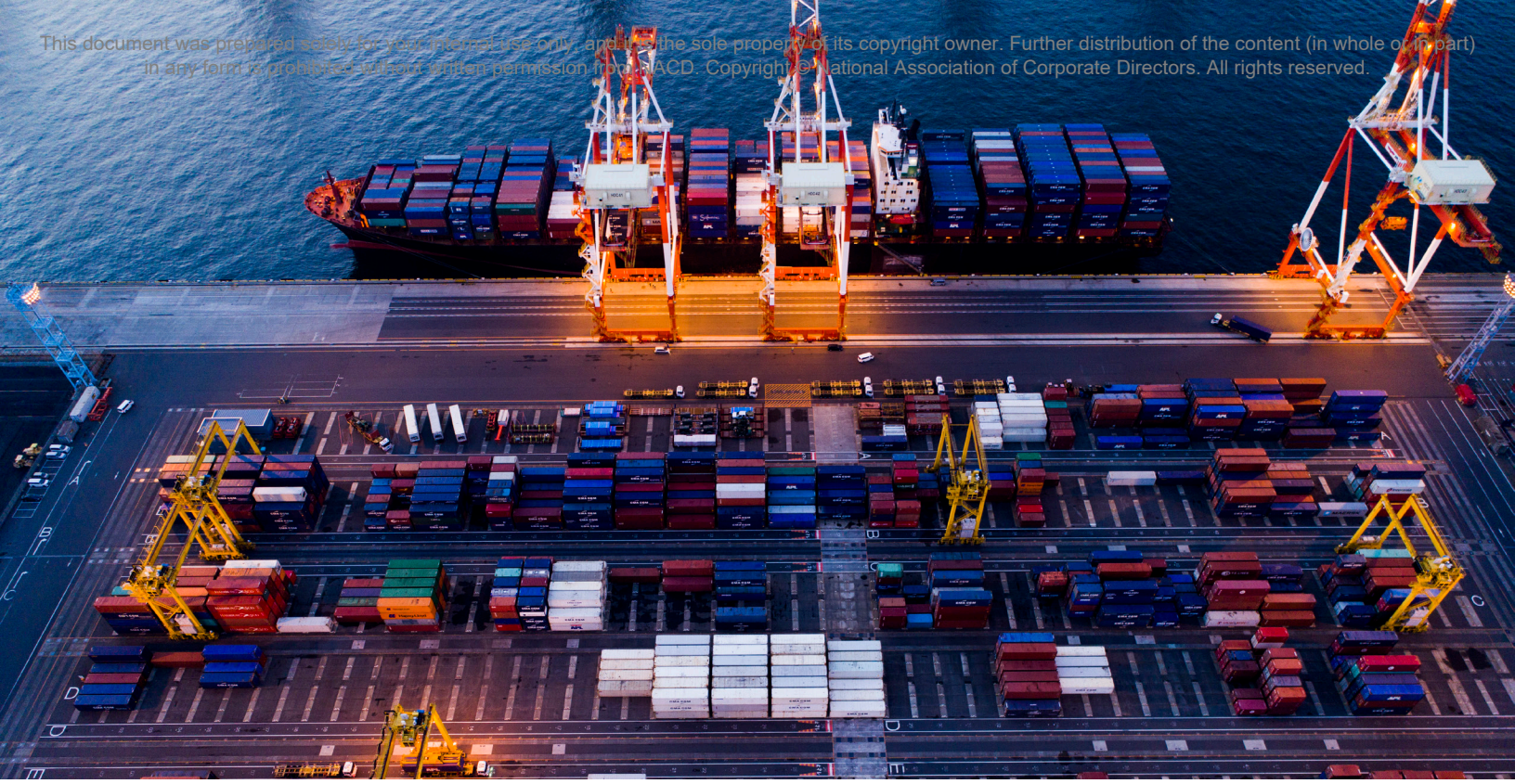

Third-Party Risk Oversight

Growing Engagement, Action Expected at the Board Level

By Dan Kinsella and Adam Thomas, Deloitte & Touche LLP

In many companies, boards of directors and C-suite leaders have seen firsthand how rapidly risks related to third parties can threaten their own company's ability to deliver on its mission and strategy. Some companies have also experienced how significantly the missteps of third parties—as well as fourth parties, fifth parties, and sixth parties in a third-party ecosystem—can tarnish the company's brand and reputation.

As an example of how third-party breakdowns can affect companies, consider which entity is typically the focal point when a supply chain failure leads to outages, cancellations, or other disruptions. Is it the third parties whose failures led to production or service interruptions? Or is it the entity doing business with end users who are left empty handed?

Although pandemic-era supply chain issues have filled the news headlines, supply chain challenges are not new. What is new is the increasing frequency of adverse events that disrupt supply chains, combined with the scope of risk that exists—often undetected—in increasingly dispersed supply chain ecosystems that are often highly interconnected and interdependent.

In many organizations, corporate directors and C-suite leaders are still working to understand the breadth, depth, and significance of their company's relationships with third parties and other business partners, even though it has become an important risk area with possibly far-reaching consequences.

As boards become more engaged with understanding their dependencies on vendors and other third parties, what measures can they take to oversee third-party risk with greater confidence and efficacy? Several possibilities are on the horizon—both actions companies are likely to take with increasing frequency and actions boards can task management with considering (if they are not already on management's radar).

KEY PROJECTIONS

Managing third-party resilience. Due to the impacts of COVID-19-related supply chain challenges, many organizations have elevated their focus on their third-party networks, the strategic impact of third-party failures, and the importance of improving resilience in third-party ecosystems.

According to Deloitte Global's 2022 global third-party risk management (TPRM) survey, 60 percent of respondents say resilience and business continuity planning is a strength in an organization, but only 36 percent indicate they have high or very high global supply chain contingency management capability, and 21 percent report lower or very low capability.[1]

Third-party risk includes not just those entities where a company has direct contractual relationships but also fourth, fifth, sixth, or even more extended participants in a supply chain ecosystem. A growing number of companies have developed reliance on such entities to meet strategic objectives, not just to achieve a cost reduction or other short-term objective. Awareness is also growing about the importance of managing a broad variety of partners beyond suppliers whose activities represent risk: joint venture or alliance partners, subsidiaries, affiliates, retailers, distributors, service providers, agents, brokers, and franchisees.

Companies increasingly recognize how interconnected and interdependent they have become with these entities, which presents an opportunity for companies to perform analysis on financial and operational metrics to help spotlight third parties that may be better positioned to help the company achieve its objectives. This might include vendors of goods and services, but it could also include sales agents or franchisees, for example, who should be targeted for growth opportunities. These types of third parties are often overlooked.

Companies are expected to demonstrate an increased strategic alignment between sourcing, business, and risk management objectives, which can drive decisions, governance, and operating models.

Interconnectedness also helps companies to identify where a breakdown may be accelerated or exacerbated by real-time technologies. Consider, for example, how quickly real-time access across supplier networks can multiply errors or allow a cybercriminal to access systems and data.

This focus on resilience is expected to continue to intensify in the coming year, as a newer spectrum of risks across a growing number of domains—geopolitical; geographic or supplier concentration; export controls; and sanctions—continues to develop. Companies are expected to demonstrate an increased strategic alignment between sourcing, business, and risk management objectives, which can drive decisions, governance, and operating models.

Integrated TPRM. To help provide a more efficient and effective approach to TPRM, some organizations are generally expected to prioritize the integration of contract and legal management systems with TPRM to develop a broader approach to managing complex risks.

Data from the TPRM survey indicate 70 percent of respondents want to drive a more integrated approach to increase efficiency by avoiding duplication across functional teams and exploiting synergies across TPRM processes. The survey further indicates that approximately two-thirds of

[1] Deloitte, *Emerging Stronger: The Rise of Sustainable and Resilient Supply Chains* (New York, NY: Deloitte Touche Tohmatsu Ltd., 2022), p. 13.

participating TPRM teams already recognize that the scope of their work is broadening into related functional areas, such as contract and legal management (63%), business continuity and resilience management (51%), and third-party performance management (51%).

Survey responses suggest varied organizational priorities for widening the scope of TPRM: improved contract and performance management, business continuity and resilience, and improved management of relationships, financial performance, and data. Despite intentions, only 23 percent of respondents indicate their organizations have been able to make significant progress in integration, which suggests companies may want to consider prioritizing further integration in the coming year.

Opportunities for integrated TPRM are expected to continue to increase for companies that have made the necessary investments. Transformation is more likely in organizations that expand their focus beyond narrow cost-savings objectives to consider more broadly the possibility of profitable growth using a customer-centric approach. Improved integration is also more likely where companies adopt more accurate forecasting techniques and improved visibility into the lowest tiers of their extended enterprises.

Many companies are recognizing the challenges of historic, reactive approaches to risk identification and response, increasingly taking steps to becomemore proactive and responsive at greater speed.

Boards can have an important role in promoting a more integrated approach to TPRM by asking probing questions of management regarding its understanding of risk in third-party relationships that exist in the lower tiers of the extended enterprise.

Increased move to real-time or near-time identification of risks and mitigation responses across supply chains. Companies are expected to increasingly move from point-in-time risk management toward approaches that are more real time, near time, or continual. Many companies are recognizing the challenges of historic, reactive approaches to risk identification and response, increasingly taking steps to become more proactive and responsive at greater speed.

Digital transformation is an important foundation for achieving such a shift. With increased use of more advanced digital technology, continual monitoring can become a substitute for point-in-time assessments to leverage real-time data feeds and analytical capabilities that provide improved, more actionable insights regarding threats and vulnerabilities.

Technology can also enable more forward-looking indications of risk instead of relying on historic information that provides lagging indications of where risk may be accelerating or increasing. Dashboards can present data on key risk indicators as well as anomalies that merit further intervention, which can be undertaken more rapidly. Companies can increase their focus on improving not only their gathering of risk data but also their interpretation of data and their responses.

Understanding environmental, social, and governance (ESG) risks. Awareness and actions are expected to grow incrementally regarding the ESG risks that exist within third-party networks. As an example, evolving regulatory requirements with respect to Scope 1, 2, and 3 carbon emissions may drive an increased focus in this area. In another area of ESG, diversity, equity, and inclusion, or DE&I, is an important topic where many companies are increasing their focus on relationships with third parties as they seek to increase their relationships with diverse suppliers and as stakeholders ask questions about where and how goods and services are sourced.

Organizations are expected to place an increased focus on the quality of internal and external data used for managing and reporting ESG factors related to their extended enterprise of third parties. According to Deloitte's TPRM survey, there's room for growth in this area; only 49 percent of respondents indicated their companies have formal mechanisms in place to monitor internal and external changes to relevant ESG-related risk information, and only 16 percent indicated the quality of their internal data is high or very high.[2]

The complexity of defining, identifying, and reporting on ESG risk is growing as companies seek increased understanding of their third-party relationships and how they may affect ESG strategy. Many companies are recognizing that high-quality internal and external data is key to understanding and managing ESG risks in complex supply chain ecosystems. An integrated, broad view of the extended enterprise is a clear prerequisite to identifying data-related needs and addressing ESG considerations across enterprise activity.

MAJOR BOARD IMPLICATIONS

As recent trends and elevated risk levels have shone a spotlight on the scope and depth of third-party risk in many companies, the board and C-suite are generally expected to increase their engagement on TPRM, which may drive increased investment in a quest for transformational change. Boards can hold C-suite leaders accountable for demonstrating a laser focus on managing identified risks compared with a check-the-box program, with a clear operating model that defines process owners, controls, and accountability, as through goals and compensation.

In response to the challenges that are driving third-party risk, boards may consider several ways they can increase their level of understanding and engagement on the scope of risk and opportunity. Board actions may include the following:

- Boards may devote more space and time on their agendas to third-party risk, engaging with C-suite leaders on key risks, management and mitigation strategies, and plans for developing a more integrated approach to TPRM.
- Board members may consider more carefully where responsibility for oversight of these critical areas resides within the board and its committee structure as well as among management.
- Boards may task C-suite leaders with providing an improved quality of information about the third-party ecosystem providing goods and services that are core and noncore to the company's strategy and execution.
- Boards may require more frequent or recurring risk reporting based on the risk profile of critical business partners.
- Boards may hold management accountable for setting and meeting targets for improving TPRM while more closely monitoring this activity.
- Boards may increase investment in extended enterprise digital platforms that provide more real-time insights into evolving and emerging third-party risks to enable more proactive, near-time responses to mitigate risks. Boards can encourage C-suite leaders to consider multiyear investments in an integrated technology architecture and automation across

[2] Deloitte, *Emerging Stronger: The Rise of Sustainable and Resilient Supply Chains* (New York, NY: Deloitte Touche Tohmatsu Ltd., 2022), p. 10.

sourcing and risk management platforms. Such investment could lead to increased focus on customer characteristics and experience and improve network analysis across third parties, services, and risk categories.

BOARD OVERSIGHT QUESTIONS

1. Where does oversight responsibility for third-party risk reside within the board and its committee structure? Where does responsibility reside within management?
2. What information is the board receiving from management with respect to third-party risk? With what levels of quality, frequency, and relevance is the information presented?
3. To what extent does information presented by management enable a well-informed TPRM strategy, and how can the information be improved?
4. What are the key risks the company faces stemming from third parties? What are the key risks from more extended suppliers, such as fourth, fifth, or sixth parties?
5. To what extent are siloed processes exacerbating the company's approach to TPRM, and how can TPRM be more broadly integrated?
6. What tools does the company use to measure and manage TPRM, and how effective are they? How are third-party risks escalated? How effectively does escalation trigger mitigation responses, and how effective are mitigation responses?
7. What investments could the company consider to improve its approach to TPRM and integrate it across the enterprise?
8. What skill sets does the board have to advise management on third-party risk and opportunity?

Dan Kinsella is the Americas extended-enterprise and third-party assurance leader for Deloitte & Touche LLP and serves as managing partner of Deloitte's Omaha office. Combining business and technology experience to help clients create and enhance their extended enterprise through cost and revenue recovery services, Kinsella specializes in creating efficient exchange of risk information synergies in the marketplace. He leads Advisory Service Delivery Transformation, helping clients' efforts in shared services and outsourcing environment improvements.

Adam Thomas, a principal with Deloitte & Touche LLP, is the Extended Enterprise offering leader for the Cyber & Strategic Risk portfolio of Deloitte Risk & Financial Advisory. He has more than 20 years of experience in the field of risk management, with a focus on helping to design and implement third-party, technology risk management, and cybersecurity programs for complex, regulated global financial services firms. He has assisted with many significant third-party risk program transformations in response to various risk and compliance-related concerns, and he led the development of Deloitte's program for managing its third-party risk as well as several third-party risk utilities focused on the financial services industry.