Awareness and actions at the forefront of third-party risk management

November 2024

kpmg.com/in

KPMG. Make the Difference.

In an increasingly interconnected global business environment, firms are becoming more reliant on third parties for critical operations, processes, and functions. Globally, regulatory bodies are emphasising for transparency in third party relationships, setting higher standards for risk oversight. This shift isn't just a strategic imperative, but it's a recognition of third-party risk management (TPRM) as cornerstone of responsible and ethical business practices.

The pulse of modern business comes with rising risks

In the intricate web of modern businesses, third parties – including suppliers, business partners, vendors, contractors, service providers, customers, as well as the fourth, fifth and nth parties are essential. But they also come with apparent and hidden risks, ranging from compliance with regulations to addressing cybersecurity and data protection risks.[1]

According to a recent survey conducted by KPMG International, **three-quarters of respondents said that their company faced major reputational risks and business disruptions** because of a third party in the last three years.

1. Ten ways to optimize your TPRM program – KPMG International, 2024; Third-Party Risk Management Outlook – KPMG International, January 2022

When a third-party falters, the impact cascades like dominoes: for instance, operational setbacks may lead to financial strain, reputational harm, and shaken stakeholder trust. While some risks are visible, others remain hidden along the way.[2]

What's apparent?

- Regulatory and compliance risk
- Brand and reputational risk
- Fraud and corruption risk
- Operational risk
- Financial risk
- Strategic risk.

What's hidden?

- Cyber and privacy risk
- Business continuity and resiliency risks
- Environment, health and safety risk
- Hidden liability and legal exposure
- Geopolitical risk
- Concentration risk.

Global regulatory actions put third-party relations under the scanner

As businesses face an expanding array of regulations, third-party relationships are taking centre stage. In India, the regulatory framework for TPRM has been strengthened in recent years, with specific guidelines issued by key regulators. One such regulation is the Reserve Bank of India's master direction on outsourcing of information technology services[3] to third parties, introduced in November 2023. This aims to highlight the importance of identification, measurement, mitigation, management, and reporting of third-party risks.

Globally, TPRM has evolved to address the emerging risks with increasing use of third parties. Some highlights from major markets include[4]:

European Union

The **Digital Operational Resilience Act (DORA)** unifies information and communication technology (ICT) third-party risk in the financial sector.

United States

In 2023, the Office of the Comptroller of the Currency (OCC), jointly with other regulatory bodies, issued guidance **'Interagency guidance on third-party relationships: risk management'** on managing third-party risks.

United Kingdom

In 2021, the **Prudential Regulation Authority (PRA)** issued a supervisory statement outlining expectations for PRA-regulated firms on outsourcing and third-party risk management compliance.

Australia

The Australian Prudential Regulation Authority (APRA) detailed third-party management requirements, including the 2023 **"Prudential practice guide: draft CPS 230 operational management."**

2. Types of Third-party Risk – Central AI, June 2022; Top 5 Third-Party Risks – ISG; TPRM – Service Now; TPRM: A guide for community banks – OCC, May 2024
3. Master Direction on Outsourcing of Information Technology Services – RBI, April 2023
4. DORA – European Securities and Markets Authority, January 2024; TPRM: A guide for community banks – OCC, May 2024; TPRM: A guide for community banks – FRB, May 2024; Interagency Guidance on Third-Party Relationships: Risk Management – FDIC, June 2023; SS2/21 Outsourcing and third party risk management – Bank of England, March 2021; Prudential Practice Guide – APRA, July 2023

Redefining third-party risk: from basics to breakthroughs

While traditional TPRM is integral to organisational resilience, a closer examination reveals significant gaps. The fast-evolving risk landscape and the complexities of modern markets leave organisations increasingly vulnerable to unforeseen threats[5].

Inefficiencies in traditional TPRM framework

- Tick-box compliance, rather than actual risk reduction
- One-size-fits-all solutions for all
- Inadequate subjective scoring
- Static evaluations, rarely adapting to changing vendor landscapes
- Overlook industry-specific risks.

Ineffective outcomes for businesses

- False assurance from incomplete assessments
- Overlooked risks, due to overreliance on questionnaires
- Misallocated resources
- Repeated assessments strain vendor relationships
- Lack of actionable strategies for risk mitigation.

5. The Farce and Ineffectiveness of Third- and Fourth-Party Risk Assessments – LinkedIn, October 2024
6. Ten ways to optimize your TPRM program – KPMG International, 2024; Risk monitoring best practices – Fraud.com; How TPRM needs to evolve– LinkedIn, July 2023; TPRM: A boardroom perspective, KPMG India, 2024

As organisations face an evolving risk landscape, traditional third-party oversight methods reveal critical gaps. However, by embracing modern strategies, businesses can move beyond compliance checklists to create a more adaptive and resilient approach to managing risks. Some highlights[6]:

Implementing a risk-based approach

Adopting a risk-based approach is essential for effective TPRM. By **focusing on the high-risk third parties**, organisations can better safeguard their operations. This ensures that **high-risk areas**, such as politically exposed persons or jurisdictions with high corruption levels, **receive focused attention.**

Defined contractual requirements

Incorporating **compliance obligations directly into contracts** can be crucial for effective regulatory adherence. By utilising adaptive clauses, organsations can **minimise the need for manual revisions and guarantees continuous compliance**, allowing focus on strategic growth.

Creating a risk management framework

Establishing and integrating **end-to-end risk management** allows for the **analysis of the overall TPRM framework** using metrics from ongoing monitoring. Protocols should link incidents to their impact on the firm and the risk rating of the third party

Governance and structure

To respond to complex risks, organisations should adopt a **hub-and-spoke model** for TPRM. The TPRM function acts as the hub, with subject matter experts from various risk domains as the spokes, providing crucial insights.

Leveraging technology and automation

Implementing technology can be a game changer for enhancing routine operations in TPRM. Advanced tools can streamline risk assessments, enhance due diligence, and automate monitoring activities, providing real-time insights to stay ahead of potential threats.

Effective ongoing monitoring

By continuously assessing the third-party risk profiles and contract performances, organisations can establish a **comprehensive view of key metrics** across all third-party relationships.

Centralised third-party inventory

A single, unified inventory of third parties provide a clear view of risk exposure and simplifies compliance tracking. This approach boosts visibility and enhances proactive management of potential risks.

Concentration risk analysis

Conducting concentration risk analysis helps identify if the organisation is overly reliant on specific third parties. By assessing dependency levels, businesses can reduce the risk of disruptions from single source partners.

Establishing three lines of defence in TPRM framework

Using three lines of defence model to ensure a robust and coordinated defence against third-party risks and spilt of roles and responsibilities across the organisation

Convergence

Organisations now approach third-party risk with **integrated, multidisciplinary approaches**. Functions like procurement, legal, cybersecurity, privacy, finance, and business work together to understand and mitigate these risks holistically.

6. Ten ways to optimize your TPRM program – KPMG International, 2024; Risk monitoring best practices – Fraud.com; How TPRM needs to evolve– LinkedIn, July 2023; TPRM: A boardroom perspective, KPMG India, 2024

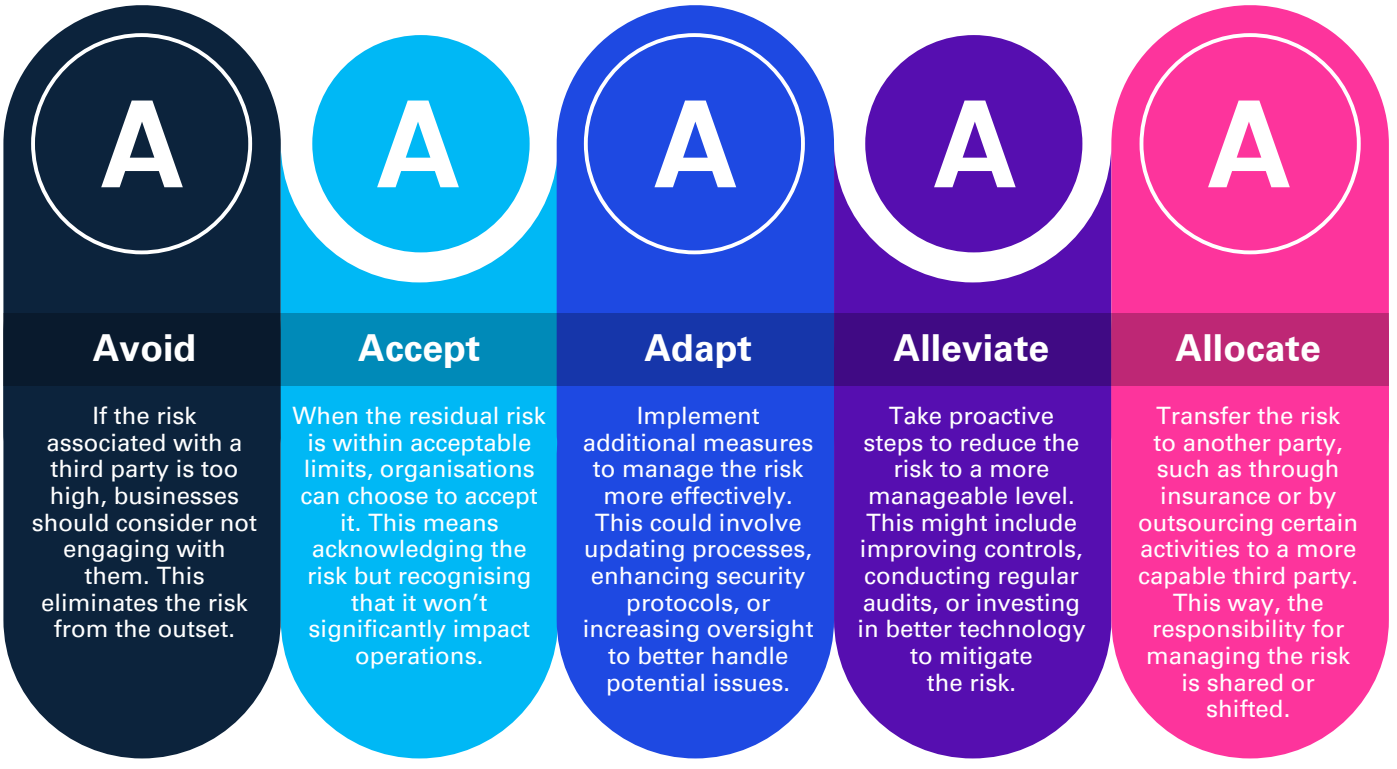
Assessing an organisations' TPRM programme maturity ?

- Is the TPRM programme implemented as a holistic, organisation-wide initiative that effectively integrates risk management and compliance functions?
- Are the specific expectations and obligations of both the organisation and the third party clearly outlined in a written contract? Additionally, do these contracts include clauses addressing adaptive requirements, audit rights, incident reporting, and consequences for compliance breaches?
- What processes are established for conducting due diligence on third parties both before and after engagement? Are these processes customised according to the risk profile of each third party?
- Is there a system in place to promptly address and manage reports of incidents or breaches? How does it integrate with enterprise risk management?
- Does the organisation have a cohesive technology strategy that aligns with the overall TPRM programme while also addressing the specific needs of individual risks and business units?
- Is the organisation fully leveraging real-time data to monitor third parties effectively? Additionally, what safeguards are included in our contracts to ensure that third parties meet their obligations?

Mitigating the last mile: reducing residual third-party risks[7]

An effective outcome of a well-functioning TPRM programme is enhancing an organisation's ability to identify and manage the residual risks associated with its third-party universe. Residual risk can be visualised as the risk which continues to be associated with the engagement (or entity) that the organisation may continue to have despite the diligence and controls framework. The following framework can help guide an organisation's response to residual risk:

Tips to mitigate residual risk with 5 As:



7. How to Determine Residual Third-Party Risk and Next Steps – Verminder, Third Party Risk Association Blog, August 2024; The (mis)perception of risk maturity – KPMG Switzerland, 2020

Conclusion

The terrain of third-party risk management (TPRM) is swiftly transforming, driven by tech-driven changes, regulatory shifts, and newer and emerging risks. Effective TPRM isn't just about dodging failures or ensuring regulatory compliance, but also a method to streamline operations and improve business outcomes.

The distinction between external and internal risks is increasingly becoming blurred. Modern practices require an integrated strategy that combines vendor risk management with internal risk frameworks, creating a cohesive and comprehensive defence mechanism. While not exhaustive, below are a few actional insights for getting the TPRM right:

- **Empower accountability**
- **Focus on the big risks**
- **Strengthen your digital shield**
- **Track and refresh third-party profiles**
- **Collaborative ecosystems**
- **Scope partnership for risk**
- **Rely on trust, reinforce with checks**

KPMG in India's experience underscores that an evolving third-party ecosystem demands a significant understanding of emerging risks. Organisations that overlook these rapid changes risk falling behind, making it essential to implement adaptive strategies that ensure robust oversight and informed decision-making. By leaning into these trends and evolving our strategies, we're not just mitigating risks—we're building a secure, compliant, and resilient organisation.

KPMG in India contacts:

Akhilesh Tuteja
Head – Clients & Markets
P: +91 124 254 9191
E: atuteja@kpmg.com

Manoj Kumar Vijai
Office Managing Partner and Head – Risk Advisory
P: +91 22 6257 1056
E: mkumar@kpmg.com

Rajosik Banerjee
Head Financial Risk Management and
Deputy Head – Risk Advisory
P: +91 22 6134 9200
E: rajosik@kpmg.com

Maneesha Garg
Partner and Head – Managed Services
Forensic, F&A, HR, Learning, Insight Led Sales,
Digital Business Operations and Sourcing
P: +91 120 386 8000
E: maneesha@kpmg.com

Vipul Jain
Partner – Managed Services
Forensic
P: +91 124 336 9001
E: vipuljain@kpmg.com

Ummehaani
Partner – Managed Services
Forensic
P: +91 2040194000
E: ummehaani@kpmg.com

kpmg.com/in

Follow us on:

kpmg.com/in/socialmedia

Access our latest insights on KPMG Insights Edge