Empowering Your Business

10 Steps to Effective Third Party Risk Management

WAVESTONE

Contents

Introduction

Establishing Effective TPRM Capabilities

2024, and moving into 2025, will be significant for third party risk management (TPRM).The business landscape is changing rapidly, driven by external factors including regulations and wider market movements. Organisations are now increasingly reliant on third parties and their subcontractors to deliver critical services, meaning there's more risk to consider than ever before.

Traditional TPRM methods just aren't up to the challenge anymore, and it's clear that a new approach is needed.

But in this complex new landscape, how do you begin designing and developing a robust TPRM capability for your organisation?

This whitepaper outlines 10 practical steps to establish effective TPRM capabilities.

By focusing on what matters most, setting a clear vision, and implementing a strategic approach, you can navigate the complexities of the modern business environment and mitigate the risks associated with third-party relationships.

Overcoming Barriers to Effective TPRM Implementation

While the benefits of a robust TPRM programme are clear, there are several significant hurdles that can impede successful implementation.

Here, we delve into these common barriers and explore strategies to overcome them.

Securing board support and investment

Historically, TPRM hasn't always received the necessary backing from leadership. Here's how to shift the perspective:

Highlight the value proposition:

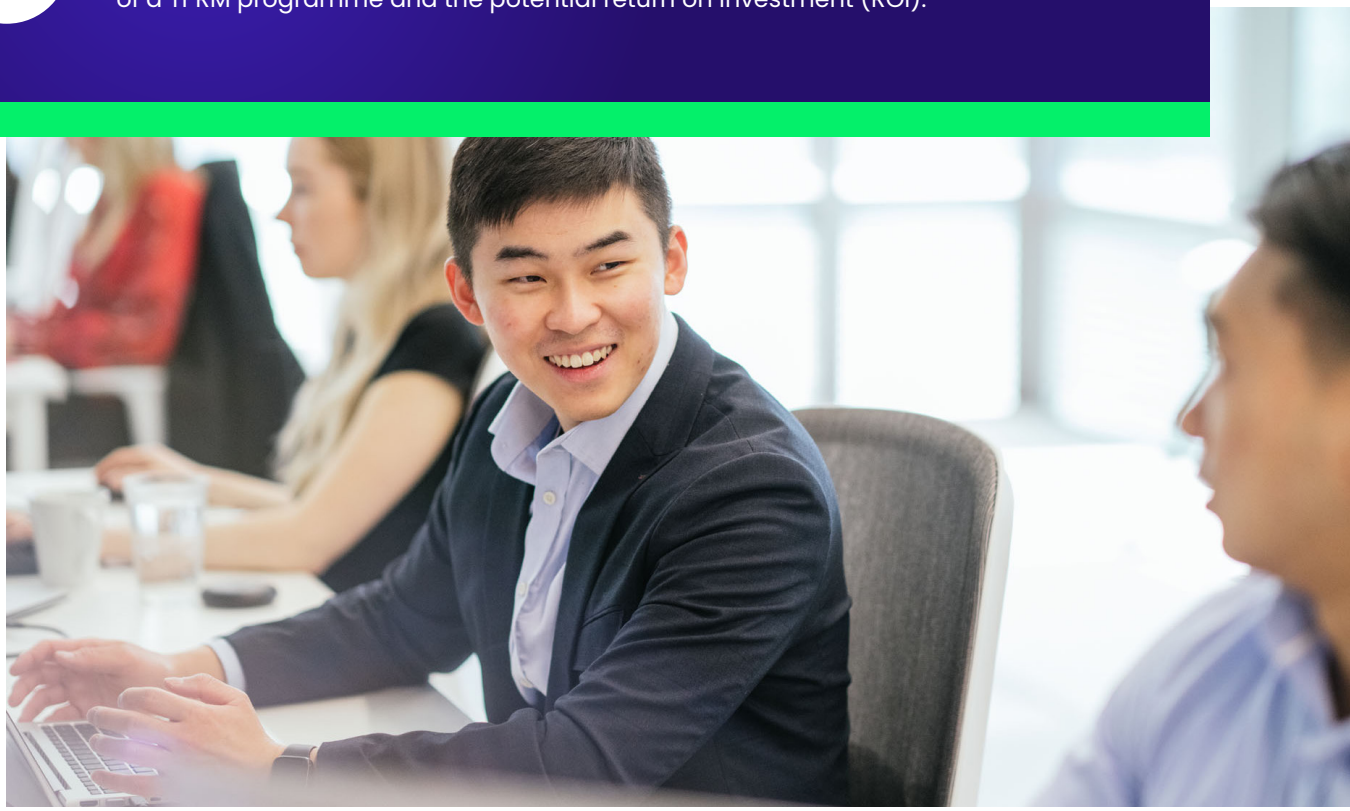
Clearly articulate the financial and reputational risks associated with inadequate TPRM. Showcase how a robust programme can prevent costly incidents and enhance brand reputation.

Demonstrate alignment with regulations:

Emphasise how effective TPRM aligns with evolving regulations that demand robust oversight and governance of third-party relationships.

Build a compelling business case:

Develop a data-driven business case outlining the cost-effectiveness of a TPRM programme and the potential return on investment (ROI).



Addressing the expanded risk frontier

The ever-expanding risk landscape necessitates a broader organisational approach to managing third-party risk. This requires:

Collaborative risk management:

Work closely with third parties to identify, understand, and control risks throughout the entire value chain. This fosters a shared responsibility for risk mitigation.

Lifecycle risk culture:

Align risk management practices across the entire third-party lifecycle, from onboarding to offboarding.

Governance maturity gaps:

Close gaps in governance frameworks and processes to ensure consistent oversight and control throughout the third-party relationship.

Overcoming institutional silos

Fragmented operations and a resistance to change can hinder TPRM implementation. Foster a collaborative environment through:

Cross-stakeholder collaboration:

Break down silos by establishing clear communication channels and collaborative working groups that involve key stakeholders from Risk, Legal, IT, Operations, Security, and other relevant departments.

Enterprise-wide risk management:

Integrate TPRM with existing enterprise risk frameworks, ensuring consistency and alignment across the organisation.

Risk-based approach:

Implement a risk-based approach to TPRM, prioritising efforts based on the potential impact of third-party relationships.

Aligning framework fragmentation

Historically, third-party management practices often relied on disparate frameworks and processes. Here's how to create a unified approach:

Gap analysis:

Conduct a comprehensive review of existing frameworks, processes, and procedures related to third-party management. Identify overlaps, redundancies, and areas where practices fall short of best practices or regulatory expectations.

Standardisation:

Develop and implement standardised TPRM frameworks, policies, and procedures that apply across the organisation.

Consolidation:

Consolidate fragmented practices into a single, unified TPRM framework that provides a holistic view of third-party risk.

Developing a sustainable operating model

Short-term solutions may seem quicker and easier, but they lack long-term sustainability. Build a future-proof model through:

Strategic focus:

Develop a long-term strategic plan for TPRM that aligns with the organisation's overall risk management objectives.

Scalability and agility:

Design a TPRM operating model that is scalable and flexible enough to adapt to evolving regulatory requirements and the ever-changing risk landscape.

Continuous improvement:

Establish a culture of continuous improvement within the TPRM programme, regularly evaluating its effectiveness and incorporating best practices.

10 Steps to TPRM Success

Drawing on our extensive experience of programme delivery and deep subject matter expertise, we have identified the 10 essential steps you need to take to establish a robust TPRM programme for your organisation.

1. Set a clear vision and strategy

TPRM is a maturing risk management principle. Establishing a vision and strategy requires a coordinated effort from senior management, including a board-level mandate, investment, and cross-departmental engagement.

Depending on your existing TPRM practices, functions such as Risk, IT, Information Security, Legal, and Procurement may already manage specific elements. A network of existing frameworks and processes likely supports TPRM activities. Due to its cross-functional nature, multiple stakeholders will contribute to the overall vision and strategy. This can be a resource-intensive exercise, especially for large firms, and may require a multi-year programme to fully define, design, and deploy a sustainable TPRM capability.

Therefore, setting a clear vision and strategy from the outset is essential to laying the right foundations.

2.

Establish and mobilise a TPRM programme

A dedicated TPRM programme team should be responsible for executing the vision and strategy, and coordinating the activities needed to define, design, and deploy the necessary TPRM capabilities.

The programme should begin by assessing how your organisation currently manages third-party risk. This initial assessment will identify and bring together key stakeholders, raise awareness of the challenge, and inform effective planning.

The programme will also play a crucial role in overcoming any barriers to change, and drive efforts in addressing organisational, cultural, technological and data issues that could impact the ability to determine, assess, manage and control third party risk.

3.

Develop an actionable roadmap

To achieve your desired outcomes, the TPRM programme needs a documented roadmap. This roadmap acts as a compass, guiding the implementation process from vision to execution and supporting the overall strategic direction.

Having a clear roadmap ensures proper programme governance, execution oversight, and accountability. It also demonstrates to the board how the TPRM investment aligns with the overall vision and strategy.

4.

Leverage existing initiatives

In recent years, attention has been focused on initiatives such as Operational Resilience and Outsourcing Compliance programmes.

As a result, most firms should have a clear idea of their most critical and dependent third-party relationships by now, as well as mapping dependencies. This is a good starting point for any TPRM Programme to understand the nature and extent of critical third parties within their wider populations.

Leveraging and collaborating with other strategic initiatives will also be mutually beneficial. Operational Resilience programmes, for example, may require a more robust TPRM focus to address key dependencies and gaps in oversight and governance.

5.

Review and harmonise existing frameworks

Many organisations may not be fully aware of their existing TPRM capabilities and resources, due to a lack of formalisation and a previously fragmented approach. A company-wide review can help identify all resources and artefacts currently deployed that touch upon TPRM.

This exercise will determine the effort needed to harmonise disparate frameworks and identify areas where skills or capabilities need strengthening.

6. Develop a sustainable enterprise-wide TPRM operating model

There are various TPRM operating models to consider, ranging from decentralised (local or entity ownership of third-party relationships) to centralised (harmonised oversight across the organisation), with hybrid models offering a balance between the two.

However, the fragmented nature of third-party risk environments necessitates a shift towards centralised control, and we have seen a progressive shift towards centralisation to manage and control TPRM capabilities across organisations, starting with the most critical services.

This allows for the development of integrated, company-wide oversight capabilities to assess, manage, and control TPRM risk posture. However, choosing the right model for you will depend on your organisational structure and legal entities.

7.

Build an effective TPRM risk and control framework

Organisational complexity, unclear roles and responsibilities, and fragmented governance structures can all hinder the effectiveness of the TPRM engagement model across the three lines of defence – preventing vertical and horizontal alignment.

Multiple business units, legal entities and control functions can often have a degree of involvement in third party risk management. By reviewing the current framework environment to address fragmentation, as well as defining the TPRM target operating model, the TPRM programme will be able to identify and implement improvements needed to establish a holistic TPRM risk and control framework.

This framework ensures clarity, consistency, and effectiveness of the TPRM model across all three lines.

An integrated framework empowers stakeholders to understand their roles and responsibilities within TPRM by establishing common risk and control standards. The specific design and implementation will vary depending on your risk management maturity, the nature of your third-party population, and internal complexities.

8. Implement risk-based principles throughout the third-party lifecycle

Risk assessments should be conducted throughout the entire third-party lifecycle, starting with a comprehensive assessment at the onboarding stage.

This assessment should utilise tiered risk factors based on the type of third party and the services they provide.

The TPRM framework should define risk segmentation, categorising relationships from low-risk to high-risk, with the latter requiring the most stringent oversight and control.

Implementing a lifecycle approach ensures a comprehensive and risk-centric framework throughout the entire third-party relationship.

> The TPRM lifecycle model should embed risk management principles through the start, middle, and end of a third-party arrangement so that the risk profile is dynamically adjusted throughout.

9. Establish framework alignment and cascade matrix

Organisations can struggle to integrate TPRM frameworks with their existing strategic frameworks. Focus on strategic alignment and a functional cascade of the Enterprise Risk Management Framework (ERM Framework) and Operational Risk Management Framework (ORM Framework) into the TPRM Framework.

Successful strategic alignment and functionality will better enable a top-down integration of risk appetite statements and metrics combined with framework standards and functional alignment. This ensures a clear demarcation between the three lines of defence, along with oversight, governance, reporting, and transparency.

A framework alignment and cascade model will enhance and drive a level of embeddedness and standardisation throughout the firm. However, organisations often struggle to align and stack the right building blocks to enable effective integration.

10. Implement a TPRM technology platform to automate risk reporting and management

There is still a heavy reliance on fragmented manual processes, with many organisations using numerous documents, spreadsheets, and duplicate reports.

This highlights a real need to address risk data, process workflows, and disparate technological solutions. Utilising TPRM technologies and reporting tools to improve and automate oversight and governance tasks will enable the aggregation of risk and provide robust intelligence. However, this will also require initiating a TPRM data strategy to ensure data quality and integrity.

The first priority on the road to a technology platform is to address the completeness of the third-party population by having a fully centralised inventory of all third-party relationships.

Secondly, the platform should be able to read across regulatory and compliance requirements to support risk identification and categorisation activities. TPRM policies, procedures, and process monitoring must be enabled through integrated risk-centric tools to improve the holistic monitoring and control of third-party risk.

Together with automated risk workflows, businesses will be in a better position to oversee and govern their third-party risk environments.

> Utilise technology to help automate and streamline processes, and establish a technology and data architecture that delivers the right level of agility. This will aid senior decision-making by integrating and connecting oversight, risk management, and governance processes, vastly improving the accuracy of risk intelligence.

In Summary

By following these 10 steps, your organisation can build a strong foundation for effective TPRM capabilities, navigate the complexities of the modern business environment, and mitigate the risks associated with third-party relationships.

To discuss any of these steps in more detail, or find out how Wavestone can support the design and implementation of your TPRM strategy, please get in touch with the team.

WAVESTONE