Third-party risk management (TPRM)

Compliance with RBI circulars on TPRM

August 2023

pwc

Overview of regulatory requirements for third-party risk management (TPRM)

Through its circulars dated 10 April 2023 and 3 November 2006,* the Reserve Bank of India (RBI) highlighted various aspects that banks should observe in their operational controls and governance structure while outsourcing services. Some of the key aspects are listed below:

01 **Outsourcing risks** to be assessed around some key risks such as strategic risk, reputation risk, compliance risk, operational risk, legal risk, exit strategy risk, counterparty risk, country risk, contractual risk, access risk, concentration and systemic risk.

02 Outsource financial and information technology services but **refrain from outsourcing core management functions, including internal audit, compliance and decision-making functions**.

03 **Bank to always retain ultimate control of outsourced activity** and should not affect the rights of a customer against the bank, including the ability of the customer to obtain redress as applicable under relevant laws.

04 Establish a **comprehensive outsourcing policy, approved by its board**, which incorporates a criterion for selection of such activities as well as service providers/vendors and parameters for defining material outsourcing.

05 **Defined roles and responsibilities** of senior management and the board.

06 Seek to ensure the preservation and protection of the security and confidentiality of customer information. Access to customer information by staff of the service provider should be on a 'need to know' basis.

07 Banks need to ensure that service providers periodically tests their business continuity and recovery plan. They also need to conduct occasional joint testing and recovery exercises with their service providers.

08 The bank should have in place a management structure to monitor and control its outsourcing activities. Regular audits by either the internal auditors or external auditors of the bank should assess the adequacy of the risk management practices adopted in overseeing and managing the outsourcing arrangement, the bank's compliance with its risk management framework and the requirements of these guidelines. Banks should, at least on an annual basis, review the financial and operational conditions of the service provider to assess its ability to continue to meet its outsourcing obligations.

09 **Due diligence** to be performed to assess the capability of the service provider/vendor to comply with obligations in the outsourcing agreement and should include:

- evaluation of past experience and capability to implement
- investigation of security and internal control, audit coverage, reporting and monitoring environment and business continuity management of the service provider/vendor
- ensuring due diligence is conducted by the service provider/vendor of its employees
- the contract should provide for continuous monitoring and assessment by the bank
- the service provider/vendor should provide the bank with the right to conduct audits and obtain copies of any audit or review reports and findings made on the service provider/vendor.

* 1) RBI/2006/167 DBOD.NO.BP. 40/ 21.04.158/ 2006-07
2) RBI/2023-24/102 DoS.CO.CSITEG/SEC.1/31.01.015/2023-24

Despite being run for many years, operational issues exist in a TPRM programme

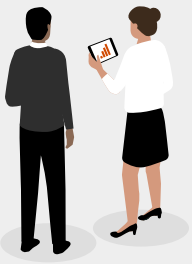
Through multiple regulatory circulars and guidelines, the RBI has consistently maintained that third-party risk needs to be addressed holistically by banks and other financial institutions. Despite the numerous controls that organisations have put in place to address these risks, challenges and inefficiencies remain. Banks and financial institutions need to up their programme governance to ensure that they are in control of outsourcing risks.

Third-party risks

- **Compliance risk:** Non-compliance with statutory and regulatory requirements
- **Concentration risk:** Supplier concentration across services and skills
- **Contractual risk:** Unfavourable clauses, insufficient coverage of all clauses in third-party contracts
- **Cyber risk:** Security breach and data leakage from third party's database
- **Environmental, social and governance (ESG) risk:** Higher scrutiny from regulators amid increased awareness of climate sustainability
- **Financial risk:** Failure to fulfil contractual obligations, putting the third party's going concern status in question
- **Fraud and corruption risk:** Frauds and misconduct by third parties
- **Geopolitical risk:** Unsuitable geographical and political business environment
- **Operational risk:** Inadequate services, leading to disruptions which can further lead to threats to business continuity
- **Reputational risk:** Business disruption due to third party's misfunction

Key issues

- Lack of governance model to continuously monitor third-party risks
- Lack of process framework to manage and mitigate third-party risks
- Lack of data to make informed third-party decisions
- Inadequate infrastructure for smooth running of TPRM programme



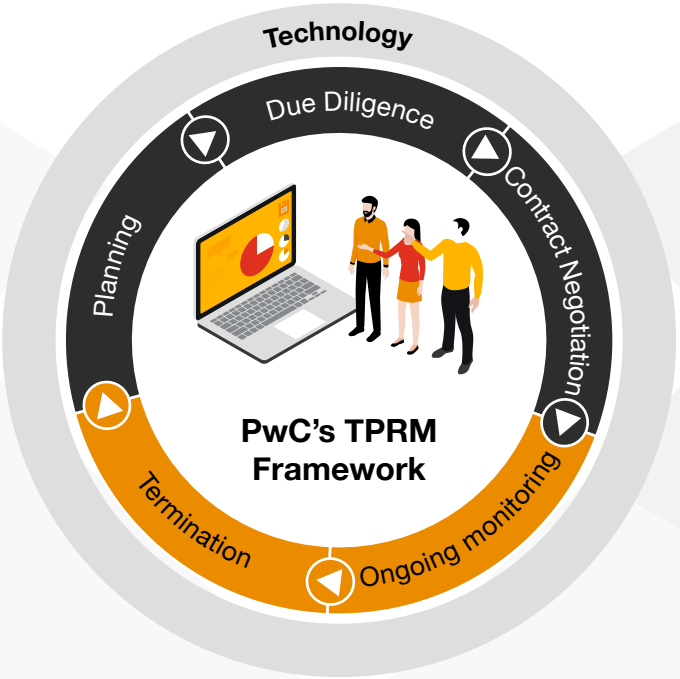
Key impacts

- Vendors with high compliance risks continue to support critical business processes
- Governance and security posture of the enterprise does not percolate to vendors, leaving organisations with risks such as:
  - business disruptions
  - cyberattacks
  - fraud
  - excessive cost
  - regulatory non-compliances
  - penalties resulting from the above
  - resilience issues.

Cornerstone principles of an effective TPRM programme

A robust TPRM framework is focused on understanding and managing risks associated with third parties with which the company does business and/or shares data, to strengthen the organisation's position and build more effective partnerships that protect the brand and business.

Third parties
Vendors
Suppliers
Joint ventures
Business channels
Marketing partners
Affiliates
Subsidiaries
Regulated entities



Risk considerations
Reputational
Operational
Credit/financial
Business continuity and resiliency
Regulatory/compliance
Concentration
Cyber and technology
Info security and privacy
Compliance

There is a need to transform the TPRM programme so that it is forward-looking and meets management's expectations

Desirable end state of an ideal programme – from a senior management perspective

TPRM programme

Desired state TPRM

01 A risk management mechanism that clearly rates a vendor's risk to the enterprise

02 A risk model that allows senior risk leaders of enterprises to block high-risk vendors from working with the enterprise

03 A unified vendor compliance framework that entails a comprehensive review of a vendor at one go, covering all compliance aspects

04 A clear-cut context-based baseline compliance model for vendors to observe at minimum

05 An executive vendor performance dashboard that provides a point-in-time clear-cut status of each vendor, compliance due dates and blacklisted vendors

- Easy to implement
- Clear framework
- Decisive risk view
- Effective control framework

How to optimize your existing TPRM Programme?

The TPRM programme is an ongoing and continuous process. It is driven by constant programme uplifts, process optimisations and innovations:

Strategy & Oversight

- **Applicable laws & standards**
- **Policy & SOP**
- **Set and Maintain global standards**
- **Central Governance, Oversight and Guidance**

Data Sources-
Public databases, Information provided by TPs,
Internal transactional data from CRMs, ERPs

Exiting/ New Third Parties	Third-Party Prioritization	Third-Party Risks Addressed	Risk Assessment Approach
Third-Party Identification	**Materiality** • Spend • Revenue • Strategic Importance • Single Source	1. Financial Risks	Self Assessment (questionnaire)
Third-Party Evaluation	**Third Party Profile** • Inherent Risk • Services/Goods Categorization • Terms of Trade	2. Operational Risks	Desk Research
Third-Party Selection	**Geographical Location** • Geo-political Stability • Corruption Index • Availability	3. Management Risks	On-site Inspection
Third-Party On-board	**Third-Party Risk coverage** • Review Method • Frequency of Review • Reporting	4. AML/KYC & Other Compliances	Off-site Inspection
Third-Party Termination		5. Modern Slavery	Hybrid
		6. ESG Risks	
		7. Cyber & Information Security	

Assess, Monitor and Remediate

Tool- Third Party Risk Tracker

Modules to customize	Dashboards/ Scorecards	Work-flows	Audit trail	Risk Assessment

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Puneet Garkhel
Partner
Partner +91 98203 20181
puneet.garkhel@pwc.com

Mitun Bhattacharjee
Director
Director+91 88794 86112
mitun.bhattacharjee@pwc.com

pwc.in

Data Classification: DC0 (Public)

HS/July 2023 - M&C 30376