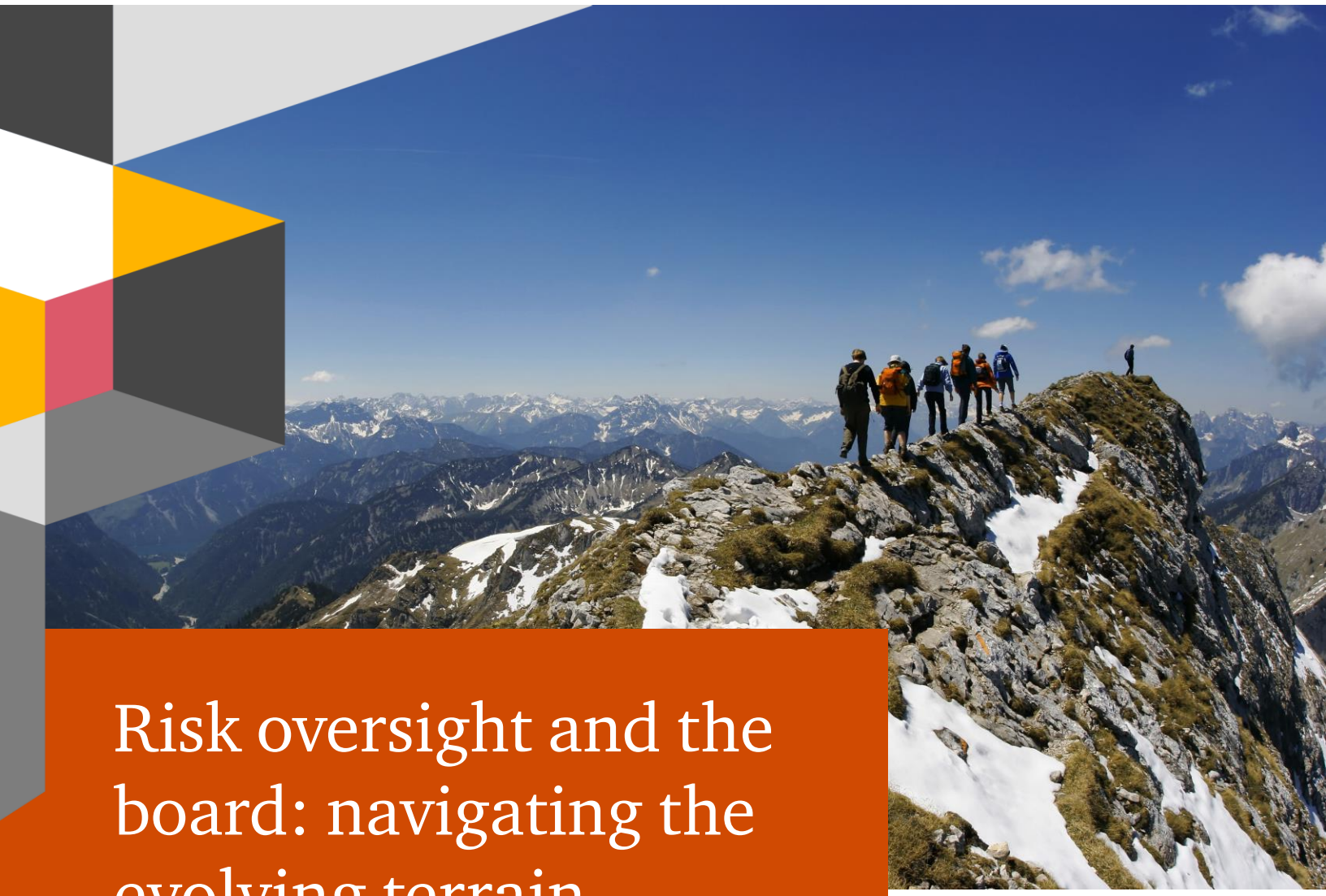
August 2022



Risk oversight and the board: navigating the evolving terrain

Robust and active risk management oversight at the board level is more important now than ever before.

The board's risk oversight role is a critical one. It can bring tangible value to a company and its shareholders both in times of crisis and when things are just business as usual. It starts with understanding the strategic direction of the company and considering the broader stakeholder perspectives and competitive landscape. How does your board define its approach to risk oversight, and how does it put that oversight into action?

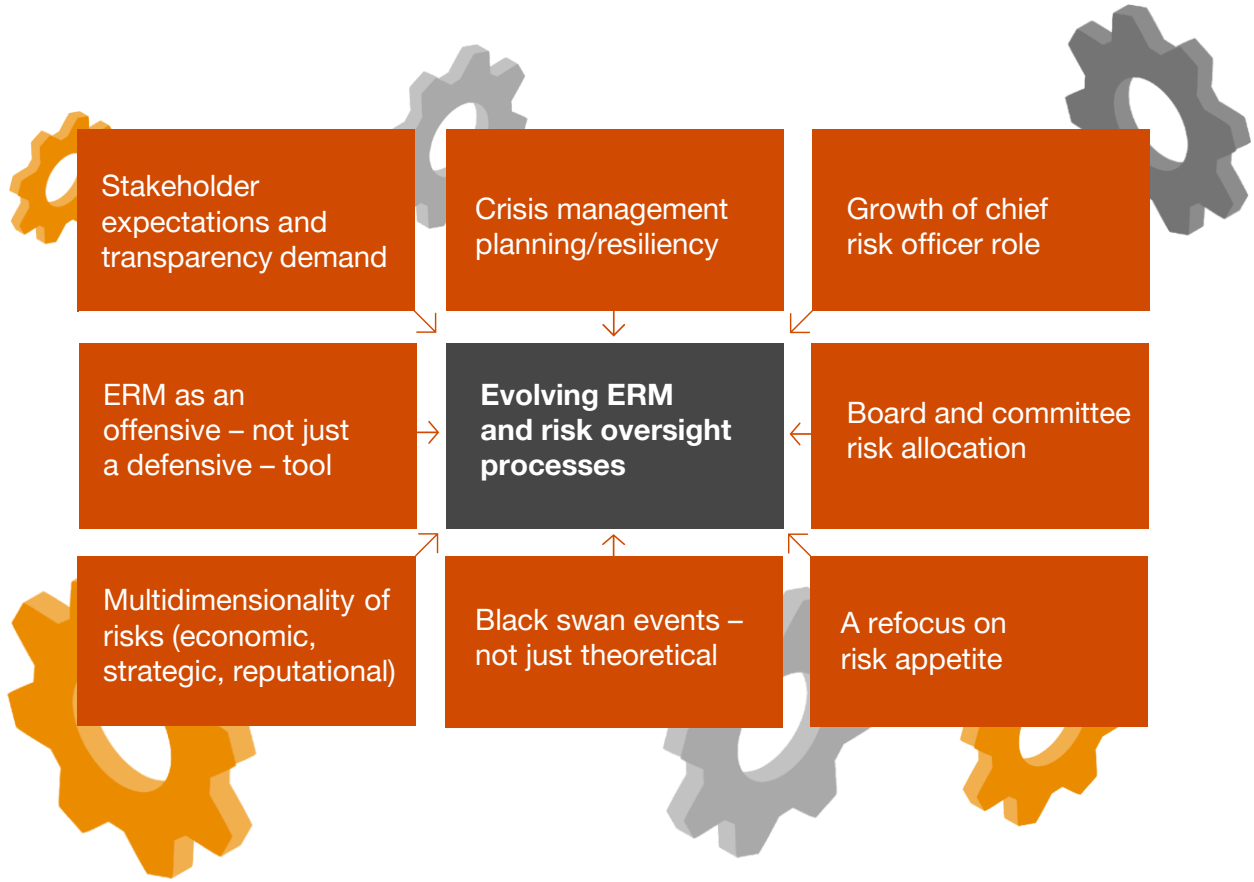
pwc

We're living in an era of unforeseen events that give rise to risks, including geographic conflicts and a "black swan" event—something so unpredictable that it's not on anyone's radar—a global pandemic with far-reaching economic and social consequences. While a company can't always anticipate what might be around the corner, strong risk oversight by the board can help the company respond with more rigor and agility. The number and types of risks the board oversees continue to grow, even as their nature changes. Some become more likely as businesses are more interconnected. Some are likely to impact just a certain area of the business. Others could severely impact the entire brand.

The last few years have reinforced the need for companies to recognize the possibility of what once seemed like unlikely events. How can organizations and their boards use this lesson to improve their risk oversight processes? Keeping an open, yet skeptical, mind is a big piece of it. Given the collective experience of most boards—and the fact that directors sit outside of the day-to-day running of the business—they are well-suited to bring this open-mindedness and willingness to explore the "what-if" scenarios. Taking a long view on risks aligned to the strategic plan at the board level allows company leadership to focus on the day-to-day management of those risks.

The evolution of ERM

ERM has always been about identifying and managing the top risks to the organization. That hasn't changed. The inputs, the methodology, the output, and the overall process have—because they had to. As depicted below, there are several drivers for the evolution of ERM and risk oversight processes.



The link between strategy and risk

Large institutional investors have been pushing for more information about how a company's statement of purpose is linked to its long-term strategy and success. With this growing external focus on strategy, boards should understand how their company's purpose informs its processes to both identify risk and determine the company's risk appetite. The company's risks and risk appetite should be viewed not only from the company's perspective, but also from the perspective of shareholders and other stakeholders (e.g., employees, customers, suppliers, communities, and regulators).

Let's use ESG risks to illustrate this. For many companies, these risks were already on their radar—somewhere. But the recent focus by large institutional investors, combined with an increase in shareholder proposals seeking disclosure, have brought these risks to the forefront. Large institutional investors are suggesting that ESG risks could have an impact on the long-term sustainable value of the company. For example, perhaps the company relies on water as a key resource. Due to climate change, sourcing that water in the future might be a challenge, which will ultimately affect the long-term value of the company. Companies are now more focused on identifying material ESG risks of this type, monitoring and overseeing those risks, and communicating their efforts to shareholders and other stakeholders.

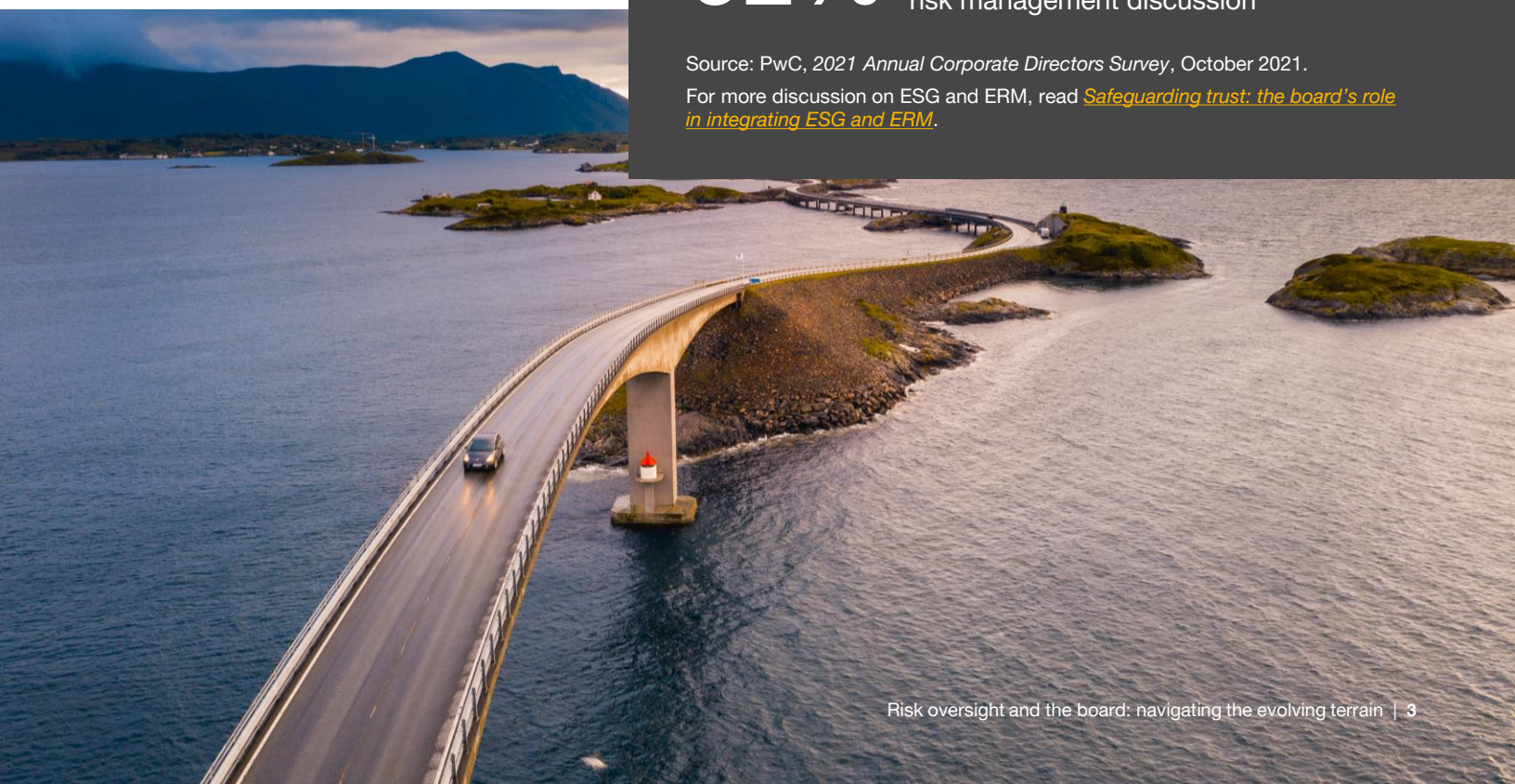
The board needs to focus on which key business risks are actively tracked and monitored at all levels, including at the board level. They can add real value by stepping back and asking about what risks might be missing and what risks may not be fully appreciated.

Room for improvement in ESG discussions

62% Only 62% of directors say their boards discuss ESG as part of the enterprise risk management discussion

Source: PwC, *2021 Annual Corporate Directors Survey*, October 2021.

For more discussion on ESG and ERM, read *Safeguarding trust: the board's role in integrating ESG and ERM*.

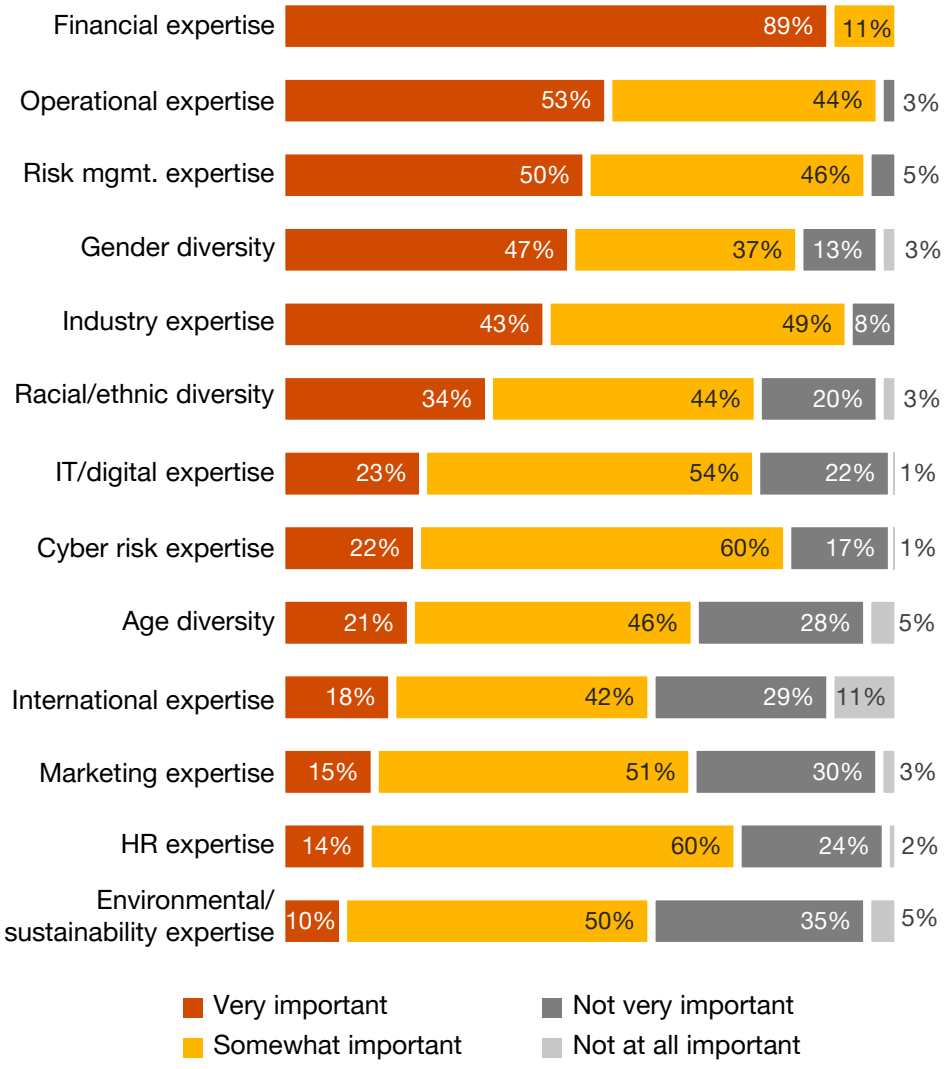


First things first: board composition

Risk oversight is a full board responsibility. Having diverse skills, backgrounds, and experiences on the board is vital to understanding the broad range of risks a company can face. It is important to have some board members with deep expertise in the industry who can help anticipate what's to come. On the other hand, it is also important to have fresh perspectives—whether it's new directors, those with experience in different industries, or different skill sets—to view risk through different lenses. Directors who have specific risk management expertise can also bring real value.

Board composition and diversity

How would you describe the importance of the following skills, competencies, or attributes on your board?



Source: PwC, *2020 Annual Corporate Directors Survey*, September 2020.

Risk management expertise closely trails financial and operational expertise as an important skill directors seek for their boards. But ESG skills—covering a wide range of risks from environmental and social to governance—are less coveted, for now at least.

Board diversity can also impact risk oversight. In fact, 76% of respondents to our *2021 Annual Corporate Directors Survey* agreed that diversity on the board improves strategy/risk oversight and may alleviate the chance of missing out on key risks.

Once directors have evaluated the board's composition and whether they have the right skills on the board to effectively oversee risk, the next area of focus is understanding how the company is identifying and managing these risks.

Board diversity impacts oversight

76%

of directors say that board diversity improves strategy/risk oversight

Source: PwC, *2021 Annual Corporate Directors Survey*, October 2021.

Understanding and maximizing ERM

Enterprise risk management (ERM) means different things to different people. Some companies simply use ERM to identify, prioritize, and report on risks—protecting value. The best companies also use ERM to make better, more informed decisions, and improve their strategic, financial, and operational performance—driving value. But it takes work and buy-in at all levels to make that happen.

The best companies also use ERM to make better, more informed decisions, and improve their strategic, financial, and operational performance—driving value.

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, manage, and monitor risks so the company can meet its objectives. It's most valuable when it's integrated with strategic planning and decision-making.

Just assessing risk—identifying and prioritizing the key risks—isn't ERM. If a company stops there, it may know about risk, but not be actively managing it. That's not to say that identifying and assessing risk isn't a key part of maximizing the value of ERM to the company. Searching for risks requires not only understanding the organization's value drivers but also the risks—and opportunities—that may arise when those value drivers change. ERM can be a tool to help organizations consider the potential upside of the decisions associated with each particular risk. For example, many organizations changed their business models as a result of the COVID-19 pandemic, embracing a remote workforce and providing customers and clients with other ways of interacting with them, thus opening new distribution channels that will continue.

Boards and senior leaders need to look beyond this quarter or this year to craft the right strategy and take the right bets. ERM and senior management are unlikely to predict the next "black swan" event. But robust ERM can shine a light on disruptive technology; new competitors; environmental or social issues; and changes in regulations, economics, or the political landscape. The company's ongoing risk assessment should encompass emerging risks to help the company focus on future risks to identify any strategic impact.

It's also important to bear in mind that risk oversight isn't just about avoiding all risks. To have a successful strategy, companies must take some risks. Properly done, 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?

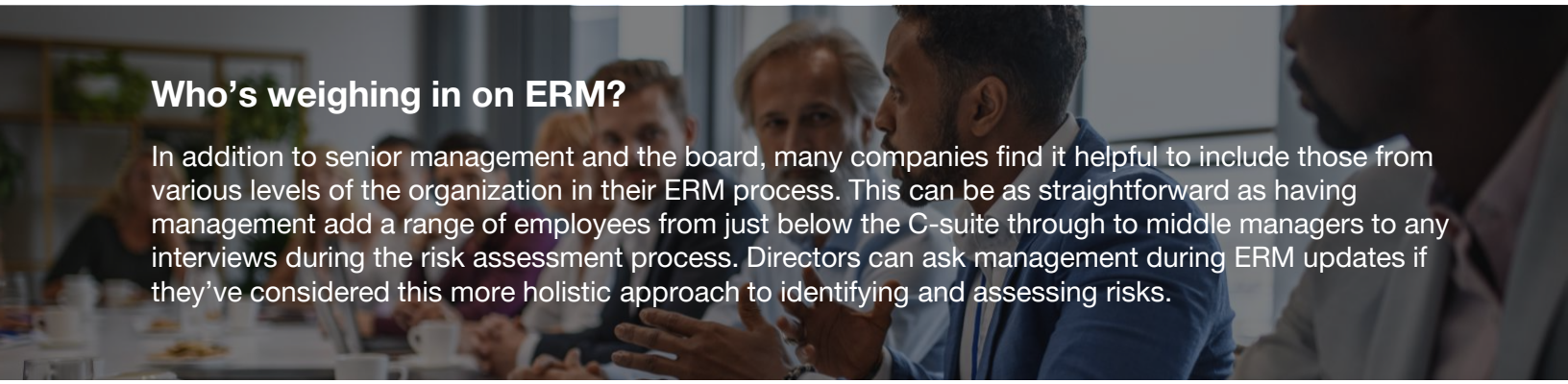
Signs that management could enhance ERM

Symptom	Possible causes	Board considerations
Strategy discussions focus mainly on opportunity without mentioning risk	• Risk may not be fully integrated into strategy development • Management may be focusing on the positive without providing the full picture	• Do the ERM risks identified line up with what the board considers to be the unique strategic risks to the business? • Do board discussions on strategy include using risk and ERM results as tools to identify opportunities?
List of risks provided doesn't include a connection to the company's strategic objectives	• ERM may be not be optimized to its fullest potential but rather viewed more as a compliance exercise • ERM may be used as an annual risk self-assessment survey rather than an ongoing process	• How often is the board receiving updates on ERM—annually? Or more frequently? • How are the outputs of ERM integrated into the board's strategic decision-making?
Heavy focus on easily understood and discrete risks—such as financial reporting, compliance, and/or operational risks	• ERM methodology may be identifying risks only from the bottom up without linking them to strategy • Risk management may be focused in the wrong areas	• What is the process for identifying risks—is it a balance of top-down and bottoms-up? • How is the output of ERM being vetted with senior leaders and the board?
ERM doesn't have visibility at the board or senior management level	• The ERM leader may not be getting the right level of support internally	• Is the ERM leader (often the chief risk officer or CFO) an executive that understands the company well and can appropriately lead the risk effort?
ERM discussions feel stale— covering the same risks every year	• ERM isn't challenging management to understand what's changed and what may lie ahead	• Has the ERM process considered emerging risks? • Is management considering how risks may evolve or emerge and what impact (positive or negative) that might have to the business?

For more on enhancing ERM, see the *2022 Global Risk Survey*.

Making sure ERM lives beyond the C-suite

If ERM operates only at the executive level, it's not going to influence behavior across the organization. In fact, some companies find it helpful to assess risks or risk prioritization at different levels. If you ask different groups of people to prioritize a handful of key risks at the company, you may get different answers based on each individual's purview. The board and the executive team might be aligned on risk prioritization, but middle management might have a very different prioritization. It's worth asking those outside the C-suite how they might prioritize risks. This could identify two things—either middle management is getting more risk insights from customers, suppliers, and other employees that the ERM process is not picking up, or the executive team is not effectively educating middle management about key risks and the need to focus on mitigation. Either way, this insight can be very helpful in understanding how the company is aligned on identifying and prioritizing risks.



Who's weighing in on ERM?

In addition to senior management and the board, many companies find it helpful to include those from various levels of the organization in their ERM process. This can be as straightforward as having management add a range of employees from just below the C-suite through to middle managers to any interviews during the risk assessment process. Directors can ask management during ERM updates if they've considered this more holistic approach to identifying and assessing risks.

Risk appetite

We've all read headlines about companies that took bets involving levels of risk they didn't fully understand. There's also concern about taking on too little risk and missing opportunities for performance and growth. In light of what they see happening, it's not unusual for directors to wonder: how much risk does our company need to take to realize the strategic plan?

Instinct drives risk-taking at many companies. Most people have a sense of how they should behave and what risks are acceptable. But how can senior management and the board know everyone is on the same page when it comes to taking risks? It comes down to leveraging a risk appetite. Management can let employees know how much risk is okay in trying to achieve its objectives by articulating its risk appetite statement. Some companies see this as an academic exercise that ends up on a shelf. But when done right, it can provide real insight into the types and amount of risk that are suitable for the company and where risk decision-making sits in the organization.

Successful risk appetite statements fit the strategy and inform business decisions. The risk appetite statement includes both quantitative and qualitative information. The board reviews the risk appetite statement annually as part of its ERM oversight efforts. And as part of regular reporting, boards get a consolidated view of risk across the organization to be able to assess the aggregation of risk against the risk appetite.

What makes a good risk appetite statement?

A good risk appetite statement may promote a healthy culture and aid in decision-making. It becomes a company playbook for how much uncertainty is acceptable. It sets the boundaries of how much risk to take to meet strategic and operating objectives. (Those boundaries will be different for different kinds of risks.) In reality, it may take several sentences to express how much risk is needed (the floor) and how much is acceptable (the ceiling) to achieve objectives. In summary, it makes risk-taking more transparent.

For examples, see COSO's *Risk Appetite - Critical to Success*.

What role does culture play in the risk discussion?

Risk appetite is a key part of the company's culture. A corporate culture that reflects a clear, consistent, ethical tone at the top can promote appropriate risk-taking and transparency. On the flipside, if the tone from the top is one of mistrust and micromanaging, decision-making may be paralyzed and lead to risk-averse culture. And a corporate culture that provides mixed messages—actions and words don't align—can lead to inappropriate risk-taking. Keen boards assess leadership, people, communication, strategy, accountability, reinforcement, risk management, and infrastructure to evaluate how risk impacts the company's risk culture.

See *Why do boards need to know their company's culture? Hint: to make sure it's an asset, not a liability* for more information on the board's role in overseeing culture.

The key elements underpinning an effective risk management function:

When understanding a company's risk management program, boards may find it helpful to consider these broad leading practices:

A single risk language. Common definitions and standard categories of risk make it easier to accurately combine risk information across the business and spot discrepancies and interdependencies.

A common risk assessment approach. One risk assessment approach with a single set of criteria makes it easier to share, compare, and combine different teams' perspectives on the various risks the company faces.

A streamlined approach to controls. As companies address specific risks over the years, they can end up with inefficient and overlapping controls. When possible, streamlining those processes can improve performance without sacrificing effectiveness.

Cross-functional collaboration. Better information-sharing across all functions that contributes to risk management can improve processes.

A single risk officer. A chief risk officer or similar executive can support risk management efforts across the company and coordinate risk reporting for both executive management and the board.

Risk reporting

Many companies use a silo-based and manual approach to managing and reporting on risks. This means that various parts of the company may report risks to the board at different frequencies, in different formats, and with different focus areas. Compounding the inefficiency of that fragmented approach, each part of the company may be using different systems, therefore reporting different types of data.

Some companies prepare comprehensive risk reports by distilling the information delivered by various risk management groups. But such an approach raises other challenges and the process itself can be inefficient. More and more companies are leveraging a GRC (governance, risk, and compliance) technology platform to consolidate and streamline the risk reporting process.

The board should determine what type, level, and frequency of reporting would enable it to effectively deliver on its risk oversight responsibilities. Leading organizations report quarterly to the board on ERM. As part of an annual deep dive on the overall ERM process, management may present its process for identifying and assessing the top risks to the organization. These top risks (generally between 10-15 risks, but could vary based on the company) and any changes in them would be part of the consistent quarterly pre-read report for the board.

Is your company getting the data it needs to manage risk?

Of PwC's 2022 Global Risk Study participants:

38% said their company's risk function is not actively seeking external insights to assess and monitor risks

Source: PwC, *2022 Global Risk Survey*, May 2022.

For each key risk, a senior leader should be assigned and a mitigation plan detailed. This tracking should specify key risk indicators (KRIs) for each risk being monitored at the board level. KRIs can serve as early warning signs and can be especially helpful for directors. These metrics can give boards a feel for how management scans the risk horizon for red flags. KRIs don't predict the future, but they allow management to monitor possible changes in either the impact or the likelihood of key risks to help minimize surprises. For example, a drop in gross domestic product or a rise in unemployment may signal to a retailer that holiday sales won't be as robust as expected and it may be time to lighten inventory or reduce staffing. KRIs should be closely linked to key performance indicators (KPIs) because effective risk management helps drive expected performance.

In addition to the recurring quarterly pre-reads for the board, the organization's ERM owner and a few of the risk owners may provide commentary during the meeting on what risks have changed and what may be emerging. Questions the board may want to consider asking include: (1) Are there risks not on the key list that might pop next? (2) What happens if two or more of the risks interact? It may be most helpful to consider ones for which the probability seems remote, but the impact would be critical.

The bottom line is that regular discussions with management on risk are imperative. Management's reporting and/or discussions with the board should, at a minimum, identify the most critical risks to the company, the possible impact and likelihood of these risks, the identification of risk owners, and the status of mitigating activities.

Board structure and oversight practices

Full board or a committee responsibility?

The full board is responsible for risk oversight and should understand a company's ERM program. However, the board may want to delegate the details of oversight for specific risks to committees. For example, the compensation committee may focus on risks posed by revamped compensation plans while the technology committee focuses on those inherent in a new IT systems integration.

With the increase in the number and type of risks that boards are overseeing, many boards are taking a fresh look at how they allocate risk oversight between the full board and committees. Leading boards revisit risk allocation at least annually to make sure that nothing is falling through the cracks and that all key risks are on the agenda at either the full board or a committee.

There's a lot of interest in risk committees—but risk committees are still relatively rare. How rare? Only 12% of companies in the S&P 500 have risk committees. This includes companies in the financial services industry and other highly-regulated sectors, where they may be required.

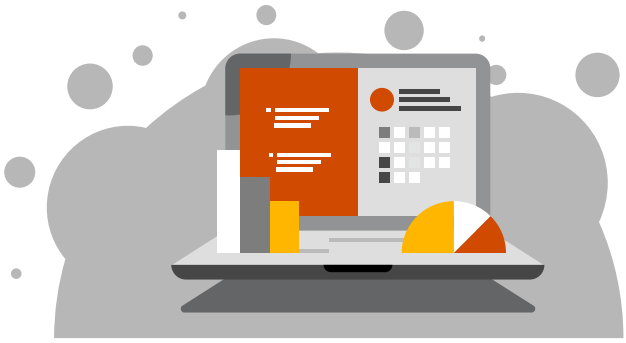
While the full board is responsible for overseeing risk, many assign the day-to-day oversight broadly to the audit committee, which already has significant demands on its time. Discrete risks are then assigned across the committee structure, with the audit committee picking up some of those as well. In addition to time constraints and broad scope, the audit committee may not be the right place for oversight of certain risks that may require more subject-specific experience.

No matter what oversight allocation structure the board decides to use, directors need to ensure that they are able to connect the dots later. A siloed focus on individual risks could prevent the board from identifying how risks intersect. Robust committee read-outs help ensure that important insights and conclusions are communicated to the full board. For effective oversight, it is critical to ensure that discrete aspects of risk management come back together at the enterprise level for a review of how those distinct risks interact, whether they can become co-variant, and what external circumstances might lead to seemingly independent risks aligning or cascading.

Using a risk allocation matrix

Some companies benefit from using a risk allocation matrix, which can be part of the key risk summary provided to the board. A risk allocation matrix, which works best when it is part of the ERM governance framework, helps board members understand which committee, or possibly the full board, owns the oversight responsibility for each risk. It should also be part of the ERM governance framework, a key component that clearly lays out who is managing and who is overseeing each risk.

According to an NACD survey, only 53% of directors indicated that their boards had assigned clearly-defined risk oversight roles to each of their committees.



Sample risk allocation matrix

Key risks	Executive owner	Board/committee oversight	Frequency	Source of assurance
Breaches in IT security	CIO	Audit committee	Quarterly	• Internal audit • IT consultant • Ethical hacker
Inaccurate financial reporting	CFO	Audit committee	Quarterly	• Internal audit • External audit
New acquisitions or partnerships	CEO	Board	As needed	• Internal audit
Third parties	COO	Board/audit committee	Semi-annually	• Internal audit
Human capital	CHRO	Compensation committee	Semi-annually	• Internal audit
Culture	CEO	Board	Annually	• Internal audit • External audit • Ethics officer/HR
Compliance	GC	Board/audit committee	As needed	• Internal audit • Compliance officer
Regulatory	GC	Audit committee	Quarterly	• Internal audit • External audit • Outside counsel

Making the most of meeting times

Whether it is the full board or a committee overseeing risk, periodic deep dives can help directors understand key risks more fully. The risk owners (business unit or functional executives) can explain the nature of the risk, its potential impact on strategic goals, how it's being managed—including acceptable limits—and what kind of controls are in place. It's also a great time to find out how they embed risk management practices in their businesses. And it's an opportunity to understand if they're managing risk and performance together, since individual risks can impact multiple objectives. Highlighting 1-2 key risk areas each quarter is good cadence, depending on how full agendas may be. Consider building these sessions into the annual agenda planning calendar.

Directors can then spend meeting time discussing the risk and how management's assessment may be shifting—for example, whether the potential impact is more severe or changing more quickly than expected.

And finally, directors should seek other opinions on how management is handling a specific risk by asking ERM, compliance, and internal audit personnel for their views.

Board transparency

How can a board reassure investors and other stakeholders that it is overseeing risk effectively?

Since 2010, public companies have been required to include disclosures about the board's role in risk oversight in their proxy statements. Early proxy disclosure included few details. They often simply stated that the board has overall responsibility for overseeing risk, the audit committee oversees financial-related risks, the governance committee oversees governance-related risks, and the compensation committee oversees compensation-related risks. Such basic disclosures don't give shareholders much confidence that the board is actively overseeing the risks that matter.

Recently, shareholders have encouraged companies to offer more meaningful and transparent disclosures on the board's risk oversight activities and performance. In particular, major investors want to understand how companies are focusing on sustainability risks that could have an impact on a company's ability to deliver long-term value. To urge action, some investors have even announced changes in their director voting policies. In certain cases, a company's failure to appropriately focus on these risks and disclose relevant metrics could now trigger votes against directors from influential shareholders.

In response to investor demand, regulators have also started to push for more risk oversight disclosure. In 2022, the SEC proposed rules related to both climate change and cybersecurity disclosures. The proposed rules address disclosing more information on both the company's risk management in these areas and the board's oversight in each. Given this heightened focus on risk oversight by investors and regulators, many companies are now expanding their risk disclosures.

Directors should read their current proxy statement disclosures with a critical eye and be sure they are taking credit for the work they are doing. Directors can ask management to benchmark the company's disclosures about the board's oversight of risk. Reviewing best in class disclosures can challenge the board to be more transparent. This exercise may also point to the need to devote more board time to risk management or identify other gaps in the board's oversight process that need to be addressed.

How robust are your risk oversight disclosures?

Well-crafted proxy statements have evolved to include additional information related to risk oversight such as:

- Whether the full board is engaged
- A description of how the board reviews the company's risk management function
- The board's approach to allocating risk oversight by committee including a detailed listing of the key risk areas each committee focuses on
- The nature and frequency of reporting to the board or committee
- The role of senior management in connection with risk oversight, including a description of the management risk committee, its members, and its responsibilities
- Specifics regarding cybersecurity oversight, including number of times cybersecurity was on the board agenda, who (e.g., CIO, CISO, CRO) presents updates to the board, whether they also hear from outside experts, and whether they hold private sessions with the CIO or CISO
- Specifics regarding ESG risk oversight, including objectives and targets
- How the board gets comfortable with its own technical knowledge in these areas—whether through specific expertise, use of third-party advisors, or ongoing education/upskilling

In conclusion…

In a business risk environment that is becoming more complex and interconnected, boards play a crucial role in overseeing risk and keeping shareholders informed.

- To begin, boards can start by looking around the table. Is there diversity of experience, thought, gender, and race to bring different perspectives on risk?
- Boards will also want to understand their company's ERM program—and how they can contribute to that program.
- The board will also want to spend time on its own structure for oversight.
- And finally, boards will not want to forget about the company's various stakeholders—what information is provided to them about the company's risk management programs and activities?

By examining and refining its approach to risk oversight, a board can deliver enhanced value to the company and its shareholders.

How PwC can help

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

Maria Castañón Moats
Leader, Governance Insights Center
maria.castanon.moats@pwc.com

Paul DeNicola
Principal, Governance Insights Center
paul.denicola@pwc.com

Stephen G. Parker
Partner, Governance Insights Center
stephen.g.parker@pwc.com

Brian Schwartz
Cyber, Risk and Regulatory Partner and
Author of PwC's Global Risk Study
brian.schwartz@pwc.com

Jamie Gamble
Managing Director
jamie.gamble@pwc.com

Catie Hall
Director, Governance Insights Center
catherine.hall@pwc.com

Carin Robinson
Director, Governance Insights Center
carin.l.robinson@pwc.com

© 2022 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, 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. This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.