Risk oversight: Reassessing board and committee structure

With the rapid expansion of risks in cybersecurity, generative artificial intelligence (AI), climate, and other areas, many boards are reassessing how best to structure board and committee oversight and focusing on director expertise and education—particularly relating to new and emerging risks.

Lead directors of Fortune 100 and other large companies shared their views on those issues during a quarterly peer exchange led by KPMG LLP Deputy Chair and COO Laura Newinski. She was joined by KPMG Audit Committee Institute Leader Stephen Dabney and KPMG Board Leadership Center Senior Advisor Claudia Allen.

Key takeaways

- Given the velocity of change around risks, boards should periodically reexamine their board and committee oversight structures to determine whether changes may be needed.
- Coordination among committees and committee chairs and communication between committees and the full board are critical.
- Reassess the skill sets of the full board and committee members to help ensure effective oversight of emerging risks. Consider whether to add additional directors, bring in third-party experts to educate and/or advise the board and/or committees, or create an advisory board to bring focus to an issue.

Committee structure

Board leaders participating in the conversation shared how their companies are structuring risk oversight at the board and committee level. The directors agreed that, given the pace and velocity of changes in the business and risk landscape, every board should periodically reassess whether its existing oversight structures are still appropriate, as well as whether committee charters reflect current priorities and mandates.

"Many lead directors and nominating and governance committee chairs—who are often the same person—are taking a fresh look at the major risks the board is overseeing and trying to map them to committees and adjusting committee responsibilities as needed or considering forming new committees," said Allen.

A number of lead directors said their boards reviewed how they allocated risk oversight to standing committees and made changes to charters, committee names, or both to reflect shifting oversight responsibilities. For example, one director shared that a board that established a risk committee consisting of committee chairs several years ago subsequently eliminated the committee. "It became clear that there was too much information concentrated in a single committee and made available to only the members of that committee," the director said. "We determined that a single risk committee wasn't in the best interests of our fiduciary oversight responsibilities." The company's major risks were redistributed appropriately across other committees, which were renamed to reflect the changes. Additionally, responsibilities for ownership at the management level and for annual review by the committees were established.

Few among the group said their boards had separate risk committees. Data shows that relatively few boards of companies outside highly regulated industries such as financial services and healthcare have risk committees. Only 12 percent of S&P 500 companies had a separate risk committee as of September 2023, according to data from The Conference Board and ESGAUGE.[1]

The board's chosen risk oversight structure is driven by a number of factors, including the company's industry and regulatory demands. "I think committee structure can depend on the history of the company and whether it's got major issues or not," said a director who serves on two boards—one with a separate risk committee and another without. "I think both approaches can work." While one board established a risk committee several years ago that addresses operational and enterprise risks, the other oversees enterprise risk at the full board level, with certain elements of risk assigned to designated committees. "The charters are clear in terms of which element of risk each committee is responsible for, and the information flow is good from the committees to the board."

Another lead director of a board with a separate risk committee said that model is still effective for the company. "We make all of the information available to the entire board through the portal. We expect the board members to review the committee information to make sure they're comfortable with it. We get enterprise risk reports four times a year where we have management come in and discuss those risks… For us, the risk committee works very well."

Board leaders noted that it's an ongoing conversation. "None of the boards I'm on have a separate risk committee, but we talk about it a lot," said one director. "We are keeping our minds open to whether we need a separate risk committee or separate cyber committee, but we haven't taken that leap yet."

Committee coordination

Where multiple committees own oversight of different aspects of a risk, it's critical to have coordination among the committees and committee chairs, as well as clearly delineated responsibilities, said Allen. For example, a technology committee might have oversight of technology risk, while the audit committee might retain oversight of the disclosures and controls over technology.

Allen noted a number of practical issues to consider in determining whether to form a separate risk committee or other additional standing committee. For example, "Who would serve? When considering a risk committee, many times, it's essentially the members of the audit committee. How do you draw the lines between audit and risk and make sure that information is coordinated and flows up to the full board? And depending on the number of committees you have, you may need to run meetings concurrently rather than sequentially, which may effectively limit the ability of directors to serve on certain committees."

Specific risks

While not new, oversight of cybersecurity risk is an issue that boards continue to struggle with due to the pace of change, increasing complexity of threats (including as a result of generative AI), and the potential impact of cyber incidents. "We look at the amount of time cyber is taking at the audit committee. We don't run the committee meetings concurrently so that others can join. Generally, we find that the full board sits in. That makes us ask, should we even have a committee?"

Sustainability issues are also on every board agenda today, although how they are overseen depends on the industry and specific company. As an energy company director stated, "Sustainability in a broad sense is on everyone's agenda, but in the fossil fuel business you're in the crosshairs." While initially energy transition was a board-level function, the board established a separate energy transition committee to help it focus on the issue. "Our board committee meetings have always been open to all directors, but nobody showed up [to committees they weren't members of] before we formed that committee. All of the directors show up to those meetings every time."

At a consumer-facing retailer, reputational risk has been elevated to the full board level. "We are talking about it as one of the critical enterprise risk concerns we have, in addition to geopolitical, supply chain, economic, and financial risk." The conversation is led by the CEO, CFO, and chief growth officer.

Skill sets and expertise

Directors said their boards are taking a close look at the skill sets of the full board and committees and considering potential gaps. Since the audit committee is often the default home for new risks, Allen noted, "It's important to look at whether the audit committee has the skill sets and bandwidth to oversee the risks that are being allocated to it."

[1] The Conference Board, Corporate Board Practices Live Dashboard, data retrieved September 2023.

Participants shared examples of how their boards are addressing the need for directors with risk expertise:

Expanding audit committee skill sets: "One of the things that we're doing is reassessing the skill sets on our committees to make sure we are keeping current … [For example], at the audit committee, not just finance and accounting [backgrounds] … people with more technology, cybersecurity backgrounds, and current backgrounds in the world of technology."

Nontraditional director backgrounds: "We changed the charters of the committees to cover additional areas of risk. From that came a skills assessment, then we looked at who we have on the board that could deliver on those skills needs. That led us to bring in some nontraditional board candidates."

Cyber, tech, and regulatory expertise: "We're looking at emerging risks and identifying areas where we might want to bring in expertise that might not have been represented. We recently brought in the CEO of a tech committee to help us think about cyber and AI, and we brought in somebody from healthcare because of the heavy focus on regulation and compliance."

Other options include forming an advisory board or bringing in third-party experts to help directors stay current, in addition to board education. "We see a number of boards engaging third parties to help educate the board around a range of issues like AI and cyber," said Dabney. Directors cautioned against adding specific expertise at the expense of broader business and/or industry experience. "Getting that balance right, is, of course, highly dependent on the company, industry, and the board's approach to governance and its evolving expertise," said Newinski.

Additional insights

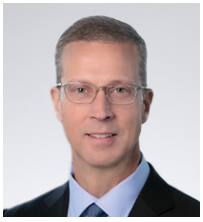
[Shifting geopolitics and the role of the board]

[Advancing the board-management climate conversation]

[SEC's final cybersecurity rules: A board lens]

Contact us

Laura Newinski
Deputy Chair and COO, KPMG LLP
T: 612-232-0675
E: lnewinski@kpmg.com



Stephen Dabney
Leader, KPMG Audit Committee Institute
T: 713-319-2389
E: sdabney@kpmg.com

Claudia Allen
Senior Advisor, KPMG Board Leadership Center
T: 312-665-2180
E: claudiaallen@kpmg.com

The views and opinions expressed herein are those of the speakers and participants and do not necessarily represent the views and opinions of KPMG LLP.

Some of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia