BROOKLYN SOLUTIONS

TPRM: RIGHT PEOPLE, SKILLS, PLACE

Organisational Structures & Capabilities within Third Party Risk Management (TPRM) E-Book

Nick Francis

Chief Technology and Marketing Officer
Brooklyn Solutions

Companies increasingly rely on third-party suppliers and partners to drive growth, innovation, and operational efficiency. While these relationships offer significant advantages, they also introduce a wide array of risks that can impact an organisation's financial stability, reputation, and compliance standing. This is where Third-Party Risk Management (TPRM) comes into play.

What is a TPRM Function?

The Third-Party Risk Management (TPRM) function is a strategic approach to identifying, assessing, mitigating, and monitoring risks associated with third-party relationships. This function encompasses the policies, procedures, and practices necessary to manage the entire lifecycle of third-party interactions, from initial selection and due diligence to ongoing monitoring and contract termination.

The core mission of a TPRM function includes:

- Managing Third Parties, Insights, Risks, and associated services pre- and post-contract award.
- Driving the adoption and continuous improvement of Vendor Management best practices.
- Focusing on capturing business value and reducing third-party risk exposure.

Why is TPRM Essential in Customer/Supplier Management?

1. Risk Mitigation:
Third-party relationships can expose organisations to various risks, including operational, financial, legal, compliance, and reputational risks. A robust TPRM function ensures that these risks are identified early and managed proactively to prevent potential disruptions and losses.

2. Regulatory Compliance:
Regulatory bodies worldwide are increasingly scrutinising third-party relationships. Compliance with regulations such as GDPR, DORA, and PRA is critical. TPRM helps organisations maintain adherence to these regulatory requirements, avoiding fines and legal consequences.

3. Business Continuity:
Ensuring that third parties have the capability and resilience to meet contractual obligations is vital for uninterrupted business operations. TPRM evaluates and monitors third-party performance to ensure alignment with organisational goals and continuity of service.

4. Reputational Protection:
Third-party failures or misconduct can significantly damage a company's reputation. Through continuous oversight and risk assessment, TPRM helps safeguard the organisation's brand and public trust.

5. Cost Efficiency:
Effective TPRM practices lead to better vendor performance and optimised contract terms, resulting in cost savings and improved return on investment. By managing third-party risks efficiently, organisations can also avoid costs associated with risk events.

6. Strategic Advantage:
Businesses with mature TPRM functions can make informed decisions about third-party engagements, leveraging these relationships for strategic advantages while minimising potential downsides. This strategic management of third parties can drive innovation and competitive differentiation.

By integrating a comprehensive TPRM function into their Customer/Supplier Management framework, organisations can not only mitigate risks but also harness the full potential of their third-party relationships. This e-book will explore the organisational structures and capabilities essential for a successful TPRM function, providing a roadmap for building a robust and resilient third-party risk management system.

What is the Typical Organisation Structure of a TPRM Function?

TPRM Function Mission

The TPRM Function is comprised of existing Third Party Risk, Vendor Managers, and team members who are dedicated to:

- Managing Third Parties, Insights, Risks, and associated services pre- and post-contract award for the duration of their life.
- Driving adoption and continuous improvement of Vendor Management best practices.
- Focusing on capturing business value and reducing third-party risk exposure.

Responsibilities of a Third-Party Risk Manager

As a Third-Party Risk Manager, your responsibilities will encompass the following: processes and strategies.

1. Oversight and Management:

Take charge of managing and monitoring all third-party relationships in accordance with established risk processes and frameworks.

2. Process Development and Maintenance:

Develop and maintain a comprehensive set of core processes and governance structures to ensure that risk management practices remain effective, efficient, and aligned with organisational objectives.

3. Advisory Role:

Provide guidance and advice to distributed functions and roles across the organization that interact with third parties. Align these functions with best practices in third-party risk management to enhance overall risk mitigation efforts.

4. Collaboration and Continuous Improvement:

Foster collaboration with domain experts in critical functions to gather insights and feedback. Incorporate input from these experts to continuously enhance and refine risk management processes and strategies.

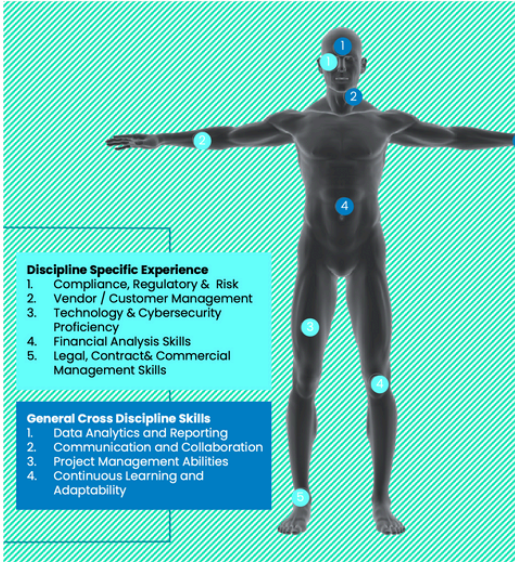
5. Risk Mitigation:

Work towards reducing risk exposure to within acceptable levels for each third-party relationship and across the entire vendor landscape. Develop and implement risk mitigation strategies to align

6. Compliance Enhancement:

Drive compliance initiatives to elevate adherence to regulatory requirements, industry standards, and internal policies. Ensure the effectiveness of control environments to minimise compliance risks associated with third-party relationships.

Capabilities for a TPRM Function



Building a third-party risk management function requires a multidisciplinary team with a diverse set of skills and expertise. Here are the key skills and roles needed to establish an effective third-party risk management function:

TPRM Specific Capabilities

1.Risk Management Expertise:

Individuals with a background in risk management, including experience in identifying, assessing, mitigating, and monitoring risks. Familiarity with risk frameworks, methodologies, and best practices is essential.

2.Compliance and Regulatory Knowledge:

Professionals with expertise in compliance and regulatory requirements relevant to the financial services industry. Understanding regulations such as GDPR, CCPA, SOX, PCI-DSS, and industry-specific regulations is crucial.

3. Vendor Management Skills:

Experience in vendor selection, contract negotiation, performance monitoring, and relationship management. Understanding the complexities of managing third party relationships is key.

4. Cybersecurity Proficiency:

Cybersecurity experts for assessing and managing cybersecurity risks associated with third-party vendors. Knowledge of cybersecurity frameworks, controls, threat intelligence, and incident response is necessary.

5. Financial Analysis Skills:

Expertise in financial analysis to assess the financial stability, viability, and creditworthiness of third-party organisations. Analysing financial statements, ratios, and indicators to evaluate financial risk is required.

6. Legal and Contract Management Skills:

Legal experts to review and negotiate contracts, service level agreements (SLAs), and other legal documents with third-party vendors. Ensuring that contracts

include appropriate risk mitigation measures and compliance requirements is important.

General Capabilities

1.Data Analytics and Reporting Skills:

Proficiency in data analytics to identify trends, patterns, and anomalies related to third-party risk. Ability to generate insightful reports and dashboards for anomalies related to third-party risk. Ability to generate insightful reports and dashboards for decision-making and risk monitoring.

2.Communication and Collaboration Skills:

Effective communication and collaboration skills for engaging stakeholders, building relationships with vendors, and facilitating cross-functional collaboration. Clear and concise communication of complex

3. Project Management Abilities:

Project management skills for planning, executing, and monitoring third-party risk management initiatives. Ensuring tasks are completed on time, within budget, and according to established objectives is crucial.

4.Continuous Learning and Adaptability:

A mindset of continuous learning and adaptability given the evolving nature of third-party risks. Staying updated on emerging risks, industry trends, and best practices in third-party risk management is essential.

By assembling a team with these skills and roles, organisations can establish a robust third-party risk management function capable of effectively identifying, assessing, mitigating, and monitoring risks associated with external vendors and partners.

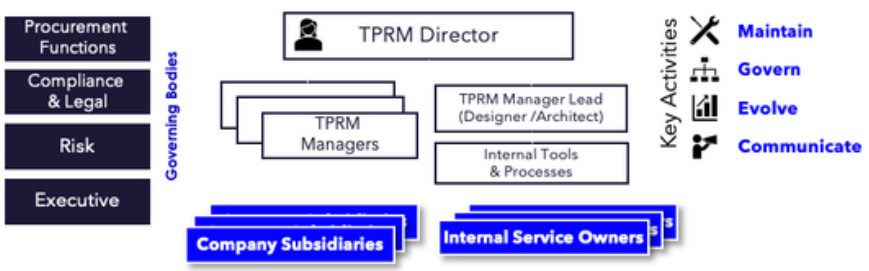
Team Structure

Regarding Third-Party Risk Management (TPRM) teams, selecting the appropriate operating model archetype is paramount. Achieving the necessary balance between control and scalability is essential for effective risk management. Both centralized and decentralized operating models offer distinct advantages and challenges.

- Centralized Model:
  - Maximizes control and quality due to the consolidation of management and oversight functions.
  - Often struggles to scale efficiently and can incur higher costs due to centralized resources and processes.

- Decentralized Model:
  - Distributes control to individuals in direct daily contact with vendors, allowing for more agile decision-making and responsiveness.
  - May compromise overall control and quality, particularly when visibility into vendor activities is limited.

- Hybrid Model:
  - Combines elements of both centralised and decentralised operations in a coordinated and aligned manner.
  - Leverages the strengths of each approach while mitigating their respective weaknesses.
  - Strategic allocation of responsibilities and resources to achieve greater flexibility, responsiveness, and efficiency in managing third-party risks.



Crucially, the success of any operating model relies on the support of high-quality guidance and digital tooling. Robust policies, procedures, and best practices provide the foundation for effective risk management, ensuring consistency and compliance across the organisation. Meanwhile, advanced digital tools and platforms streamline processes, enhance visibility, and facilitate data-driven decision-making.

When implemented correctly, this integrated approach can yield significant benefits while minimizing drawbacks. Studies have shown that organizations utilizing a hybrid operating model supported by comprehensive guidance and digital tools can realize over 99% of the benefits associated with both centralized and decentralized models. Moreover, the few drawbacks encountered are far outweighed by the overall gains in risk management effectiveness and efficiency.

Implementation Approach

Start small and execute at pace, growing in line with Vendor onboarding priorities:

- By Segment x Category (Critical to less so)
- By role – TPRM Managers, Buyers, IT Risk + Compliance
- Critical processes reviewed across the Third Party Lifecycle
- From the center out to units/subsidiaries

Get in touch

The Brooklyn Platform streamlines the whole risk lifecycle, from risk assessments pre-contract to monitoring ongoing third-party risk post-contract award at the front line. Actively manage third-party risk beyond surveying and throughout the life of the contract.

To speak to someone from the Brooklyn team about the solutions that we offer,

Request a demo