Governance Insights Center
Risk Oversight Series

November 2018

How your board can oversee third-party risk

Third parties are critical to business today. But they also mean big risks.

Given the sheer number of third parties that companies use, it's important to evaluate and manage the related risks. Boards can play an important role in encouraging companies to establish effective third-party risk management programs.

pwc

pwc.com/us/governanceinsightscenter

Many companies rely on third parties to some extent. Some have thousands of third-party relationships. They help companies save costs, improve service speed and provide global access. They also allow companies to be more flexible and competitive.

What is a third party?

A third party is any individual, company, customer, vendor, supplier, agent or distributor that interacts with or on behalf of a company. Third parties provide all types of services, from processing payroll to running data centers. Some companies use third-party local country experts, lobbyists or joint venture partners to drive business in new locations. Often, third parties have their own vendors.

But third parties can also create big risks, from reputational and brand risk to the risk of serious financial damage. This means companies need to carefully select and monitor their third parties. We're not only talking about bribery, fraud and legal compliance. Some vendors access or store your company's intellectual property, records, data and network—raising cybersecurity and data privacy issues. Those that manufacture on your behalf can bring worker safety and human trafficking issues. And the implications go on.

The number of third-party relationships a company has can be staggering. In our experience, companies underestimate the number they interact with by a factor of three to five.

Common areas of risk when using third parties

Money laundering
Privacy *Environmental*
Trade, sanctions, export controls
Fraud *Health and safety* *Kickbacks*
Business continuity and resiliency
Cybersecurity *Antitrust* *Conflict minerals*
Trafficking, slave or child labor
Intellectual property theft
Technology *Bribery*

Managing third-party risk usually gets the most attention when:

- A company is in a highly regulated industry—think financial services or pharma/life sciences
- A company has run into Foreign Corrupt Practices Act (FCPA) issues, and regulators require robust compliance and monitoring programs as part of a settlement agreement

But how can boards make sure there's sufficient focus on third-party risk management before problems come to light? And what can companies do to have a better chance at avoiding problems?

21%

of organizations have no dedicated budget for third-party risk management[1]

What are the hurdles to understanding third-party risks?

Getting a handle on a company's third-party relationships can be overwhelming, for a number of reasons.

No complete list identifying third parties. The vast number of third parties makes it tough to inventory even the ones the company works with on a regular basis. Companies may not know who all their third parties are for a number of reasons. For one thing, managing third parties is often siloed: the IT department engages IT vendors; procurement engages supply chain vendors; country management engages local vendors; and so on. For another thing, many countries rely on historical relationships. Plus, in some cultures, businesses rely on a person's word or handshake and so there may not be contracts or formal agreements at all.

Even if a company has adequate programs for setting up new vendors, local offices may do "shadow" procurement to get around the controls. That means the head office may not know all of the vendors being used.

And what about the vendors of vendors? In PwC's *2017 Global Third Party Risk Management Survey*, 83% of respondents say they rely on their third parties to perform due diligence and monitoring of their *own* third parties or subcontractors (sometimes called "fourth" or "nth" parties), and 24% said they don't have contractual rights to perform due diligence or monitoring on subcontractors. Only 8% of respondents say they perform their own due diligence and monitoring of the fourth parties used by their third parties.[2] While the survey was of financial institutions, we expect other sectors would have similar results. So a company's supply chain can bring huge brand or reputational risk from suppliers it doesn't even know it has.

Third parties and acquisitions

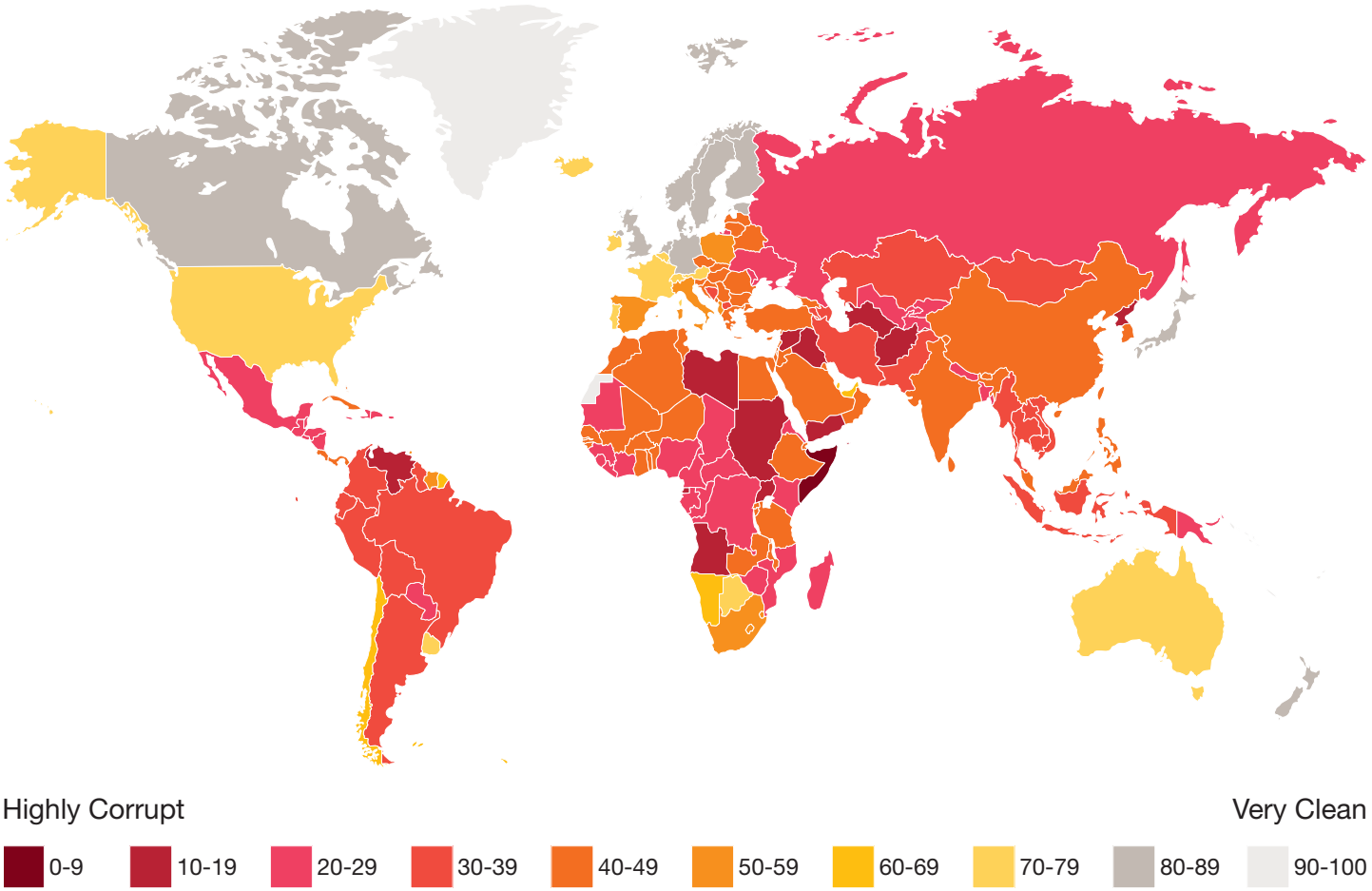
- Have you inherited third parties as part of an acquisition?
- What happens if you find problems with the target company's third parties? How serious would problems have to be to postpone or jeopardize the deal?
- What if it postpones or jeopardizes the deal?
- Have you considered what you will do if a third-party relationship needs to be terminated and impacts deal price?
- What about concerns related to joint venture partners and other alliances?

Incomplete understanding of what third parties are doing. Companies often don't have a centralized or real time view of what their vendors are doing. Companies may also lack a consistent way to categorize or tag their third parties based on the service they provide. A vendor might have been approved for one use (say, processing certain data), so a manager may think it's okay to use that vendor for something else (say, providing cloud storage). But different services should prompt additional evaluations—even for approved vendors.

Little appreciation for how third parties operate. Many third parties have key operations outside the United States—in countries with significantly different business practices. Some of those may violate US laws, as well as contravene the company's ethical culture and operating standards. For example, providing gifts and other incentives may be common practice in other countries as a way to build—and maintain—business relationships. But those gifts may be considered bribes under US law.

Many companies do business in other countries, so it's important to understand what the customs are and whether those customs might violate US laws. Half of respondents to a Navex survey say they engage with third parties in Asia, just over 40% engage with third parties in Latin America, one-third do so with those in the Middle East and 28% do with those in Africa.[3] And companies will want to know if the countries they're doing business in are perceived to conduct business in an above-board way or not.

Almost 70% of countries have a perceived serious corruption problem



Source: Transparency International, *Corruptions Perception Index 2017*, February 2018.

The process to select third parties is flawed. Too often when a company is engaging or evaluating a third party, the correct leaders are not at the table, and there is not a complete understanding of all elements that need to be considered. For example, a company might bring on a third party to expand into another country without thinking about potential data-sharing risks.

It costs an arm and a leg. We mentioned earlier that many companies take a siloed approach to managing third parties. That adds to cost inefficiency, as each group runs its own process. Cataloguing and analyzing a company's third parties can also be expensive, particularly for companies that are starting from scratch. Often, there is little appetite to dedicate resources to such a process unless there is a burning platform to do so.

It takes time—time the company may not have when the business is trying to react quickly. Shepherding a third party through a thorough evaluation and approval process takes time. Often, the business may be impatient to activate the third party—and it can be tempting to circumvent the process.

Factors in assessing third-party risk

It can help to understand exactly what risks companies face from using third parties. Services provided by a single third party may represent risks in multiple areas.

Cybersecurity and data privacy

Cybersecurity and data protection is the top concern and challenge relating to third parties.[4] Companies are relying more on the internet of things, cloud computing and data analytics. Many use third-party vendors for these technologies. But often, companies don't know how many of their third parties have access to sensitive data. There has been an increase in the number of companies that have fallen victim to data breaches because of third parties—in 2017, 56% of data breaches related to third parties, compared to 49% in 2016.[5] Third parties often are targets because of their access to data, while others have insecure entry points. And some companies don't believe their third parties would notify them if they had a breach.[6]

Plus there are privacy laws to comply with. For example, the European Union's General Data Protection Regulation (GDPR) took effect on May 25, 2018.

For-profit companies can be fined up to $24 million, or 4% of global revenue (whichever is greater), for GDPR violations.

Bribery/FCPA

Every US company conducting or seeking business abroad is subject to the FCPA. The FCPA's anti-bribery provisions prohibit paying bribes to foreign officials to help get or retain business. That prohibition extends to the agents, distributors and other third parties who work on a company's behalf.

From 2013 to 2017, 50 of 64 corporate FCPA settlements pertained to underlying misconduct involving third parties. Those ranged from consultants to sales agents and distributors to customs brokers.[7]

Compliance

There's more to comply with than simply FCPA and data privacy laws. There are also anti-money laundering, and consumer and employee protection laws. There are also stringent industry requirements for certain sectors, such as for medical devices.

Ethical/Social/Environmental

Mass subcontracting means companies are outsourcing production to factories and network suppliers all over the world, where costs are lower. This makes it very difficult to track a company's complete supply chain. And that often opens up ethical and social risks—and the possibility of a lawsuit or negative publicity. In 2016, Amnesty International discovered child labor in the supply chains of some big technology and automotive companies.[8] Food manufacturers have also come under fire for using child labor in poverty-stricken countries. And sweatshops still exist in the retail industry, with the pressure to produce cheaper products faster. Such facilities can have worker safety issues.

More than 152 million children worldwide between 5 and 17 are victims of child labor.[9]

Brand/Reputation

Consumers increasingly want to understand the practices of the businesses they interact with. In today's always-on environment, unethical practices of third parties could go viral and turn into a brand crisis.

Vulnerability

A natural disaster or some form of cross border trade restriction (think Brexit) that disrupts the supply chain can hinder operations. That's especially true if alternative sources aren't readily available.

Materiality

How much a company spends with a third party will always be part of the risk calculation. But the amount of spend isn't the sole criteria. A third party that represents a relatively minor expense may present more significant risk depending on the nature of its services. Think IT access.

In ***68%*** of the cases where external actors are identified as the main perpetrators of disruptive fraud, those external actors are "frenemies" of the organization—agents, vendors, shared service providers and customers.

Source: PwC, *2018 Global Economic Crime and Fraud Survey*, 2018.

What does an effective third-party program look like?

Ideally, an effective third-party program would give management a current inventory or catalog of all third parties and their risk level, and provide information on how well the risks are being addressed. But that's a tall order. It's vital that the CEO supports addressing third-party risk—to ensure it receives the right resources and attention. Of course, there are benefits to addressing third-party risk beyond simply avoiding disaster. It can also bring efficiencies as companies streamline procurement and other processes.

Breaking it down, the program should:

- Have the right leader. If your company has a chief risk officer, that person could take the lead. If not, think about using the head of supply chain or some other global/operational function. Whoever is selected, that individual needs to have the ability to break down silos between functions and territories.
- Get access to all needed resources. In our experience, highly-regulated companies make the resources available, but many other companies struggle. Assessing risk appropriately usually requires resources from IT, compliance, legal, HR, finance, cybersecurity, procurement, internal audit and business units.
- Assess third parties against a third-party risk framework. Identify the third-parties the company deals with and understand the scope of the risk for each relationship. Determining which relationships are the riskiest can be the most difficult aspect for many companies.

How to establish an effective third-party program:

Identify third parties. First, the company has to figure out how it will define a third party. Then it has to figure out which categories of possible risk (bribery, cyber, environmental, etc.) are most critical. That will help it understand which categories of third parties (e.g., suppliers vs. distributors vs. agents) to start with.

While companies may know who their critical vendors are, unfortunately, most don't have a complete list of third and fourth party vendors and suppliers. A good place to start is by looking at who the company pays—using information from procurement, contracts and finance. It can also take some digging to uncover "shadow" vendors—ones that fall outside of the formal control. (For example, employees may use software-as-a-service products and cloud services without going through the IT department.)

Only 35%

of companies have a comprehensive inventory of all third parties with whom they share sensitive and confidential information[10]

Establish policies and processes. Ideally, companies have one central place, often in procurement, to assess a potential third party and the service it proposes delivering. One way to address third-party risks is to include contract terms that establish the standards and level of compliance the company expects. For instance, some companies set environmental, social or employment standards for their third-party vendors. As a company updates or strengthens its contract terms, they will apply to new vendors. The company can then prioritize (based on level of risk) which existing parties it should renegotiate with first.

It's a challenge to calibrate the third-party approval process. It needs to be rigorous without interfering with business. A process that is so strict that operations grind to a halt isn't going to work over the long term—and it may not work over the short term either. But any effective approval process is going to take time. So it's vital to train the business to factor in additional time to work a new third party through the evaluation process.

Evaluate individual third parties. This entails assessing which risks a third party exposes the company to—against all risk domains (e.g., business continuity, bribery, financial, cybersecurity, data privacy, reputation). If new third parties have issues that might expose the company to an unacceptable level of risk, they would need to remediate them before being engaged.

Because of the high risk of cyber breaches, understanding how third parties process, transmit and store data is vital. This includes attributes like the volume of transactions, sensitivity of the services provided, whether the data is regulated (think privacy legislation) and how sensitive it is.

Most companies use a combination of on-site visits and having third parties complete questionnaires. The frequency of these types of monitoring will depend on the risk level. Many build monitoring frequency and approach into contracts. Others require questionnaires to be completed periodically, require annual audit reports on the third party's compliance with contract provisions and/or some retain access rights to send in their own auditors.

The bottom line? Companies need to evaluate third parties not only before engaging them, but on an ongoing basis.

Simplify the vendor base. Many companies use the third-party assessment process as an opportunity to reduce and rationalize the number of suppliers. Some vendors are removed due to an unacceptable risk level. In fact, 53% of 539 compliance, risk, audit and IT executives said their companies are planning to "de-risk" their third-party vendor relationships that pose the highest risk by either exiting or changing them.[11] In other cases, a company may simply realize it has multiple vendors doing the same thing or that it doesn't need as many vendors in an area. The assessment process provides an opportunity to streamline the procurement process, improving efficiencies and saving money without sacrificing supply chain reliability.

One key to improving how a company handles third-party risk is to reduce its number of vendors.

Leverage technology. Given the amount of time and effort it can take to address third-party risk, it's worth asking how technology can help. Many companies invest in tech-enabled infrastructure to support this aspect of risk management.

Understand where to start. Like many complex projects, it's hard to know where to start. It would be costly and possibly overwhelming to inventory all third parties. By starting with new vendors and applying the third-party risk assessment and contracting process to them, companies can learn from the process what works and what doesn't. Then they can systematically start applying it to existing vendors—ideally starting with the highest risk populations. Practically speaking, a company may never fully cover all of its third parties—but it can at least manage a good part of its risk.

Only one way in—Companies struggle with implementing thorough third-party approval processes. For example, when they start restricting new third parties—in effect, barring the door—managers often find other ways in, bringing third parties in through a window. In order to build an effective process, companies have to make sure there is only one way to work with a third party. How? One approach is to make sure that a vendor can't get paid without going through the assessment process—by not allowing payments with local or manual checks.

What role should the board play?

First, determine where at the board level you'll oversee third-party risk. Many boards give it to the audit committee. Some have a risk committee, though this is not common.

And however companies decide to establish a third-party program, boards will want to be sure to get updates from management on the program's progress.

How should the board oversee third-party risk management?

Only 33% of respondents to a 2017 survey say their companies regularly report to the board on the effectiveness of the third-party management program and potential risks to the organization.[12] The board is critical to risk management oversight—so directors will want to push management for regular reports on the third-party risk management program, including reports on the company's key third parties and third-party risks.

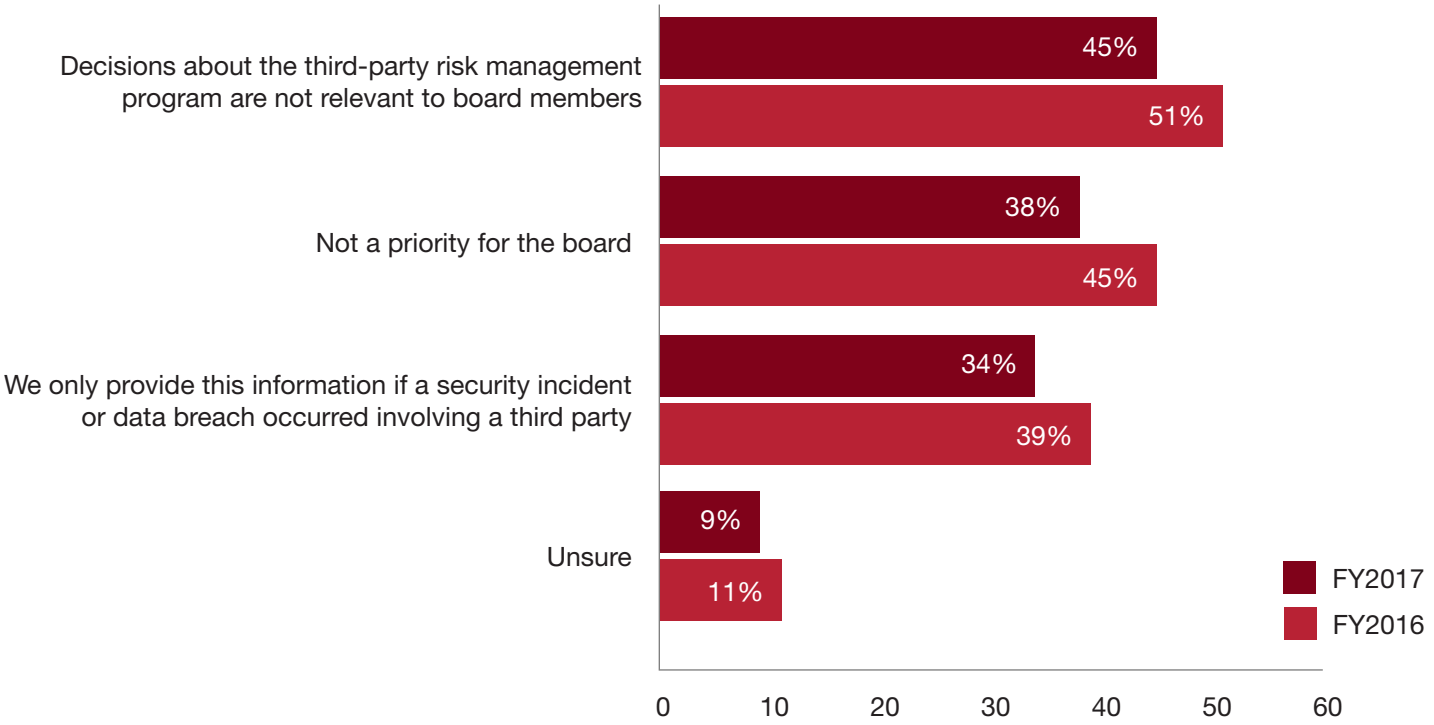
The reports can include the total catalogue of third parties the company uses (once the company goes through the inventory process), as well as lists of new and approved third parties and terminated or "de-risked" third parties. Boards should understand how management assesses its third-party risks—which ones are critical to the company and which ones are not. Boards will also want to know if any significant third-party contracts are up for renewal in the next year, whether management plans to renew them and if not, why not. Boards will also want to discuss and determine how often to get these reports.

Example dashboard: How boards can get a handle on the company's key third-party risks

Key risk	Type of third party	Number of vendors	Risk rating	Steps needed to reduce risk
Cybersecurity/Data privacy	IT Services/Contractors	30	HIGH	
Labor	Contractors, Suppliers, Agents, Distributors	25	MEDIUM	
Business interruption	Suppliers, Resellers	5	HIGH	
Compliance	Lobbyists, Country experts, Joint venture partner	10	MEDIUM	
Bribery/FCPA	Distributors, Agents	10	HIGH	

Why aren't third-party risks reported to the board?

Reasons for not regularly reporting third-party risks to the board of directors
More than one response permitted



Source: Ponemon Institute, *Data Risk in the Third-Party Ecosystem - Second Annual Study*, September 2017.

Questions boards can ask about third-party risk

About the program

- What is the current status of the company's third-party risk assessment programs?
- Who has responsibility for it? Who is involved? Are there adequate resources?
- If the program is being developed, what's the timeline and is progress on track? What percentage of third parties have been covered? What is the outcome of assessments already completed?
- What approach does the company take to perform due diligence on its third parties?
- How does management assess its long-standing relationships? Are there different criteria for those third parties? Should there be?
- Is management leveraging the program to its best advantage? Or is it seen solely as a compliance exercise?
- How is internal audit involved in assessing the program?
- Does the company have a robust third-party risk management program? Is it bringing value to the business?
- How does the company monitor fourth and nth parties?

About third parties

- How does management rank the third parties that represent the biggest risks to the company?
- Why does management consider them so risky? Is management thinking about terminating them as a result? If not, how is management monitoring them?
- What controls are in place to mitigate the risks that third parties present?
- How often does management update their ranking and risk scoring?
- Do the third parties have all of the necessary licenses to operate? Do they have the expertise, processes and resources to implement needed controls to stay compliant with changing laws and regulations?
- How many third parties have been terminated as a result of our third-party risk management process?

In conclusion…

Using third parties, business partners and outsourcing is part of the business landscape. Third parties provide companies with many benefits, but they carry inherent risks. And the sheer number of third-party relationships companies have makes it difficult to oversee the risks they bring. That's why having an efficient and effective third-party risk management program is critical—and boards need to know if the risks are being adequately addressed.

How PwC can help

To have a deeper discussion about how this topic might impact your business, please contact your engagement partner, or a member of PwC's Governance Insights Center.

Paula Loop
Leader, Governance Insights Center
(646) 471 1881
paula.loop@pwc.com

Catherine Bromilow
Partner, Governance Insights Center
(973) 236 4120
catherine.bromilow@pwc.com

Patricia Etzold
Partner, Forensics
(646) 818 7196
patricia.a.etzold@pwc.com

TR Kane
Global Third Party Risk Leader
(440) 390 8502
t.kane@pwc.com

Dean Spitzer
US Third Party Risk Leader
(917) 841 2976
dean.v.spitzer@pwc.com

Tiffany Gallagher
Pharmaceutical Third Party Risk Leader
(973) 236 4646
tiffany-anne.gallagher@pwc.com

Project team

Elizabeth Eck
Senior Manager
US Integrated Content Team

Karen Bissell
Marketing Manager
Governance Insights Center

Meredith Martin
Marketing Senior Manager
Process Assurance

Daniel Graffe
Senior Designer
US Creative Team

Other "Risk Oversight Series" topics include:

- ***Why your board should take a fresh look at risk oversight: a practical guide for getting started***
- ***How your board can influence culture and risk appetite***
- ***How your board can ensure enterprise risk management connects with strategy***
- ***Why your board should refocus on key risks***
- ***How your board can be ready for crisis***
- ***How your board can decide if it needs a risk committee***
- ***How executives and boards can get the risk information they need***
- ***How your board can better oversee cyber risk***

Endnotes

1. Navex Global, *2017 Ethics & Compliance Third-Party Risk Management Benchmark Report,* November 2017.
2. PwC, *Global Third Party Risk Management Survey – 2017 Results Summary: Financial Services,* 2018.
3. Navex Global, *2017 Ethics & Compliance Third-Party Risk Management Benchmark Report,* November 2017.
4. Ibid.
5. Ponemon Institute, *Data Risk in the Third-Party Ecosystem – Second Annual Study*, September 2017.
6. Ibid.
7. PwC analysis of FCPA settlements, 2012 through 2017.
8. Amnesty International, "Exposed: Child labour behind smart phone and electric car batteries," January 19, 2016.
9. United Nations website, World Day Against Child Labour 12 June, http://www.un.org/en/events/childlabourday/background.shtml.
10. Ponemon Institute, *Data Risk in the Third-Party Ecosystem – Second Annual Study,* September 2017.
11. Protiviti and Shared Assessments, *2017 Vendor Risk Management Benchmark Survey*, 2017.
12. Ponemon Institute, *Data Risk in the Third-Party Ecosystem – Second Annual Study,* September 2017.

pwc.com