KPMG

Clarifying committee oversight responsibilities for evolving enterprise risks

The unprecedented events of the past two years have put corporate governance processes, particularly board and committee oversight of the company's major enterprise risks, to the test.

With board standing committees now playing such a vital role in helping boards carry out their risk oversight, there is a premium on clearly delineating the responsibilities of each committee for the various categories of risk, particularly where there are overlapping responsibilities.

Given the increasing number and complexity of risks companies face today, many boards are delegating specific risk oversight duties to standing committees for a more intensive review than the full board can undertake. Depending on the company size and industry, we see boards delegating to various committees responsibility to support the board's oversight of mission-critical risks, as well as climate; environmental, social, and governance (ESG); human capital management; cybersecurity and data governance; legal and regulatory compliance; supply chain; mergers and acquisitions; and more.

At the same time, many boards are looking to reduce the burden on the audit committee to oversee major categories of risk beyond its core oversight responsibilities (financial reporting, related internal controls, and oversight of internal and external auditors). This is in response to concerns about the committee's already heavy workload in its core areas of responsibility, and whether it has the expertise to oversee major evolving risks such as cybersecurity, data security, and global regulatory compliance, as well as climate and other ESG risks.

In this environment, boards may need to reassess whether their delegation of risk oversight responsibilities to each standing committee is clear, properly aligned, and coordinated across committees—particularly when there is overlap. For example, the nominating and governance (or sustainability), compensation, and audit committees likely have overlapping responsibilities in the oversight of ESG issues. Cybersecurity oversight may reside with a technology or other committee, but the audit committee likely has oversight responsibility for some aspects of cybersecurity and data governance. Human capital management issues—from ethics and compliance to talent development and performance incentives—may also touch different committee agendas.

The challenge for the board is to clearly define the risk oversight responsibilities of each committee, with the goal of ensuring "that management has implemented an appropriate system to manage these risks, i.e., to identify, assess, mitigate, monitor, and communicate about these risks," as noted in the *Report of the NACD Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward*.

A particular area of focus should be the clarification of overlapping risk oversight responsibilities. For a particular category of risk, boards should clarify a standing committee's versus the audit committee's oversight responsibility for:

- Periodic risk inventories and assessments for the risk category
- The quality of risk information, data, communication, and reporting (internal and external), including the quality of data and information included in sustainability reports
- Monitoring enterprise risk management performance
- Internal and external assurances regarding risk assessments and controls
- Monitoring internal controls to mitigate the risk and respond if a risk event occurs (the audit committee's responsibility to oversee internal controls over financial reporting is clear; however, there may be a need for more clarity regarding the role of the audit and standing committees in overseeing the broader internal control environment)

Even when the board assigns oversight responsibility for a particular category of risk to another committee, the audit committee will continue to have important responsibilities, including oversight of internal audit's assurance activities for that risk, as well as oversight of management's disclosure controls and procedures for reporting on the risk in US Securities and Exchange Commission filings.

Oversight of a company's major enterprise risks is a formidable undertaking for any board and its committees. Critical to meeting that challenge is to ensure that there is a clear delineation of the risk oversight responsibilities of each standing committee, and that the standing committee structure enables effective board oversight of the company's enterprise risks.

This article was originally published in the Spring 2022 issue of NACD Directorship *magazine.*

Patrick A. Lee is a senior advisor with the KPMG Board Leadership Center.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center (BLC) champions outstanding corporate governance to drive long-term value and enhance stakeholder confidence. Through an array of insights, perspectives, and programs, the BLC—which includes the KPMG Audit Committee Institute and close collaboration with other leading director organizations—promotes continuous education and improvement of public and private company governance. BLC engages with directors and business leaders on the critical issues driving board agendas—from strategy, risk, talent, and ESG to data governance, audit quality, proxy trends, and more. Learn more at kpmg.com/us/blc.

Contact us

kpmg.com/us/blc
T: 1-800-808-5764
E: us-kpmgmktblc@kpmg.com

kpmg.com/socialmedia

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