



April 2017

How your board can ensure enterprise risk management connects with strategy

Any major strategic decision carries uncertainty. A well-developed enterprise risk management (ERM) program can help executives meet key business objectives.

Good risk management doesn't happen overnight. Management teams often struggle to get it right. Boards can play a key role encouraging executives to shore up risk management practices in their companies. But first you need to know what signs to look for that indicate ERM may be falling short.





Spotlight on enterprise risk management

Every company has to manage risk, but some do it better than others. The companies that excel don't do it by chance—they work to understand the risks they're taking and everyone in the company

understands the role they need to play. As a company becomes more complex, that gets harder. This paper looks at how boards can figure out whether their company has effective enterprise risk management.¹

Key challenges directors face when overseeing ERM:



How can directors know if ERM is adding value?



Board action: Dig into how well ERM works and whether changes should be made.



How can the board ensure that executives take their responsibility for risk seriously?



Board action: Discuss with senior management how they have put ERM into practice, including who's accountable for key risks and how ERM works at lower levels in the company.



How can the board better understand what risks may emerge in the future?



Board action: Push executives for regular forward-looking, strategic input on emerging risks.



How can the board get the reporting it really needs on risk?



Board action: Be clear on the kind of risk information you need from management and how often you want to see it.

¹ In another module in this series, *Why your board should refocus on key risks*, we cover how boards can improve how they oversee individual key risks.



Challenge: How can directors know if ERM is adding value?

“ERM” means different things to different people. Some companies simply use ERM to identify, prioritize and report on risks—*protecting value*. The best companies use ERM to make better decisions, improve their strategic, financial and operational performance and *create value*. But it takes work and buy-in at all levels to make that happen.

What ERM is—and isn’t

ERM is the collection of capabilities, culture, processes and practices that helps companies make better decisions as they face uncertainty. It gives employees a framework and policies to help them understand, identify, assess and manage risks so the company can meet its objectives. It’s most valuable when it’s integrated with strategic planning.

Just assessing risk—identifying and prioritizing the key risks—isn’t ERM. If a company stops there, it may know about risk, but that’s not the same as taking an active approach to manage it.

Good ERM doesn’t happen overnight. It takes time to create a suitable risk management framework. It then takes buy-in throughout the company. For companies where this works well, it becomes part of their culture. Every time they consider new opportunities, they also make the connection to how they would manage the risks. ERM should also look at whether the company is taking enough risk and focus on areas of overperformance as much as poor performance.










The best ERM programs allow companies to have both risk agility (can you quickly adapt to a changing environment?) and risk resilience (can you withstand business disruption?). And companies that are committed to effective ERM

programs periodically assess how they can be further improved. It's not easy to get ERM right. Only 52% of the over 600 respondents to our *2016 Risk in review: Going the distance* survey rate their US headquartered companies highly in both risk agility and risk resiliency categories.²

Signs that management could improve the way it addresses ERM

<i>Symptoms</i>	<i>Possible causes</i>
 <p>Your strategy discussions focus only on opportunity without mentioning risk.</p>	<ul style="list-style-type: none">• Risk isn't an integral part of strategy development.• Management isn't giving the board the full picture.
 <p>You get a laundry list of risks—no analysis, no connection to the company's strategic objectives.</p>	<ul style="list-style-type: none">• Management views ERM as a compliance exercise.• ERM is seen as just an annual risk self-assessment survey.
 <p>There's a heavy focus on easily understood and discrete risks—such as financial reporting, compliance and/or operational risks.</p>	<ul style="list-style-type: none">• Management is identifying risks from the bottom up, not linking them to strategy.• Risk management may be focused in the wrong areas or simply not reporting the right information to the board.
 <p>ERM doesn't have visibility or credibility at the board or senior management level.</p>	<ul style="list-style-type: none">• The individual leading ERM doesn't have the clout to get meaningful input or buy-in from senior executives.• The chief executive officer doesn't value ERM.
 <p>ERM discussions feel stale—covering the same risks every year.</p>	<ul style="list-style-type: none">• ERM isn't challenging management to understand what's changed and what's ahead.

² Certain sectors, like Healthcare Providers and Automotive rank highest in risk agility and risk resilience.



Board action: Dig into how well ERM works and whether changes should be made.

Why is effective ERM important? It gives the board—and management—a basis for understanding what could prevent the company from achieving its strategic and business objectives.

What does good ERM look like?

Good risk management can sound like motherhood and apple pie, but it's often tough to gauge its effectiveness. Here are some signs to look for:

- A shared understanding of how much risk the company wishes to take (risk appetite)
- A common risk language so everyone understands what different types of risks mean
- ERM is connected to strategy development
- Working communication channels—the ability to elevate risks without fear of reprisals (don't kill the messenger)
- Business unit leaders who are accountable for managing their own risks
- Coordination between ERM and other important assurance functions like compliance and internal audit
- Key performance indicators (KPIs) that link to key risk indicators (KRIs)
- Risk management practices are baked into how the company does business
- Discussions about what's coming (emerging risks)

Good ERM starts at the top of the company, then quickly becomes part of how everyone thinks and treats the risks they face in their day-to-day work.

How common are these elements at US companies?



Source: US headquartered companies in our Risk in Review study, representing over 600 responses.



Properly done,³ ERM identifies the key risks that could stand in the way and ensures they're (a) communicated to the stakeholders who need to know and (b) managed appropriately. But ERM looks and feels different at every company, so how can directors know if it's working at their company?

Ask the ERM leader (often the chief risk officer, or CRO) how much time the risk group spends helping the business fix operational processes. If it's a great deal, push to have ERM refocus on strategic goals. The best CROs are senior executives who understand the company well and are trusted by a wide network of colleagues.

If there is no separate executive-level officer responsible for risk, discuss whether the board believes adding one would help. Starting from a strategic focus can help management figure out how to organize ERM and who's the right person to lead the effort.

Finally, if the board isn't confident the company is handling ERM right, directors can suggest that management engage an outside advisor to help get it right.

What CROs typically do—and don't do

☑ Do

- Establish the framework for ERM, including approach and standards
- Help craft risk appetite
- Create tools for company personnel to use
- Train employees on risk and build a network of risk-skilled executives throughout the company
- Help pull together an aggregated view of risk across the company
- Alert senior management when risks are outside the desired limits
- Report on risk-taking to senior management and the board
- Monitor risk on an ongoing basis
- Challenge business leaders' periodic risk assessments

☒ Don't:

- Own or manage risk themselves

Note that the CRO role in financial services companies also has other dimensions. For example, many CROs are involved in establishing risk limits.

³ The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has published an ERM Framework. An updated Framework is due in 2017.



Challenge: How can the board ensure that executives take their responsibility for risk seriously?

A company can't manage risk if employees and managers don't accept they are accountable. Risk ownership is all about who has the authority to take risks. While senior executives own key strategic risks, there are risk owners at all levels. For instance, the head of Environment, Health and Safety may "own" safety risks, but a plant manager is responsible for safety within the plant.

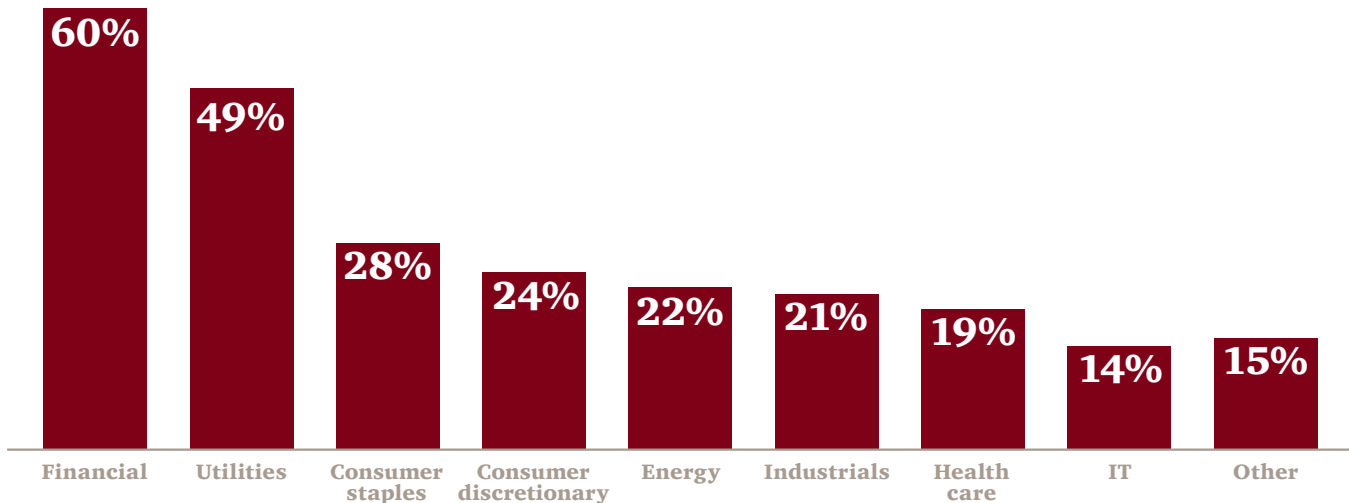
While it seems simple, it's often unclear who is, or should be, responsible. If ERM lives only at the

executive level and nowhere else, it's not going to influence everyone's behavior.

Some management teams think they are managing risks just fine and simply don't see the point of adding another oversight function. Overall, only 31% of companies have an executive level officer solely dedicated to monitoring risk.⁴ Large US-based financial services companies are required to have an experienced CRO with specifically mandated duties, and many smaller financial services companies are also adopting this model.

Apart from highly regulated industries, few companies have CROs

Use of an executive-level risk officer by industry



Source: NACD, 2015-2016 Public Company Governance Survey, 2015

⁴ NACD, 2015-2016 Public Company Governance Survey, 2015.



Board action: *Discuss with senior management how they have put ERM into practice, including who's accountable for key risks and how ERM works at lower levels in the company.*

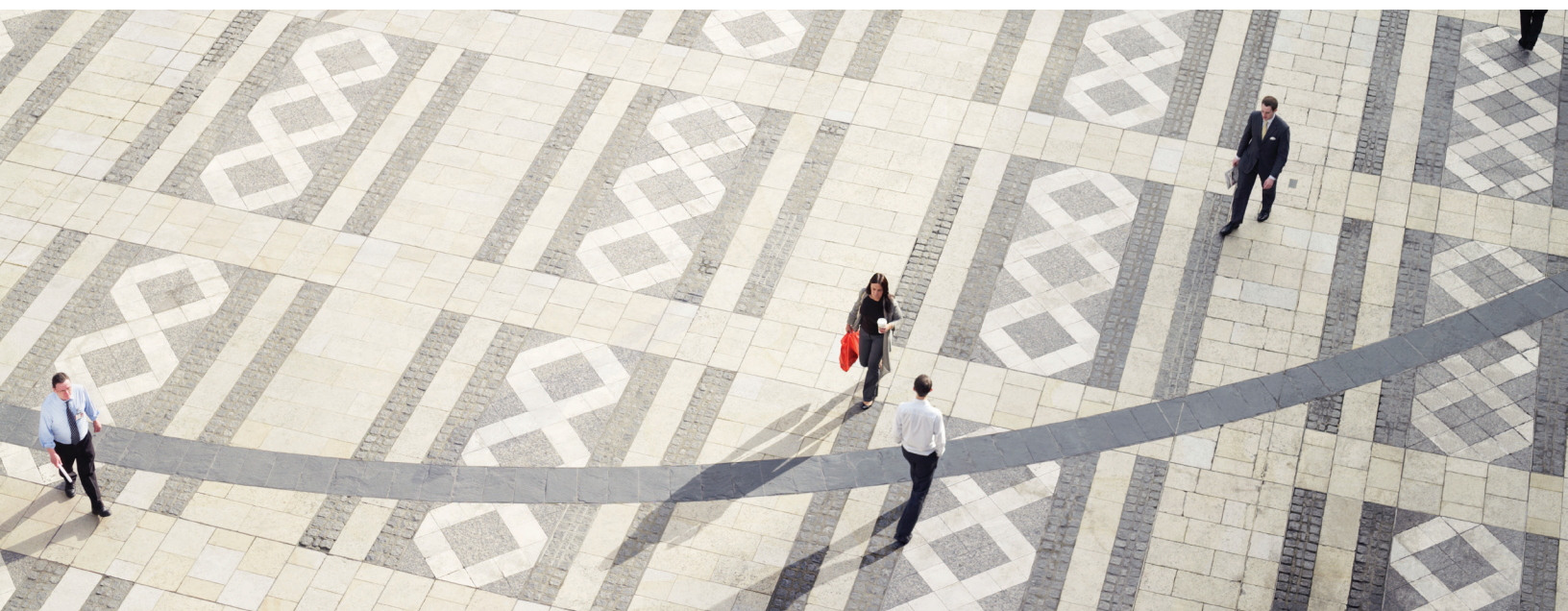
The CEO is ultimately responsible for risk. Since the CEO can't be present when many decisions are made, it's vital that there's a healthy culture throughout the company. That will support managers and employees in raising risks along with opportunities. Who else is critical?

Senior management: To be effective, ERM needs to work hand-in-hand with strategy to help executives set objectives and make sure that the risks are managed to meet those goals. Directors should ask about the relationship between risk management and strategy to understand how they influence each other. Challenge senior

management on how current and emerging risks impact strategy execution. Such discussions may help management, as well as the board, better understand key areas of risk.

Business unit management: Discuss the risks they've taken or avoided. This can be far more effective and engaging than simply discussing a long list of risks. Even better? If they don't already, encourage managers from different businesses and functions to meet, discuss risks and consider diverse perspectives. These kinds of discussions can help the company identify emerging risks that a once-a-year risk review may miss.

The board's interaction with business unit managers will also help directors understand whether these executives behave as if they own the risks. A robust discussion ought to include strategic risks or disruptors that can prevent that unit from meeting its goals.





If the company has a CRO, find out how he or she works with executives to promote good risk management throughout the business. A CRO is in the right position to spot and share good risk practices across different business lines.

Many companies have an executive-level risk management committee. Understand how frequently it meets and how robust the agendas are. How are the risk management committee decisions and information shared in the company? Are there channels to escalate risks as well as risk information coming from the top of the house? Who's responsible for prioritizing risks? What role does the CRO, if any, play in the committee? If such a committee doesn't exist, ask how risk gets covered on senior leadership's agenda.

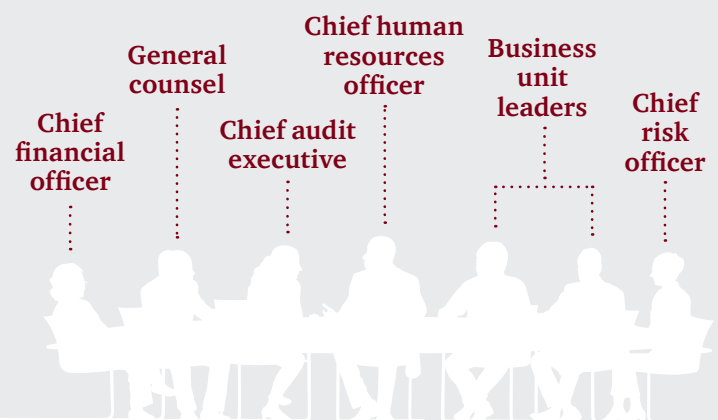
Some boards do “deep dives” on key risks with the executives responsible for those risks. That's a great time to ask them what they find useful and what else—like tools or sharing best practices—would be valuable to get from ERM. It's also a great time to find out how they embed good risk management practices throughout their businesses. And it's an opportunity to understand if they're managing risk and performance together, given individual risks can impact multiple objectives.

Finally, talking to employees outside of the C-suite can provide a sense of how they view and manage risks and what they know about ERM.

Who should be on an executive-level risk management committee?

At some companies, the CEO and his or her direct reports make up this group. Other risk committees deliberately don't include the CEO to avoid possible group-think.

Risk committees generally include:



Depending on the company, other key executives may be part of the committee, such as a chief operations officer. Another option is to regularly convene a group of executives one level down from the C-suite.



Challenge: How can the board better understand what risks may emerge in the future?

Everyone wants to know what's next. No one can predict the future, but effective ERM can prod management to envision what different risks might emerge that could affect the business. Nearly three-quarters of respondents to PwC's *2016 Annual Corporate Directors Survey* say strategic/disruptive risks are among the toughest to oversee. Only 41% rate their board as performing very well at addressing longer-term risks.

It's always easier to consider known risks and what's familiar. If that's ERM's default way to operate, the company is likely to miss opportunities. But boards and senior leaders need to look beyond this quarter or this year to craft the right strategy and take the right bets. While ERM and senior management are unlikely to predict the next "black swan" event (essentially something so unprecedented that it's not on anyone's radar), robust ERM sets the stage to shine a light on disruptive technology, new competitors, and changes in regulations, economics or the political landscape.



Board action: Push executives for regular forward-looking, strategic input on emerging risks.

If you haven't already, tell the CRO or the executive responsible for ERM you want a more strategic focus that includes expanding the risk horizon. Insist that management inform you about potential upcoming risks. The annual risk assessment should encompass emerging risks to help the company focus on future risks with strategic impact.

Including ERM in strategy development brings a risk lens to the process. ERM can help business leaders develop key risk indicators to show when certain scenarios may be playing out and how to manage the risks. Input from several internal and external sources can help executives and the CRO think more broadly to develop a list of possible emerging risks. ERM can also help draw executives' attention to changes in the business context or changes in assumptions that underpin the strategy. Both are key sources of emerging risks.

It may be a stretch to think about future risks, but that's exactly the input you need from ERM.



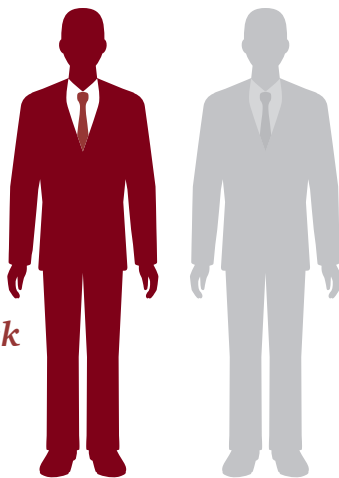
Challenge: How can the board get the reporting it really needs on risk?

Some boards just aren't getting the risk information they need, and frankly, at times don't even know what to ask for. Some are snowed under by risk minutiae, while others struggle to get a sense if management understands the big picture when it comes to risks.

In part, this may stem from management not having robust information itself. Some companies lack governance, risk and compliance (GRC) tools that would allow them to provide sophisticated risk reporting. And so many companies are still cobbling together spreadsheets and narratives to try to compile a full picture of their risks.

And, if ERM reports look suspiciously like they are re-hashing old or known risk information, then ERM is missing the boat.

Only 1 in 2 directors say their board performs very well at ensuring management reporting to the board related to risk is informative and at the appropriate level of detail.



Board action: *Be clear on the kind of risk information you need from management and how often you want to see it.*

It's up to the board to decide what it needs to oversee risk effectively and communicate that to management. And it's up to management to provide a list of key risks and how they could impact strategy. If the board doesn't get useful insights from the reports they are getting now, let management know. It's one thing to know there is a risk management process in the company and another to understand how decisions are made in the face of multiple risks.

How frequently should a board get risk reporting? Ideally risk discussions happen at the same time (and so, with the same frequency) as performance discussions. But some boards use other approaches. For some risks, the board is satisfied with a yearly report. For other, more dynamic risks, the board may want to see reports and speak to the executive risk owner twice a year or more.

Source: PwC, 2016 Annual Corporate Directors Survey, October 2016.



In conclusion...

Directors can have crucial influence on a company's ERM program. If ERM exists in the company, it's important to know how risk management is structured and how risk information flows. If there is no ERM, find out why not and how putting it in place might benefit the company.

It's helpful to gauge the value that ERM brings to the company, but it's especially important to know the value it brings to the board for strategy and risk oversight. If ERM is stuck in weeds of day-to-day operating risks, the CRO is unlikely to lift his or her head high enough to think about future risks to the company. And given the complexity of how risks can offset or magnify each other, directors need to understand that context to recognize how strategy is affected.

Done right, ERM both protects value and adds value as it helps companies look ahead, anticipate key risks and make better strategic bets.

Contacts

For more information about the topics in this publication, please contact any of the following individuals.

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

Dennis Chesley

Global Risk and Regulatory
Consulting Leader
(202) 730 8036
dennis.l.chesley@pwc.com

Jason Pett

Risk Assurance US Internal Audit,
Compliance and Risk Management
Solutions Leader
(410) 659 3380
jason.pett@pwc.com

Stephen Zawoyski

Partner, Risk Assurance Solutions - ERM
(612) 596 4931
stephen.v.zawoyski@pwc.com

*Project team***Karen Bissell**

Marketing Manager
Governance Insights Center

Nick Bochna

Project Team Specialist
Governance Insights Center

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 decide if it needs a risk committee*
- *Why your board should refocus on key risks*
- *How your board can be ready for crisis*

www.pwc.com/us/GovernanceInsightsCenter

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

©2017 PricewaterhouseCoopers LLP. All rights reserved. PwC refers to the United States 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. 270261-2017