which are not apparently aligned with the normal activities of the customer or the usual size of its operations; - an account operating mainly for significant transfers to foreign countries, or to receive significant transfers from foreign countries, whereby to the bank employee that is executing the instructions of the customer, it appears that the activities of the customer do not justify such operations; - cashing foreign checks or significant check amounts which are not aligned with the nature or size of the usual activities of the customer, or which the customer claims are gains from such things as gambling; and - significant or recurring customer operations which are related to external activities and which the bank sees as unaligned with the size of these activities.
Q14.	In what circumstances is additional due diligence required for Politically Exposed Persons ('PEPs')?
A14.	Additional due diligence is required for PEPs which are defined in the National AML Committee Instructions (1) of 2014 under article 3.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q15.	What enhanced due diligence must be performed for correspondent banking relationships (cross-border banking and similar relationships)?
A15.	As per article 6 of the Anti-Money Laundering Decree Law No. (9) of 2007: a) identify and verify the receiver institutions with which they establish banking relations; b) collect information on the nature of the activities practiced by the receiver institution; c) evaluate the reputation of the receiver institution and the nature of the supervision to which it is subject based on published information; d) obtain the approval of senior management before establishing a banking relationship with the receiver institution; e) evaluate the anti-money laundering controls implemented by the receiver institution; and f) ascertain, in the event of payment from an exporter's account, that the receiver institution has verified the identity of the client, that it implements mechanisms for constant surveillance of its clients, and that it is capable of providing relevant identifying information when requested to do so.

Q16.	Are relationships with shell banks specifically prohibited?
A16.	Yes. Financial institutions may not enter into or continue business relationships with registered banks that lack a physical presence (in the National Authority's territories) and are not subordinate to a regulated financial group that is subject to the effective supervision by the competent supervisory authorities.

Q17.	In what circumstances is additional due diligence required for non face-to-face transactions and/or relationships?
A17.	N/A

Reporting

Q18.	To whom are Suspicious Activity Reports (SARs) made? Please include a link to their website.
A18.	To FFU Director: http://www.ffu.ps/index.php?option=com_content&view=article&id=29:-2013&catid=7:-2013&Itemid=13&lang=en

Q19.	What was the volume of SARs made to the authorities in the most recent year? Please state the GDP for the equivalent year.
A19.	Information on the volume of SARs is not publicly available.

Q20.	Are there any obligations to report anything more than suspicious transactions e.g. unusual transactions, cash transactions above a certain threshold, international wire transfers, other transactions etc.?
A20.	Yes.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q21.	Are there any de-minimis thresholds below which transactions do not need to be reported?
A21.	N/A
Q22.	Are there any penalties for non-compliance with reporting requirements e.g. tipping off?
A22.	As per article 16 of the Anti-Money Laundering Decree Law No. (9) of 2007, tipping off is prohibited. As per article 43 of the Anti-Money Laundering Decree Law No. (9) of 2007, any person violating article 16 shall be punished by imprisonment of 1-3 years and/or a fine of JOD5,000 – JOD100,000 (approx. USD7,040 - 140,820) or the equivalent in the currency in legal circulation. If a person commits the crime of money laundering stemming from a predicate offence that is a felony, the person shall be punished by imprisonment of 3-15 years and/or a fine of JOD10,000 – JOD100,000 (approx. USD14,080 - 140,820) or the equivalent in the currency in legal circulation. If a person commits the crime of money laundering stemming from a predicate offense that is a misdemeanour, the person shall be punished by imprisonment of 1-3 years and/or a fine of JOD5,000 - JOD50,000 (approx., USD7,040 - 70,410) or the equivalent in the currency in legal circulation. If a person attempts to commit the crime of money laundering, or aids, abets, facilitates, or consults regarding the commission of this crime, he shall be punished by one-half of the penalty imposed on the primary perpetrator. A legal entity that commits the crime of money laundering shall be punished, without prejudice to the liability of any natural person subordinate to the legal entity, by a fine of JOD10,000 - JOD200,000 (approx. USD14,080 - 281,630) or the equivalent in currencies in circulation. A legal entity shall be jointly liable for payment of adjudicated fines and damages if the crime that occurred in violation of this law was committed by one of its employees on its behalf and to its benefit.
Q23.	Are there any requirements (legal or regulatory) to use automated Suspicious Transaction monitoring technology?
A23.	There is no mandatory requirement for the use of automated monitoring technology.
Q24.	Is there a requirement to obtain authority to proceed with a current/ongoing transaction that is identified as suspicious?
A24.	As per article 15 of the Anti-Money Laundering Decree Law No. (9) of 2007, financial institutions and nonfinancial businesses and professions (real estate agents/brokers, dealers in precious metals, high-value transactions dealers including antiquities dealers, certain attorneys and accountants, providers of credit and corporate services not covered by the law, persons who provide certain services to other parties on a commercial basis) must refrain from executing transactions which they suspect involve the crime of money laundering until they report their suspicions regarding such transactions to the FFU.
Q25.	Does the local legislation allow transactions to be monitored outside the jurisdiction?
A25.	Yes.

'Know Your Customer' quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

AML Audits

Q26.	Is there a legal requirement for a bank's external auditor/other external organisation to report on the bank's AML systems and controls?
A26.	N/A
Q27.	If an external report on the bank's AML systems and controls is required: g) how frequently must the report be provided? h) to whom should the report be submitted? i) is it part of the financial statement audit?
A27.	N/A
Q28.	What are the requirements for the content of this external report on a bank's AML systems and controls? Does it require: a) sample testing of KYC files? b) sample testing of SAR reports? c) examination of risk assessments?
A28.	N/A

Data Privacy

Q29.	Does the country have established data protection laws? If so: a) does the definition of "personal data" cover material likely to be held for KYC purposes? b) how do the laws apply to corporate data? c) does this country have a separate definition of "sensitive data"? How is it defined and what are the additional protections?
A29.	There are no special or separate legislative documents in Palestine that deal specifically with data privacy. However, there are several different laws and regulations that contain restrictions on the disclosure of certain confidential information. The main law in relation to confidential information is the Penal Law No. 16 of 1960 (the Penal Law), which criminalises the disclosure of confidential information. In particular, Article 355 of the Penal Law states that any person who discloses any official confidential information to any unauthorised person (or to any person who is not legally competent to receive such information) may be imprisoned for up to three years. Moreover, the third paragraph of the same Article provides for a similar punishment in respect of any person who receives confidential information in the context of his or her profession and reveals such information without legitimate cause. The provisions of the Penal Law are of general application, but there are also certain specific sectorial laws that place high emphasis on confidentiality and a duty to protect privileged information in different circumstances. These include: a) Law No. 3 of 1999 regarding the Palestinian Bar Association, which stipulates in Article 28 that any lawyer is under a strict obligation not to disclose any secret information that he has received from his client or obtains in the context of his profession; b) similar provisions to those imposed on lawyers noted above can be found under laws regulating doctors and medical professionals (e.g. pharmacists) as well as financial auditors; c) laws and regulations that govern the functions and duties of financial brokers and custodians (in particular, Securities Law No. 12 of 2004) impose duties on officers of the stock market and brokerage firms to keep confidential any information they receive; and d) Banking Law No. 2 of 2002 (as amended) and the newly enacted Banking Law of 2012 provide that all board members and executive officers of any bank are, jointly and severally, liable in exercising their duty to maintain the secrecy of information regarding the clients of the bank.

‘Know Your Customer’ quick reference guide

Country by country comparison of high level Know Your Customer and Anti-Money Laundering information

Q30.	Are there any prohibitions on the transfer of credit reports (for KYC and credit risk analysis purposes), criminal records (for KYC and crime prevention purposes) and medical data (for KYC and pension benefits purposes)?
A30.	N/A
Q31.	Is there case law, other constitutional law or any other laws or regulations that may impact upon the transfer of information to this jurisdiction?
A31.	N/A
Q32.	Does this jurisdiction have bank secrecy laws or other obligations of confidentiality (other than those that may have been accepted expressly under contract e.g. in account opening documentation?) If so, what data is subject to regulation?
A32.	N/A