Board oversight of third-party risk management

October 2023

by John H. Rodi and Greg Matthews

In recent years, as a result of reputational harm caused by the failure of third parties to deliver goods and services in line with expectations, management has had to sharpen its focus on third-party risk management (TPRM) programs. These third parties—including vendors, suppliers, cloud service providers, consultants, sales and distribution channels, and partners, as well as fourth, fifth, and nth parties—pose the same complex and evolving array of risks the company faces.

In a recent KPMG survey on TPRM, three-quarters of respondents said their company experienced a major business disruption because of a third party in the last three years, and that business disruptions caused by third parties have exposed their companies to reputational risks. As many companies are increasingly seeing firsthand, cybersecurity and data privacy, geopolitical risk, compliance, climate and other environmental and social risks, and business continuity issues can quickly impact business operations and the brand.

While many companies have robust TPRM programs in place as a strategic imperative today, ensuring that TPRM programs keep pace with the rapidly changing risk, regulatory, and compliance environment is a significant challenge. As boards oversee management's efforts to maintain effective TPRM programs, key areas of focus should include the following:

Third-party cybersecurity and data privacy risks

According to the KPMG 2023 Audit committee survey, third-party cybersecurity and data privacy risks rank among the top third-party risks today, and the level of risk is increasing given the growing sophistication of hackers, including their use of generative artificial intelligence (AI). As noted in a recent World Economic Forum report,[1] a key challenge for companies is to maintain continuous monitoring and real-time visibility to identify potential third-party cybersecurity risks and issues. That requires leveraging automation, aligning the company's and third-party's internal and external control assessments, and understanding how management is improving its monitoring of third-party cybersecurity threats on a real-time basis.

Given the importance of cybersecurity risks, the US Securities and Exchange Commission's (SEC's) recent cybersecurity disclosure rules require greater disclosure in this area, including whether the company "has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider." The final rules do not exempt companies from providing disclosures regarding cybersecurity incidents on third-party systems they use. However, as stated in the SEC's adopting release, companies are not required to conduct additional inquiries outside of their regular channels of communication with third-party providers and in accordance with the company's disclosure controls and procedures.[2] Nonetheless, boards will want to confirm that management has effective

[1] Global Cybersecurity Outlook 2023, World Economic Forum, January 2023.

[2] US Securities and Exchange Commission Final Rule, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," July 26, 2023.

communication plans in place with third-party service providers to enable timely assessment and disclosure of material cybersecurity incidents.

Cybersecurity also poses compliance risks if third parties have access to personal data. Many countries have already enacted privacy and personal data protection laws and regulations, and more are in the process of drafting legislation. Companies should be monitoring global legal and regulatory data privacy developments. If third parties have access to personal data, then the company needs to ensure these parties have controls in place to manage that data in accordance with the laws and regulations as well as the company's data privacy policies.

Risks posed by use of third-party AI tools

Companies are quickly recognizing the need to address the growing risks associated with their use or integration of third-party AI tools. As discussed in an April 2023 *MIT Sloan Management Review* article, "Third-party AI tools, including open-source models, vendor platforms, and commercial APIs [application programming interface], have become an essential part of virtually every organization's AI strategy in one form or another, so much so that it is often difficult to disentangle the internal components from the external ones."[3]

As a result, companies need to reassess their AI governance structure and processes regarding the development, use, and protection of AI systems and models, how and when an AI system or model—including the use of third-party generative AI tools—is to be developed and deployed, and who makes these decisions. What regulatory compliance and reputational risks—including biases—are posed by the company's use of third-party generative AI tools? How is management mitigating these risks? (Also see Assessing the risks and opportunities of generative AI.)

Third-party climate, sustainability, and other ESG risks

Stakeholder demands for higher-quality climate and other environmental, social, and governance (ESG) disclosures should be prompting boards to sharpen their focus on the company's efforts to manage a broad range of climate and sustainability risks in the supply chain. As part of the effort, boards should closely monitor SEC, state, and global regulatory developments in these areas and management's plans to comply with new disclosure mandates. Key areas include mandated disclosures regarding the impact of climate change on the supply chain; the disclosure of Scope 3 greenhouse gas emissions data; and disclosures regarding a range of sustainability and "S" risks in the supply chain, such as human rights and forced labor.

Even as they await the SEC's final climate disclosure rules, companies doing business abroad will also want monitor and maintain compliance with other climate and sustainability regimes, including the International Sustainability Standards Board's global sustainability disclosure standards and the European Union's European Sustainability Reporting Standards.

Collection and calculation of Scope 3 greenhouse gas emissions data will pose a significant challenge for many companies, given the number of third parties in the supply chain and the fact that the emissions data reside outside of the company's control. Companies need to plan now as to how they will collect and calculate quality Scope 3 emissions data.

Management's projects to address business operations vulnerabilities and improve resilience and sustainability

For the past several years, companies have been navigating unprecedented business operational stresses and strains, with failures often glaringly public. Many are undertaking major initiatives to "de-risk" the supply chain—i.e., to understand the role third parties play in the delivery of goods and services, to identify and address vulnerabilities on these dependencies, and to improve resilience and sustainability by taking a risk-based approach. The projects vary by company and may include updating business continuity and disaster recovery plans, diversifying the supplier base, re-examining supply chain structure and footprint, reducing dependency on China and developing more local and regional supply chains, deploying technology to improve business operations visibility and risk management, improving cybersecurity to reduce the risk of data breaches, and developing plans to address future disruptions.

In the near term, the board will want to help ensure that significant projects being undertaken by management to rethink, rework, or restore critical business operations are carried out effectively. Importantly, given the complexity of business operations, it is critical that the company maintain an overarching vision and strategy to manage the supply chain in the context of the company's broader business operations risks. Focused leadership, connecting critical dots, and clear accountability are essential.

---

[3] Elizabeth M. Renieris et al., "Responsible AI at Risk: Understanding and Overcoming the Risks of Third-Party AI," *MIT Sloan Management Review*, April 20, 2023.

Core questions for the board

As the issues and elements highlighted above suggest, the increasing complexity and range of third-party risks poses a significant oversight challenge for boards. Investors, regulators, ESG rating firms, and other stakeholders are demanding higher-quality disclosures about third-party risks and how boards and their committees are overseeing the management of these risks. In this challenging environment, many boards are reassessing how, through their committee structure, they can effectively oversee third-party risk.

Among the core questions for boards and board committees to keep in mind:

- Do the management team members responsible for specific risks understand the scope and magnitude of the risk being managed by third parties and whether that risk is appropriately managed and controlled in line with the company's policies?
- Does management have a complete risk-ranked inventory of critical services provided by third parties, including subcontractors?
- How often does the board want updates on third-party risk from management? How is the information provided? Is data available in real time?
- Where should board oversight of third-party risk be housed—full board, risk committee, or another committee? Does the audit committee have responsibility for supply chain risks by design or by default?
- Is the TPRM program approached holistically, as an enterprisewide activity (versus silo-driven) and effectively integrated with risk management and compliance functions?
- Do the TPRM team and other functions have sufficient skills/talent, funding, and technology to keep pace?
- When should the board be involved in the oversight and approval of large or complex services involving third parties?

Contact us

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

John H. Rodi
Partner, Audit, KPMG LLP
Leader, KPMG Board Leadership Center

Greg Matthews
Partner, Advisory, KPMG LLP

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 continues education and improvement of public and private company governance, BLC engages with directors and Business leaders on the critical issues driving board agents—from strategy, risk, talent, and ESG to data governance, audit quality, proxy trends, and more. Learn more at kpmg.com/us/blc.

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

kpmg.com/socialmedia