Risk oversight and the board of directors: navigating a complex, evolving area

December 2020

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 real value to a company and its shareholders both in times of crisis, and when it’s just business as usual. It starts with understanding the strategic direction of the company, considering the broader stakeholder perspectives, and having an effective oversight function at the board level. How does your board define and put into action its approach to risk oversight?
We’re living in an era of unforeseen risks, including a “black swan” event (essentially something so unprecedented 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 organization and agility. The number of risks the board oversees continues to grow, even as the nature of those risks is changing and they are becoming more interconnected. The probability and impact of these risks also continues to shift, with some risks just affecting a certain area of the business and others severely impacting the overall brand.

We’ve certainly learned that we all need to broaden our risk thinking, recognizing that some things we thought could never happen might, in fact, happen. This requires more skepticism when preparing for the future—a skill that the board typically has more experience with than management. Taking a long view on risks aligned to the strategic plan at the board level allows company leadership to focus on day-to-day management of those risks.

The link between strategy and risk

Large institutional investors have been pushing for more information about how a company’s purpose is linked to its long-term strategy and success. With this growing external focus on a company’s purpose, boards should understand how their company’s purpose statement informs its risk universe. The risk universe 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 environmental, social and governance (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 a material 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 sustainable value of the company.

Companies are now more focused on identifying material ESG risks of this type, monitoring and overseeing those risks and communicating these 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. Answering the questions of where and when to discuss key risks is relatively easy. Figuring out how to effectively oversee these key risks at the board level is more challenging. Here, we’ll discuss how the board can work through the challenges of risk oversight.

Room for improvement in ESG discussions

Only 55% of directors say their boards discuss ESG as part of the enterprise risk management discussion.

I. 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. Directors who have risk management expertise can also bring real value.

<table>
<thead>
<tr>
<th>Skill</th>
<th>Very important</th>
<th>Somewhat important</th>
<th>Not very important</th>
<th>Not at all important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial expertise</td>
<td>89%</td>
<td>11%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational expertise</td>
<td>53%</td>
<td>3%</td>
<td>44%</td>
<td>4%</td>
</tr>
<tr>
<td>Risk management expertise</td>
<td>50%</td>
<td>5%</td>
<td>46%</td>
<td>5%</td>
</tr>
<tr>
<td>Gender diversity</td>
<td>47%</td>
<td>17%</td>
<td>37%</td>
<td>3%</td>
</tr>
<tr>
<td>Industry expertise</td>
<td>43%</td>
<td>8%</td>
<td>49%</td>
<td>3%</td>
</tr>
<tr>
<td>Racial/ethnic diversity</td>
<td>34%</td>
<td>1%</td>
<td>44%</td>
<td>20%</td>
</tr>
<tr>
<td>IT/digital expertise</td>
<td>23%</td>
<td>1%</td>
<td>54%</td>
<td>22%</td>
</tr>
<tr>
<td>Cyber risk expertise</td>
<td>22%</td>
<td>4%</td>
<td>60%</td>
<td>17%</td>
</tr>
<tr>
<td>Age diversity</td>
<td>21%</td>
<td>5%</td>
<td>46%</td>
<td>28%</td>
</tr>
<tr>
<td>International expertise</td>
<td>18%</td>
<td>1%</td>
<td>42%</td>
<td>29%</td>
</tr>
<tr>
<td>Marketing expertise</td>
<td>15%</td>
<td>1%</td>
<td>51%</td>
<td>30%</td>
</tr>
<tr>
<td>Human resources expertise</td>
<td>14%</td>
<td>3%</td>
<td>60%</td>
<td>24%</td>
</tr>
<tr>
<td>Environmental/sustainability</td>
<td>10%</td>
<td>1%</td>
<td>50%</td>
<td>35%</td>
</tr>
</tbody>
</table>

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.
Diversity of director experience can also be helpful when thinking about risk oversight. 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.

In addition, gender diversity can impact risk oversight. In fact, 71% of respondents to our 2020 Annual Corporate Directors Survey agreed that gender diversity on the board improves strategy/risk oversight. If you don’t have enough diverse experiences or viewpoints in the room, you might want to re-evaluate your board composition.

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 board oversight

71% of directors say that board diversity improves strategy/risk oversight.

II. ERM is a good place to start

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, enabling 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, monitor 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 managing it.

Signs that management could improve the way it addresses ERM

<table>
<thead>
<tr>
<th>Symptoms</th>
<th>Possible causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your strategy discussions focus only on opportunity without mentioning risk.</td>
<td>• Risk isn’t an integral part of strategy development.</td>
</tr>
<tr>
<td></td>
<td>• Management isn’t giving the board the full picture.</td>
</tr>
<tr>
<td>You get a laundry list of risks—no analysis, no connection to the company’s strategic objectives.</td>
<td>• Management views ERM as a compliance exercise.</td>
</tr>
<tr>
<td></td>
<td>• ERM is seen as just an annual risk self-assessment survey.</td>
</tr>
<tr>
<td>There’s a heavy focus on easily understood and discrete risks—such as financial reporting, compliance and/or operational risks.</td>
<td>• Management is identifying risks from the bottom up, not linking them to strategy.</td>
</tr>
<tr>
<td></td>
<td>• Risk management may be focused in the wrong areas or simply not reporting the right information to the board.</td>
</tr>
<tr>
<td>ERM doesn’t have visibility or credibility at the board or senior management level.</td>
<td>• The individual leading ERM doesn’t have the clout to get meaningful input or buy-in from senior executives.</td>
</tr>
<tr>
<td></td>
<td>• The CEO doesn’t value ERM.</td>
</tr>
<tr>
<td>ERM discussions feel stale—covering the same risks every year.</td>
<td>• ERM isn’t challenging management to understand what’s changed and what’s ahead.</td>
</tr>
</tbody>
</table>
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. 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 annual risk assessment should encompass emerging risks to help the company focus on future risks with strategic impact.

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?

Take a fresh look at the ERM process. Based on your knowledge at the board level, do the ERM risks identified line up with what you consider to be the unique strategic risks to the business? Has the ERM process considered emerging risks? 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? Do the risks have appropriate management ownership and mitigation plans?

Making sure ERM lives beyond the C-suite

If ERM lives only at the executive level and nowhere else, it’s not going to influence everyone’s behavior. In fact, some companies like 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 will get different answers.

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 managing risks.
Risk appetite

We’ve all read headlines about companies that took bets involving levels of risk they didn’t fully understand, or that overstepped ethical boundaries. 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 succeed?

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 framework. Management can let people know how much risk is okay in trying to achieve objectives by articulating its risk appetite statement. Some chief risk officers are reluctant to help management develop a risk appetite statement because they see it as an academic exercise that ends up on a shelf. But it can provide real insight into the types and amount of risk that are suitable for the company.

If your company has a risk appetite statement, ensure that it fits the strategy and informs business decisions. The risk appetite statement should include both quantitative and qualitative information. The board should review the risk appetite statement annually along with ERM oversight efforts. If your company does not have a risk appetite statement, at a minimum, the board should understand the company’s appetite for risk and how it is embedded in the company’s culture.

What role does culture play in the risk discussion?

At its best, culture is an asset. An effective culture promotes appropriate risk-taking and transparency with a clear, consistent, ethical tone at the top, which filters through to all employees. When tightly aligned with a company’s strategy, it can be a powerful enabler of success. At its worst, culture is a hindrance. It becomes a drag on performance that makes it difficult for leaders to achieve key objectives and can trigger reputational and financial risk for the company.

What makes a good risk appetite statement?

A good risk appetite statement will 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.

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.

For examples, see the Defining Risk Appetite section of COSO’s 2017 Enterprise Risk Management—Aligning Risk with Strategy and Performance.
The key elements underpinning an effective risk function

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

- **A common risk assessment approach.** One risk assessment approach with a single set of assessment 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 have addressed different risks over the years, many have ended up with inefficient and overlapping controls. The streamlining of those processes—so that they contain fewer and simpler controls—can improve performance without sacrificing effectiveness.

- **Cross-functional collaboration.** Better information sharing through better methods across all functions that contribute 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 often manual approach to managing risks. This means that different 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 and different definitions of risks and controls, 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 the risk reporting process.

The board needs to determine the reporting it needs to effectively deliver on its risk oversight responsibilities.

At a minimum, the board should receive reporting that identifies and tracks key risks, identifies who is accountable for each key risk and the mitigation plans. An element of the key risk tracking should specify key risk indicators (KRIs) for each key risk being tracked and 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 is scanning the risk horizon for red flags. KRIs don’t predict the future—they allow management to monitor possible changes in either the impact or the likelihood of key risks to help minimize surprises so it can take action. 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 because in the end, effective risk management ought to help drive expected performance.

The bottom line is that even if a company lacks a sophisticated ERM process, regular discussions with management about the risk environment, what’s happened, what’s trending and what’s emerging is imperative to help your board oversee key risks.

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

Of PwC’s 2020 Global Risk Study participants:

50% said their company has the right data, today, to anticipate and manage existing and emerging risk

33% said they have the right technology and tools to do so

III. Board oversight

Full board or a committee responsibility?

The full board is responsible for overseeing risk and should understand a company’s ERM process. However, the board may want to delegate the details of risk oversight to committees.

With the increase in the number and type of risks that boards are overseeing, we are seeing many boards take a fresh look at how they allocate risk oversight between the full board and committees. If you’re currently satisfied with the way your board handles and assigns risk oversight, there is probably no reason to change.

There’s a lot of interest in risk committees—but risk committees are still relatively rare outside the financial services industry and other highly-regulated sectors, where they may be required. How rare? Only 13% of companies in the S&P 500 have risk committees.¹ This includes companies that combine risk with another committee, like finance or audit.

Most boards assign risk oversight to their audit committee, which already has significant demands on its time. Audit committees have more meetings—about eight times a year on average²—and those meetings last longer than any other committee. In addition to time constraints, the audit committee may not be right for other reasons. Audit committee members are often selected because of their financial acumen, while risk discussions may require other types of expertise.

It may make sense to assign certain risks to different committees—the compensation committee may focus on revamped compensation plans while the technology committee focuses on new IT systems integration. But if you are allocating risks to different committees, ensuring the board has the ability to connect the dots is important. Make sure the committee chairs share important insights and conclusions with the full board. This can be done through robust committee read-outs. That will make sure nothing falls through the cracks and different committee oversight efforts can be linked to key risks.

Committee read-outs: how can directors connect the dots across key risks and make sure they aren’t missing anything?

Some companies think they’re done once they’ve plotted individual risks on a heat map to show impact and likelihood. But it’s rare that one risk doesn’t trigger several impacts, some of which relate to other risks. For example, the wrong compensation plan may drive people to take excess risk or compromise safety to meet unrealistic production and financial targets. A siloed focus on individual risks could prevent the board from identifying how risks intersect.

Why is that? If the board or a committee discusses different key risks in different meetings, it may not be possible to see how risks can impact one another. And, if risks are discussed in committees but not included in full board discussions, it’s easy to miss the magnified impact of several risks happening together.

². Ibid.
A risk allocation matrix can be useful

It is helpful to use a risk allocation matrix, which can be part of the key risk summary that many boards currently receive. A risk allocation matrix ensures that board members understand which committee, or possibly the full board, owns the oversight responsibility for each risk.

According to one survey, only 66% of directors indicated that their boards had assigned clearly-defined risk oversight roles for committees.\(^3\)

<table>
<thead>
<tr>
<th>Key risks (illustrative only)</th>
<th>Executive responsible</th>
<th>Board oversight</th>
<th>Frequency</th>
<th>Source of assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breaches in IT security</td>
<td>Chief information officer</td>
<td>Audit committee</td>
<td>Biannually</td>
<td>Internal audit IT security consultant</td>
</tr>
<tr>
<td>Unreliable supply chain</td>
<td>Chief procurement officer or chief operating officer</td>
<td>Board</td>
<td>Annually</td>
<td>Internal audit</td>
</tr>
<tr>
<td>Integrating new acquisitions</td>
<td>Chief executive officer</td>
<td>Board</td>
<td>Annually</td>
<td>Internal audit</td>
</tr>
</tbody>
</table>

**Benefits of risk committees**

A risk committee may make sense if:

- The board simply cannot find enough time at the board level or on another committee to focus properly on risk.
- The board wants a central place to coordinate and monitor all risk discussions currently taking place in individual committees so that the governance of risk oversight is transparent to everyone and has the right directors focused on it.
- The board wants to send an important signal to shareholders and other key stakeholders, such as regulators.

**Board practices**

Whether it is the full board or a committee overseeing risk, a deep dive on a particular issue is one good approach to understand key risks more fully. The risk “owners” (business unit or functional executives) should help directors understand 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 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. KRI s should also be a topic so directors can learn what signals management uses to anticipate changes in the risk and how they might respond.

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 for their views.

IV. 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. In the past, many companies have disclosed few details. They often simply stated that the board had 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 pushed for 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 climate and social risks that could have an impact on a company’s ability to deliver long-term sustainable value. In order 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.

Regulators have also started to push for more risk oversight disclosure. In 2018, the SEC issued interpretive guidance focused specifically on disclosure about cybersecurity risks and incidents. Among other things, it identifies sections of filings where the disclosure of cybersecurity matters may be appropriate. It also provides examples of the types of disclosure that should be considered, including the nature of the board’s role in overseeing the management of cyber risk, if it is material to the business.

Given this heightened focus on risk oversight by investors and regulators, we’re now seeing many more companies expand their risk disclosures to be more specific.

Directors should read their current proxy 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 with those of peers and competitors. They should find a few examples that might be considered best in class and challenge themselves 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 can be addressed.
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? It is critical that boards understand their company’s ERM program—and how they can contribute. The board will have to spend time on its own structure for oversight—should there be a separate risk committee? And don’t 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 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
- A statement indicating that the board focuses on material and emerging risk topics
- 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
Contacts

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
Risk Assurance Partner and Primary Author of PwC’s Global Risk Study, PwC US
brian.schwartz@pwc.com

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