Third Party Risk Management:

A boardroom perspective

Board Leadership Center

In today's highly interconnected business world, organisations increasingly rely on third parties – such as vendors, suppliers, cloud service providers, consultants, and partners to perform critical functions, provide essential services, and support strategic objectives. While this reliance offers significant benefits such as cost savings, access to specialised expertise, and operational efficiencies, it also introduces organisations to a complex web of risks that can impact its organisational, financial and reputational standing. As regulatory expectations evolve, organisations are now being compelled to extend their risk management efforts beyond third parties, reaching into fourth-party relationships.

Many organisations already have robust Third-party Risk Management (TPRM) programmes in place as a strategic imperative today. However, they face a significant challenge in ensuring that these programmes are aligned with the rapidly changing risk, regulatory, and compliance environment allowing for board oversight on management's efforts to maintain effective TPRM programmes. Effective board oversight ensures that robust TPRM frameworks are in place to identify, assess, and mitigate risks associated with third-party relationships, safeguarding the organisation's integrity and success.

Emerging risks

01 **Cybersecurity and data privacy risks:** Cybersecurity and data privacy rank among the top third-party risks, posing unique challenges for companies striving to maintain continuous monitoring and real-time visibility. It is critical to ensure that management establishes robust communication plans with third-party service providers, facilitating timely assessment and disclosure of significant cybersecurity incidents

02 **Risks posed by use of AI tools:** Companies are increasingly aware of the risks associated with integrating third-party AI tools, including open-source models, vendor platforms, and commercial Application Programming Interfaces (APIs). This integration complicates internal and external distinctions in AI strategies. Consequently, companies should reevaluate their AI governance structure to better manage the development, deployment, and protection of AI systems and models, especially those using third-party AI tools

03 **Third-party climate, sustainability, and other ESG risks:** As businesses integrate complex supply chains and partnerships, they face heightened exposure to the sustainability practices of their supply chain business partners. With growing regulatory expectations and investor/consumer scrutiny, boards should look to integrate ESG related disclosures into their risk management and due diligence assessments

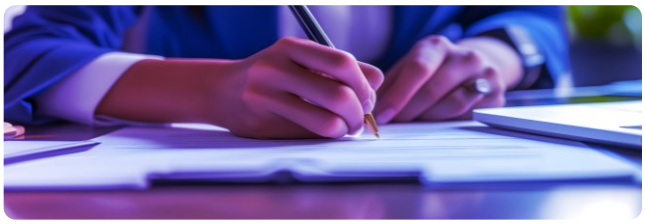
04 **Business operations vulnerabilities and improve resilience:** In the past years, companies have faced unprecedented operational stresses and failures forcing them to 'de-risk' their supply chains to address these vulnerabilities and improve resilience. This includes updating disaster recovery plans, diversifying suppliers, reducing dependency, and improving cybersecurity. The board should ensure these critical projects are effectively managed, maintaining a strategic vision to address the broader objectives

05 **Risks related to hiring of third-party staff:** Today's business environment faces heightened risks of fraud, data breaches, and compliance violations. Inadequately vetted third-party staff can lead to security vulnerabilities, operational inefficiencies, and subpar performance. To mitigate these risks, companies must conduct thorough background checks, evaluate third-party recruitment practices, and perform regular audits to ensure adherence to the company standards and regulatory requirements.

Key focus areas for boards

1. Risk assessment and due diligence:

Boards must ensure that robust processes are in place for assessing and managing risks associated with third parties. This involves thorough due diligence before entering into agreement with any third party through investigative measures such as forensic audits and evaluation of a vendor's cyber security protocol such as data encryption, firewalls, access controls and vulnerability management. Boards must also ensure that due diligence processes are not just a one-time activity but are continuously updated to address evolving risks.



Questions for boards:

- Are we considering 'third party risk' as a factor in evaluating the need of third-party services?
- Are we effectively prioritising our third-party portfolio based on risk assessments?
- Is our population of services sufficiently stratified to allow us to focus on higher-risk services?
- How comprehensive are our due diligence processes in identifying potential third-party risks?
- Are we ensuring inclusion of geopolitical factors as part of assessing third parties?
- Do we have established metrics to provide a comprehensive view on our risk exposure?

Questions for boards:

- Are compliance obligations and expectations clearly defined and embedded within our contracts with third parties?
- Are contracts with third parties regularly reviewed and updated to reflect current risks and regulatory requirements? Are we constantly updating third-parties on risks that can not be transferred to third party in letter and spirit (like reputation)?
- Are there any measures in place to ensure third party compliance with these contractual and regulatory obligations?

2. Contract management and compliance obligations:

Boards should embed appropriate risk and compliance obligations within third-party contracts and ensure that there are adaptive compliance clauses that automatically update to reflect latest changes and developments in the TPRM framework, avoiding the need for manual contract revisions.

3. Monitoring and reporting framework:

Continuous monitoring of third-party activities and performance is essential for early detection of potential risk and issues. As the business environment evolves, the third party's management structure and internal controls can increase exposure to risk and liability. To integrate third-party compliance into their own compliance programmes, firms should request third-party compliance reports such as SOC 1 and SOC 2 reports.

Questions for boards:

- Who is responsible for oversight of third-party risks? Should it be the risk committee, the audit committee, or the entire board?
- What tools and techniques are used for constant monitoring and auditing of third-party performance?
- Are we leveraging real-time data to its fullest potential to monitor third parties?
- What safeguards are in place in the contract to ensure third parties meet their obligations?
- How does the board ensure that due diligence process for TPRM is both comprehensive and integrated into TPRM framework?

Questions for boards:

- How prepared are we to respond to incidents involving third parties? What are the key components of our incident response and recovery plans?
- Do we have an appropriate plan in place for key third parties and/or services that have high-priority regulatory requirements associated with them?
- Do we have a system in place to swiftly direct and manage reports of incidents/ breaches?
- How trustworthy are the recovery and resumption plans? Have they been tested?

5. Regulatory and legal compliance: Compliance with relevant regulations and legal requirements is a critical aspect of TPRM. Companies should ensure that the third parties they are associated with, adhere to all applicable laws and standards to avoid regulatory penalties and legal liabilities.

Questions for boards:

- How effectively does our TPRM framework address risks related to cloud services, software supply chains, and AI technologies, including cyber threats and data privacy concerns?
- Are we ensuring that our organisation's reliance on digital supply chains aligns with evolving regulatory requirements?

7. Cyber resilience: As cyber threats loom larger, boards need to ensure that robust cybersecurity measures are embedded within governance frameworks to anticipate, withstand, and recover from potential breaches. There is need for continuous and real-time testing of organisational resilience to safeguard organisational integrity and stakeholder trust.

4. Incident response and recovery: Due to the increasing complexity and interconnectedness of global supply chains which amplify the impact of third-party risks, boards must establish clear protocols for incident reporting and recovery. This includes defining roles and responsibilities for remediation and escalation to ensure prompt and effective responses to any issues.

Questions for boards:

- Does the management keep track of the regulatory requirements that impact the company's third-party relationships? Do we have a plan in motion to ensure strict compliance?
- What processes are in place to manage regulatory changes and their impact on third-party risks?

6. Digital supply chain: With increasing digitization of businesses, there is a critical need for boards to manage risks across their digital supply chains including cloud service providers, software supply chains, AI vendors, etc.

Questions for boards:

- Are our TPRM frameworks equipped to effectively mitigate and recover from third-party cyber risks?
- How frequently do we update our cybersecurity measures to address evolving threats in our digital and third-party ecosystems?

Leading ways which boards can consider to optimise TPRM framework in organisations

Adopting a risk-based approach: Boards should consider implementing a risk-based approach that differentiates third parties by their inherent risk levels and the depth of assessments with associated risks.

Centralising oversight and governance: Adopt a multidisciplinary approach using a hub-and-spoke model where the TPRM function will act as a central hub supported by subject matter experts ('spokes') from relevant risk domains, such as privacy, cyber, business continuity etc.

Leveraging technology and advanced tools: Leverage the power of cutting-edge technology to strategically allocate precious human resources towards critical functions such as analysis and decision-making and staying abreast on regulatory requirements and compliance obligations.

Providing continuous education and training: Invest in regular training programs for board members and key stakeholders across the firm on emerging risks, regulatory updates, and best practices in TPRM. Additionally, considering the increasing reliance of firms on third parties for critical functions, it is prudent to extend that training to them as well.

Establishing crisis management protocols and resilience plans: Develop and refine incident response and recovery plans, clearly defining roles and responsibilities to handle third-party risk events and develop resilience plans.

Integrating compliance programs: Align third-party risk management with the overall enterprise risk management and compliance strategies to ensure a cohesive approach.

Stakeholder engagement: Foster open communication with stakeholders, including regulators, investors, and customers, to build trust and demonstrate robust TPRM practices.

Taking proactive measures and make it a continuous process: Encourage a culture of continuous improvement, leveraging feedback and learnings to enhance the framework on regular basis rather than just once.

Establishing three lines of defence in TPRM framework: Using three lines of defence model to ensure a robust and coordinated defense against third-party risks and spilt of roles and responsibilities across the organisation.

Broadening the scope of third-party relationships: Boards should extend their definition of third parties beyond traditional suppliers and distributors to encompass all entities involved in the supply chain, including agents, NGOs, staffing partners etc..

Avoiding process overcomplication: Over-engineering TPRM processes can lead to unnecessary complexity. A practical, risk-based approach is essential to create an effective and manageable framework.

Assessment of internal controls and risk management at the outset: While continuous monitoring of a third party's internal risk controls is desirable, companies are better placed to identify and mitigate risk by association, if they verify their internal controls and risk management practices at the outset.

Your contacts:

Bob Dillen
Partner, Head of Forensic
E: bdillen@kpmg.com

Cédric Biedermann
Director, Forensic Western Switzerland
E: cbiedermann@kpmg.com

Rolf Hauenstein
Partner, Head of Markets Audit,
Head of Board Leadership Center
E: rhauenstein@kpmg.com

KPMG AG
Badenerstrasse 172
8004 Zurich
Switzerland

kpmg.ch