

The director's guide to ERM fundamentals

A board primer: foundational elements of effective enterprise risk management

September 2023

Introduction

Recent bank failures have left many leaders, across industry sectors, concerned about how well their companies are managing risk. Reviews and investigations, particularly of companies in regulated sectors, can sometimes uncover weak governance structures and shaky risk and control environments. This, coupled with other major geopolitical and global events of the last few years, has increased interest in enterprise risk management (ERM) programs.

ERM programs are intended to formalize how risks are identified, assessed, managed, monitored and reported on in light of strategic priorities. But what we're seeing is that some ERM programs aren't getting the desired traction, either losing momentum or lacking adequate investment. In short, they're not doing what they're supposed to do.

Having an effective ERM program can help the board and management make more informed decisions in the face of uncertainty — whether that's specific to a particular company or sector or facing the entire economic landscape. Not all companies will have a robust ERM program, particularly in industry sectors that are not heavily regulated. But the bottom line is that even if a company lacks sophisticated ERM, regular discussions with management on their risk management strategies will help boards keep up with the evolving risk landscape and oversee the company's key risks.

How to use this guide:

The **first part** of this guide introduces what it means to build a sustainable and enabling ERM program, including how the board can assess whether their ERM program's maturity is where it should be.

The **second part** of this guide outlines six key elements that we think make up an effective **Enterprise Risk Management** program. These key elements offer directors a foundation for overseeing enterprise risk management.

E Enterprise

1. Alignment with corporate strategy
2. Risk strategy and governance

R Risk

3. A common risk language
4. Enterprise risk assessment

M Management

5. Risk response plans
6. Ongoing monitoring

The guide also includes a few supplemental tools in its appendices.

Appendix A provides an example of a risk response plan, and **Appendix B** provides several risk reporting dashboard examples.

We hope this guide will prove useful to directors. It may even allow them to rest easier — free from worrying about what “keeps them up at night.”





Board blind spot: Only 45% of executives surveyed say their boards have good or excellent risk management expertise — a strikingly low figure given that risk oversight is a key board responsibility. There is opportunity for directors to upskill and deepen their fluency in ERM practices. The board's oversight of risk starts with an objective review of management's process for assessing and mitigating risks.

How can companies build a sustainable and enabling ERM program? ERM done right can create a value-driven risk management program, propelling a company's strategy forward while navigating disruptions. The program works best when it is well defined, has a clear value proposition, and includes a plan to develop, integrate and institutionalize ERM across the organization over time. Design and implementation can take time, depending on both the complexity of operations and external environment and the resources committed to risk management across the three lines. A program also can't achieve full potential without an executive leader with the stature and credibility to build strong relationships with the board and senior leadership — and the willingness to promote appropriate risk accountability and oversight.

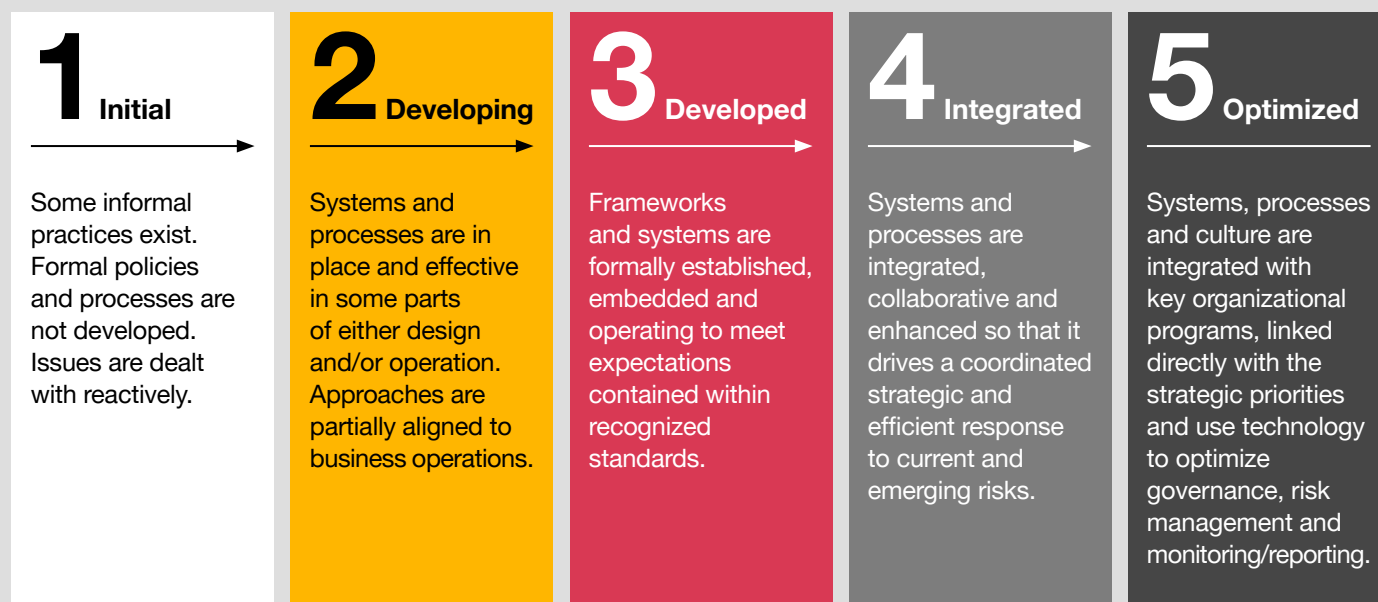
As a key stakeholder and voice on risk management oversight, the board should have a strong understanding of management's risk program objectives and activities, how those activities help achieve its strategic goals and how the program is operationalized across the enterprise.

How can we assess whether our ERM program's maturity is where it should be?

Boards should question the maturity of the company's ERM program and help management set expectations for where the organization wants to be in the future.



PwC's ERM Maturity Model at a high level:



Since a primary board responsibility is to oversee leadership's risk management process, directors should have a baseline understanding of the foundational elements of an effective ERM program. Whether the company has a robust, sophisticated program or a newer, less mature program, the board should understand the risk capabilities currently in place. The insights shared here can be used regardless of the maturity level of a company's ERM activities.



Recent research, representing different sizes and types of organizations, provides a snapshot of the state of ERM program maturity:

- Greater adoption of ERM has occurred, although not at a level many might expect in light of the risk environment we now face.
- There continues to be significant opportunity for improvement in most organizations, given that more than two-thirds of organizations surveyed in 2023 still cannot yet claim they have “complete ERM in place.”
- Only 29% of survey respondents describe their organizations’ approach to risk management as “mature” or “robust.”
- The level of sophistication of underlying risk management processes still remains fairly immature (e.g., “very immature” or “developing”) for just over one-third of those responding to the survey.



Questions the board should ask management:

- If we have established an ERM program, what are the risk program's strategy and objectives?
- What has management done in the last 12-18 months that has helped advance ERM capabilities or the program?
- Which ERM program elements are working well? What are the perceived shortcomings or enhancement opportunities? What ideas does management have for taking the ERM program to the next level?
- If we have not invested in a formal ERM program to manage, monitor and report our key risks, why not?

Foundational elements of enterprise risk management — breaking E-R-M down

Enterprise

1. **Alignment with corporate strategy:** helping boards oversee risk as part of strategic planning and execution, not separate risk from strategy

Unexpected risk events have shown boards and management the value of instituting ERM practices. The degree of complexity and change facing organizations today highlights the need for strategies that account for risk.



External factors driving the need for effective ERM linked to corporate strategy

- New strategic risks due to emerging business models
- Rapidly changing market dynamics
- Growing investor and public interest in companies' business and risk activities
- Development of new technologies
- Increasing regulatory requirements

Addressing these external trends and events has meant routinely changing strategic priorities. If risk management activities fail to keep pace, associated efforts can become reactive, misaligned and compliance-focused rather than supportive of strategic decision-making. Boards should encourage management to build risk capabilities aligned with strategy.

Start the risk conversation with strategies and goals

Strategic risks often account for corporate failures. Yet ERM programs are typically not integrated with strategic decision-making and planning. Risk-based strategy alignment provides a structured approach so that risks and mitigation are key elements in strategy discussions.

Should ERM and the corporate strategy function be put together? Leading companies leverage risk management as a strategic tool, viewing risks not only as threats but as strategic opportunities. Some companies have chosen to emphasize this through their organizational structure, by increasing the collaboration between the corporate strategy and risk management functions. This may or may not be the route your company wants to take, but starting with a strategic focus can help leadership figure out where it should be placed, how to organize ERM and who has the right capabilities to lead the effort.

Position risks within the context of the organization's strategic priorities

In identifying risks, organizations must look beyond traditional siloed categories. Management should identify the key risks for each of the organization's strategic priorities or challenges. This creates a direct line of sight between performance targets and the risks that must be managed to achieve them. When reporting risks to the board, management can list the risks beside the relevant strategic objective so the board can see each risk's relevance to the performance of the strategy. This simple approach not only can improve the overall likelihood of the strategy's success but could identify gaps in risk management.

Example risk profile

Risks can be reported alongside the company's key objectives. As a result, risks are positioned within the context of the organization's strategic plan.

Rank	Risk		Business priorities						
		# of priorities impacted by the risk	Reduce costs by 12%	Employee retention	Expand into three new markets	SAP implementation	Increase revenues by 15%	Employee health and safety	Sufficient capital to support growth
Risk profile for each priority			Medium	High	High	Medium	High	Medium	Medium
1	Can't attract skilled resources	4	x		x	x	x		
2	Lowered analyst rating	3			x	x			x
3	Major contractor cost increase	3	x		x	x			
4	Significant increase in interest rates	3			x		x		x
5	Access to capital declines	5		x	x	x	x		x
6	Environmental incident	4	x		x		x	x	
7	Loss of information to cyber intrusion	6	x	x	x		x	x	x
8	Loss of key business facility	2			x		x		
9	Negative change in compliance requirements	4	x		x		x		x
10	Loss of resources to competitors	5	x	x	x	x	x		
# of risks related to each priority			6	3	10	5	8	2	5

High Medium Low

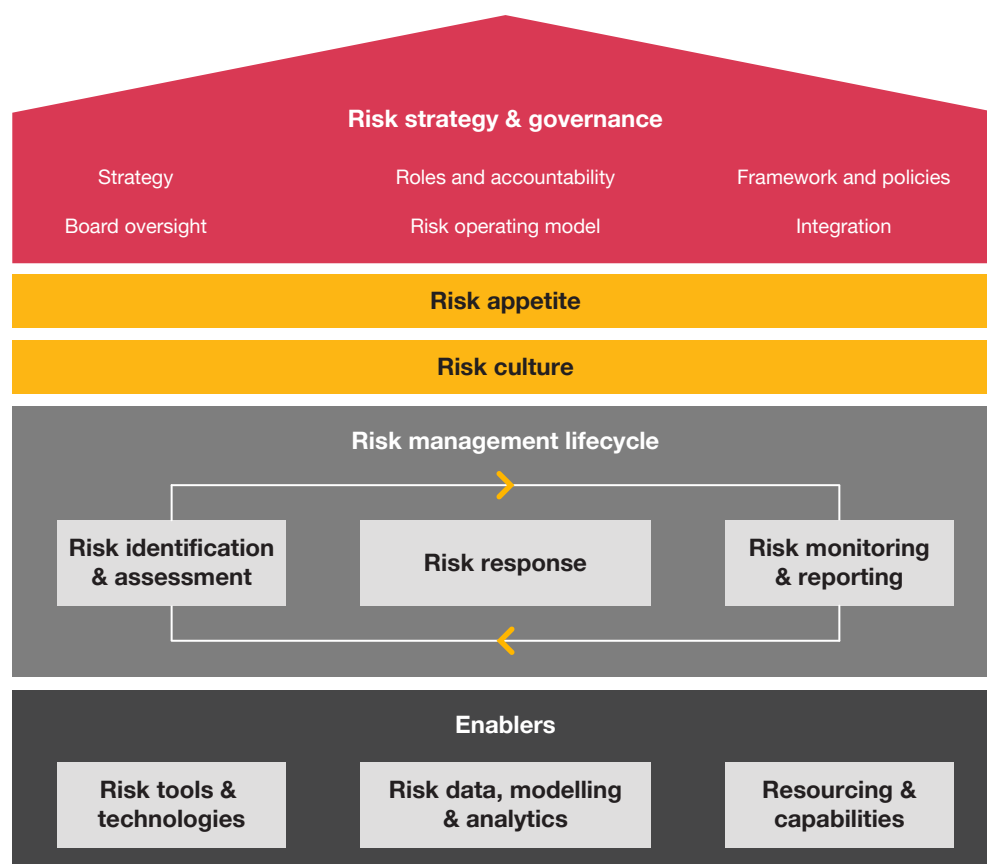
2. Risk strategy and governance: driving clarity for managing and overseeing risk

Having a written charter or plan takes a concrete step towards a commitment to action; it is critical to ERM program development and survival. *A charter or plan is a good first step...BUT if you want to really advance your program, you need a risk strategy and governance framework.* A risk strategy and governance framework provides guidance and structure to business units, executive management and the board in the identification, assessment and monitoring of business risk. At its most basic, the framework — often reviewed and approved by the board — should incorporate:

- ERM program objectives
- Metrics for tracking ERM program success
- Risk governance and reporting structure, including board oversight and allocation
- Clearly defined risk management roles, responsibilities and authorities, from the board through functional leaders
- An operating model that includes resources (internal and external) and processes that will support ERM program objectives

Example ERM framework

Not all companies will have a robust ERM framework given their program's level of maturity. But a goal can be evolving it over time.



Understand roles and responsibilities

The board needs a strong understanding of risk management and oversight roles and responsibilities to prevent finger-pointing and confusion. Along with a clear sense of its own risk oversight role, the board should be knowledgeable of executive management and risk owner responsibilities in order to hold the right people accountable.

Should someone be looking at risk management efforts across the organization?

Regulated and unregulated companies are increasingly using a chief risk officer or other senior executive to oversee the risk management function and to coordinate the risk management program across the enterprise. This may become more popular due to the evolving nature of SEC disclosures. Let's use cyber risk as an example. With the SEC's new cyber disclosure rule, companies must disclose whether cybersecurity is part of the overall risk management program. This highlights a greater need to consider a single risk leader with ownership of enterprise-wide risk, making sure that these discrete risk areas — like cyber — are being integrated into the overall enterprise risk management program.

This person normally reports to the CEO, with a dotted line to the board's audit or risk committee, though some organizations put the role under the CFO or general counsel. What is most important is that the risk leader has sufficient stature and credibility to effectively influence others.



Only

17%

of companies in the S&P 500
have a formal chief risk officer

62%

of those companies
are in financial services

Source: BoardEx, as of August 17, 2023.

Oversight of ERM



Board roles and responsibilities

- Review and approve company strategies, objectives and related risk profile
- Through discussions with management, understand the company's top risks, risk-return tradeoffs, emerging risks and interrelated risks
- Determine whether management is taking the appropriate risk management actions
- Confirm the board's committee structure and oversight processes enable effective oversight for top risks
- Empower one committee, typically audit or risk, to oversee management's progress in the design and operation of risk management
- Review and approve the company's overall risk appetite and risk policies



Board committee roles and responsibilities

- Provide risk management program oversight on the full board's behalf
- Review risk management reports quarterly, examining risk prioritization, risk plans and risk management program progress
- Review and approve risk management program design, and assess risk management program performance versus company goals, policies and procedures as well as industry practices
- Request that additional risk assessments be conducted as needed
- Report risk management program activities and progress to the full board annually or as deemed appropriate



Questions the board should ask management:

- Does management have a risk strategy and governance framework?
- How does the ERM process align with strategic planning and decision-making?
- What forum does senior management use to talk about risk? Is there a management-level risk committee? Who is on this committee? What is the committee responsible for?
- How does ERM coordinate and collaborate with the various business units and corporate functions across the three lines? How are control and assurance functions aligned and working together?
- How are roles and responsibilities communicated? What kind of training is in place to implement the governance framework?

3. A common risk language: promoting a consistent view of risk

For successful implementation of an ERM program, leaders should also institute a common risk language across all levels of the organization. This creates a single version of the truth and a consistent view of risk. Boards should look for standardization in the company's risk management terms and processes.

Create a common risk language and approach



Risk management terminology.

Arguably, traditional risk jargon — risks, risk causes, risk consequences, risk impact and likelihood, risk exposure, management capability — has contributed to a sense that it's separate from strategy and operations. Many risk executives are aiming to drive acceptance of ERM practices and better understanding of risk information by dropping the specialized terminology. What's important is that all parts of the business, including the board, are speaking the same language. This should include clear and concise risk management definitions that are easy to understand and interpret.



Risk taxonomy. The categories used to describe the company's risks should be as specific to the company as possible, establishing a comprehensive, common and stable set of risk categories that are then used to classify and aggregate risk. The risk taxonomy supports a common understanding and communication of risks, helping to focus ongoing risk monitoring and reporting and enable better insights from risk data. You may also hear this called a risk register, inventory or universe - but what's important is that the organization has a way to categorize different risk types into logical groupings. These categories could include strategic, operational, financial and compliance as well as emerging categories such as sustainability.



Risk management approach. To support the company's risk governance framework, management should put forth a clear and documented methodology for managing risk. This often includes the standards and processes for identifying, prioritizing, managing, monitoring and reporting risk across the organization.

Having a standard terminology, categorization and approach to risk management makes it easier to accurately combine risk information across the business and spot discrepancies and interdependencies. Otherwise management and the board may find it challenging to connect the dots between risks and understand their cumulative impact.

4. Enterprise risk assessment: helping senior leadership and the board prioritize risk

Many companies see a simple enterprise risk assessment as the end product of the risk management process; however, it's only one aspect of ERM. One of the most important elements in the risk assessment process is the prioritization of risks and the analysis of capabilities in order to drive the development of risk-based strategies and response plans.

Focus on the risks that matter the most

The board can't possibly oversee *all* risks, and an effective prioritization process can help directors focus their efforts. Management's criteria for prioritizing risks should reflect a combination of financial, operational, reputational and other industry-specific impact factors relevant to meeting strategic objectives, as well as an analysis of current capabilities to manage the risk. The criteria, when applied, should result in no more than 10 to 15 risks being ranked high enough to deserve executive and board attention. The management and oversight of these risks should be treated as critical to achieving the company's strategic objectives.

Continuously assess risk

Let's face it: Few of us can remember what we were working on at this time last year. Performing ERM program activities — including the enterprise risk assessment — once a year is simply not enough to maintain strong and up-to-date information in a manner that supports strategic decision-making. Boards should consider management's process for continuously reviewing the risk landscape as well as assessing emerging risks so that the company can still reach its strategic objectives. In other words, the board has a responsibility to make sure that ERM is built into the rhythm of the business.



Questions the board should ask management:

- What is the process for categorizing and assessing the company's risks? Is it a balance of top down and bottoms up? How do leaders integrate the various risk assessments conducted across the company?
- At the center, does someone understand how risks aggregate? How is the information consolidated and analyzed for interconnectivity?
- What is the company's process for identifying the top risks for reporting to the board? What are the criteria used?
- Is the risk assessment process continuous? How do leaders keep abreast of the changing risk environment? How do they monitor emerging risks?
- Are there risks in the company's inventory that do not tie to the strategy or risk profile? Should the company be tracking such risks?

5. Risk response plans: managing prioritized risks

The output of a risk assessment process is often a risk response plan — a plan that details the company's actions in mitigating risk issues. Plans should clearly articulate the risks, underlying causes, potential consequences and interrelated risks, along with how they relate to strategic objectives and current initiatives (see Appendix A). This baseline of information is critical to choosing the appropriate time-bound steps to effectively manage the risk and support additional risk analysis. The risk's materiality will determine the appropriate risk management approach, with more resources allocated to higher risks.

Build risk management accountability

The board and management should review risk response status reports with the same frequency that they review corporate performance. If risks are tied to strategic objectives, it makes sense to review risk responses at the same time.



6. Ongoing monitoring: recognizing changes in risk

Establish a risk appetite and key risk indicators

One of the most common and effective forms of ongoing monitoring is done through the development of a risk appetite framework and a set of key risk indicators. Risk appetite defines the level of risk an organization is willing to accept in pursuit of its strategic objectives; it sets the boundaries within which risks should be managed. Key risk indicators are measurable metrics that help monitor and assess the level of risk within predefined thresholds. Indicators act as early warning signs, highlighting potential deviations from the risk appetite and helping enable timely actions.



The board's role in overseeing the management of risk

The board plays a critical role in overseeing risk management and ongoing monitoring. Its responsibilities include:

- **Challenging risk appetite.** Executive management may establish the organization's risk appetite, but the board plays a critical role in challenging the risk appetite and its alignment with strategy and stakeholder expectations.
- **Monitoring risk.** The board should make sure that management has systems in place for ongoing monitoring. This involves reviewing periodic risk reports, assessing risk indicators and monitoring risk exposures against established tolerances. The board should also receive regular updates on emerging risks, potential impacts and mitigation strategies. (See Appendix B for a few examples of risk reporting dashboards.)



Questions the board should ask management:

- What is our risk appetite? How are key risk indicators defined, measured and monitored?
- How are the company's risk response plans monitored and assessed for effectiveness? How are minimum requirements for key controls and assurance determined? Do response plans include time-bound actions with assigned risk owners?
- Who is accountable for the most material risks, and what are the guardrails for managing them?
- How is the output of ERM being vetted with senior leaders and the board?
- What mechanisms are in place for ongoing monitoring and reporting of risk?

Conclusion: supporting management in the company's ERM journey

To adequately discharge their risk oversight responsibilities, boards need to understand the foundational ERM elements and where they can make a difference in supporting management in the company's ERM journey:

Enterprise. Aligning risk management with the enterprise-wide strategy, and creating a risk governance structure to oversee enterprise-wide risks.

Risk. Creating a common risk terminology, categorization and process so that the company has the same understanding of risk and the company's risk approach.

Management. Building risk management accountability through risk response plans, and establishing management guardrails through a company's risk appetite and key risk indicators to promote ongoing monitoring.

Leaders shouldn't take a one-size-fits-all approach to ERM though — the process must align with the company's culture, size and complexity. As your company's ERM program matures, the board can promote continuous improvement by challenging management on what is working and what is not.

Related content:


[*Risk oversight and the board: Navigating the evolving terrain*](#)

[*2023 US Risk Perspectives Survey*](#)

[*Risk: See it, share it, sort it*](#)

Appendix A: Example risk response plan template

1. Risk name

Risk owner	Rating	Current risk	Target risk
Description		VH	H
Risk appetite	Action	Remediate	

Causes	Action(s)	Status	Owner	Due date
Implications/impact				

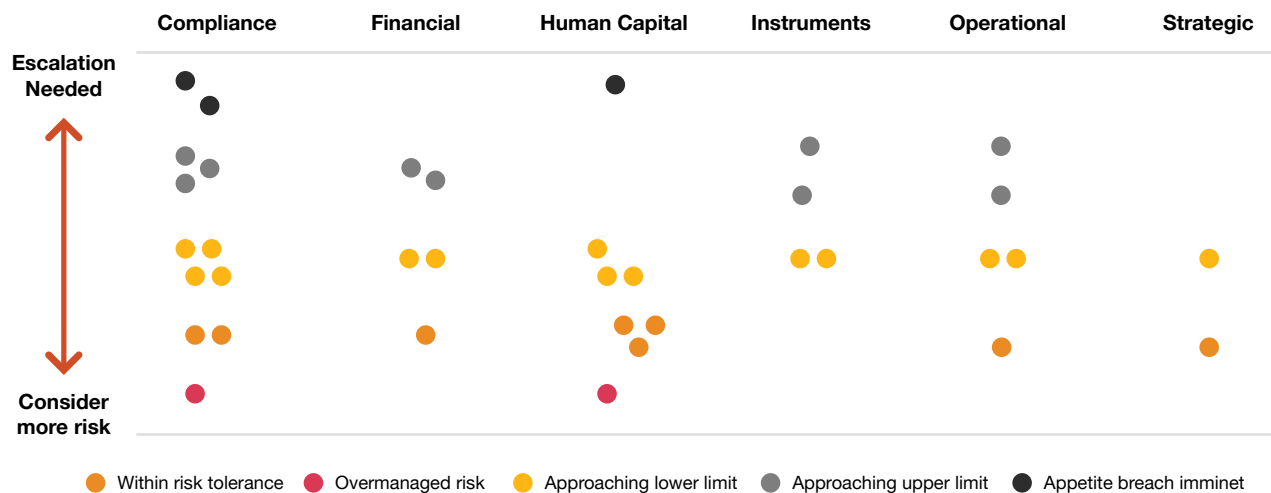
Key decisions required on this risk	[Insert further comments]
-------------------------------------	---------------------------



Appendix B: Risk reporting dashboard examples

Risk reporting dashboard – Example 1

The dashboard below displays how individual risks within each risk stripe are performing against their limits and conveys to management whether escalation protocols should be implemented or if certain risks are too conservative.



Risk reporting dashboard – Example 2

The dashboard below is a sample of what can be created to help continuously monitor risks against their set limits and provide management with timely warnings before a potential breach.

Metric name	Lower limit	Upper limit	Current month	Prior month	Trend	Action required
Operational risk						
System outages	2	5	0	1	✓	No
Operational Risk Events (ORE)	2	7	1	1	—	No
Operational losses (\$)	\$1.6K	\$2K	\$1.2K	\$1.5K	✓	No
Operational loss events (#)	3	7	1	2	✓	No
Fraud loss (\$)	\$118K	\$148K	\$20K	\$0	^	No
Fraud loss (#)	2	3	1	0	^	No
Data privacy incidents	1	3	0	0	—	No
Compliance risk						
Complaints (#)	5	10	9	5	^	Yes
Past due IA MAPs (#)	3	8	0	0	—	No
Past due compliance monitoring and testing MAPs (#)	1	4	0	1	✓	No



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.

Contacts

Maria Castañón Moats

Leader, Governance Insights Center, PwC US
maria.castanon.moats@pwc.com

Brian Schwartz

Principal, Cyber, Risk and Regulatory, PwC US
brian.schwartz@pwc.com

Lillian M. Borsa

Principal, Governance Insights Center, PwC US
lillian.m.borsa@pwc.com

Carin Robinson

Director, Governance Insights Center, PwC US
carin.l.robinson@pwc.com

Catie Hall

Director, Governance Insights Center, PwC US
catherine.hall@pwc.com

Katee Puterbaugh

Director, Cyber, Risk and Regulatory, PwC US
katee.puterbaugh@pwc.com