Third Party Risk Management: The Ultimate Guide

WAVESTONE

Authors

Mathew Wells
Senior Manager, UK Lead – Risk Advisory

Over 15-years' experience in helping firms respond to operational risk and third party risk challenges

Megan Bolland
Senior Consultant

Supporting our clients to unpick complexity and develop robust TPRM governance & oversight frameworks

Zakie Chebbo
Consultant

Supporting clients across the full end-to-end lifecycle of Third Party Management

Anna Meehan
Analyst

Recent graduate in international peace and security with a strong interest in Third Party Risk Management

Foreword

2023 is an important year for Third Party Risk Management. The landscape has changed significantly in a short period of time.

This Insight Paper covers tangible ways to tackle third party risk management. "TPRM" may be daunting and identifying where to start can be difficult. We provide context and sustainable components to help you put in place an effective operating model. We have set out **10 Practical Steps** to help you meet the challenge of TPRM head-on, navigate through complexity, as well as set a course of action to improve TPRM oversight, risk management, and governance throughout your firm.

Contents

Dealing with Complexity: Interconnected World

PARTNERSHIPS WITH THIRD PARTY PROVIDERS CONTINUE TO EXPAND WHERE OPERATIONAL EFFICIENCIES, NEW AND FASTER TECHNOLOGY DEPLOYMENT, COST REDUCTION, AND IMPROVED CLIENT AND WORKPLACE SERVICE DELIVERY ARE A FEW OF THE BENEFITS THAT FIRMS ARE REALISING.

The world has become highly connected where firms are now much more dependent on third parties to operate and deliver services than they ever used to be. This has increased exponentially firms' exposure to risks that arise from third party providers.

The COVID pandemic illustrated the rapid acceleration of digital and cloud arrangements to accommodate sudden mass remote working practices, which further stressed the risk perimeter beyond a situation that had previously been thought of as a scenario unlikely to materialise (low probability / high impact scenario). Many firms scrambled to assess the impact to risk frameworks and enhance technological solutions to combat heightened security and operational vulnerabilities.

Post-COVID pandemic, building third-party partnerships that drive innovation and customer experiences in the future have been a strategic focus. This has also led to a furtherance in digital connectedness and firms' reliance on third parties to operate has introduced new operational risks as well as compounded pre-existing ones, in particular concentration risk, data & privacy, and IT resilience risks. Functions that have oversight, management, and governance responsibility continue to struggle to keep up to date with the changes needed to risk frameworks, skills, and capabilities to deal with the accelerated pace of technological change and the interconnected web of third party arrangements, which is necessitating a need to develop integrated third party risk management (TPRM) capabilities.

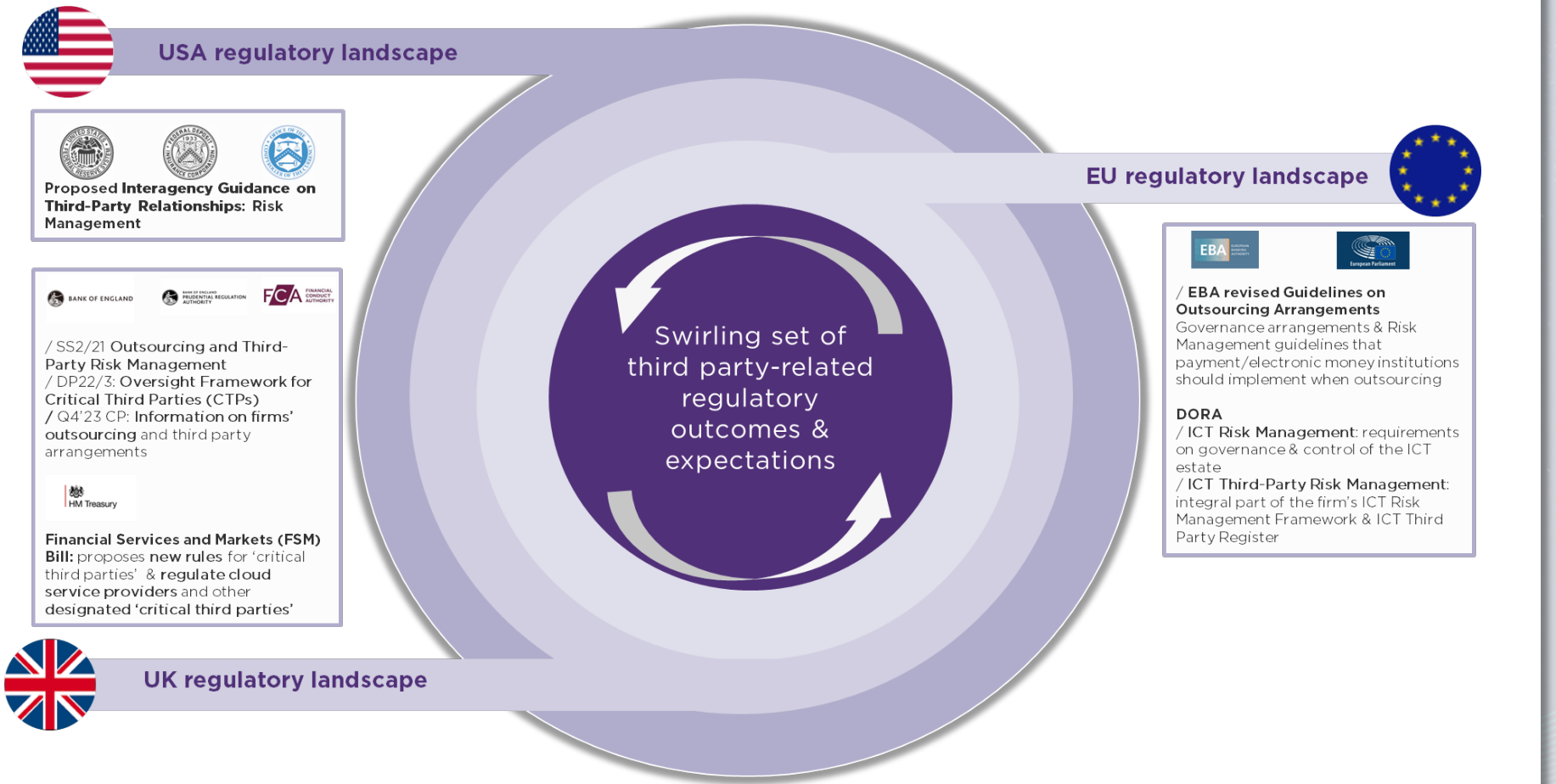
This has resulted in third party risk quickly racing up Board's "Top Risk" lists since 2020:

- ORX's '**Top Risk Review**' (December 2022) listed third party risk as the #2 top operational risk for 2023
- Risk.net's **'2023 Top-10 Operational Risks'** puts third party risk within their top 5 global operational risks – stating that firms are *"increasingly not in control of their [third party] risk perimeter"*
- **Moody's Analytics Survey** (April 2023) stated that *'69% of businesses do not have the necessary visibility over their supply chains to uncover risk'* and *'74% rated their TPRM sophistication as either poor or mediocre'*.

> **"There is now a very real dichotomy for firms in – grappling to maintain appropriate rigour in risk oversight, governance, and control of the extended enterprise that digitalisation and third parties present – whilst also adopting new technology and engaging strategic partners at a pace that maintains a competitive advantage."**

Dealing with Complexity: Regulatory Landscape

"The web of complexity also overlaps current and emerging regulatory initiatives, that has created a complex regulatory backdrop for third party oversight, governance, and compliance"



Dealing with Complexity: Enhanced Scrutiny

There is an intensification of scrutiny by the Supervisory Authorities within the UK., the EU and elsewhere on third party-related risk due to the increase in threats and the potential impact to customers and the financial sector at large. This intensification can be split into two distinct areas of scrutiny:

1. **Increasing scrutiny over how third party environments are overseen, managed, governed and controlled:**

Governance and accountability will continue to be core policy themes to drive the appropriate levels of behaviour expected within firms to address and mitigate the threats and impact third parties may present.

Current and emerging policy seeks to provide firms with the targeted focus in establishing a framework based on 'sound risk management principles' for firms to consider in developing risk management practices for all stages in the lifecycle of a third-party arrangement.

We have already seen a ramping up of requests from firms to demonstrate how they are accelerating their plans to oversee third-party risk and resilience as well as ensuring sound and effective governance arrangements are put in place.

2. Potential supervisory oversight of certain 'critical third parties' and BigTech companies:

Supervisory concerns have been mounting on material 'Cloud Service Providers' (CSP) and BigTech's involvement in financial services that present elevated levels of concentration risk, but also concerns over critical financial services provided outside of the regulatory orbit and oversight frameworks.

Therefore, we are seeing an increase in policy developments looking at addressing the '*growing dependence on a limited number of cloud service providers and other technology suppliers, including data analytics suppliers*' in order to further mitigate threats to resilience as well as market stability and integrity.

This, in turn, has meant that Supervisory Authorities within the U.K. and the EU are looking to potentially extend their reach bringing critical CSP's and BigTech firms into direct regulatory oversight. In the U.K. the Financial Services and Markets Bill currently going through Parliament will look to designate certain third parties as 'critical' and give the U.K. Supervisory Authorities the power to make rules applying to CTPs when providing services to regulated firms and FMIs and to give directions to CTPs. In addition, the Supervisory Authorities would have the power to request information directly from CTPs and third parties as well as enforcement action.

This is very much an evolving area of focus in 2023.

> **"Addressing the challenges and issues holistically will represent a significant shift in the way you manage and govern your third-party risk environments."**

Dealing with Complexity: Focus on Outcomes

In recent years there has been a shift in the way regulatory initiatives are structured by being 'outcomes based' and having cross-sector coverage. This approach allows expectations to be set for all regulated firms irrespective of sector or size with the aim for firms' being able to adapt more quickly and respond to market conditions dynamically – by using their own judgement to meet the expected outcomes rather than prescriptive rules based regulation. Aligning to an outcomes-based approach does create a number of challenges for firms, especially where expected outcomes crosscut historical organisational and functional siloes for oversight, management, and governance of third party partnerships.

Firms now need to look across their organisations more holistically and find 'unified approaches' to the way that they manage risk and governance arrangements in order to be successful and address the outcomes expected from third party risk in a streamlined and balanced way. Supervisory Authorities have been helpful in consulting with industry, and providing guidance and clarity over third-party risk-related outcomes.

- Operational Resilience of firms and FMIs engagement will continue up to 2025.
- HM Treasury proposed new statutory framework to manage systemic risk posed by CTPs, addressing market concerns on regulated activity carried out by non-regulated third parties.
- In Q4 2023, expected consultation on Incident and Outsourcing and Third-Party Reporting, which will provide clarity on the information to submit when operational events occur.

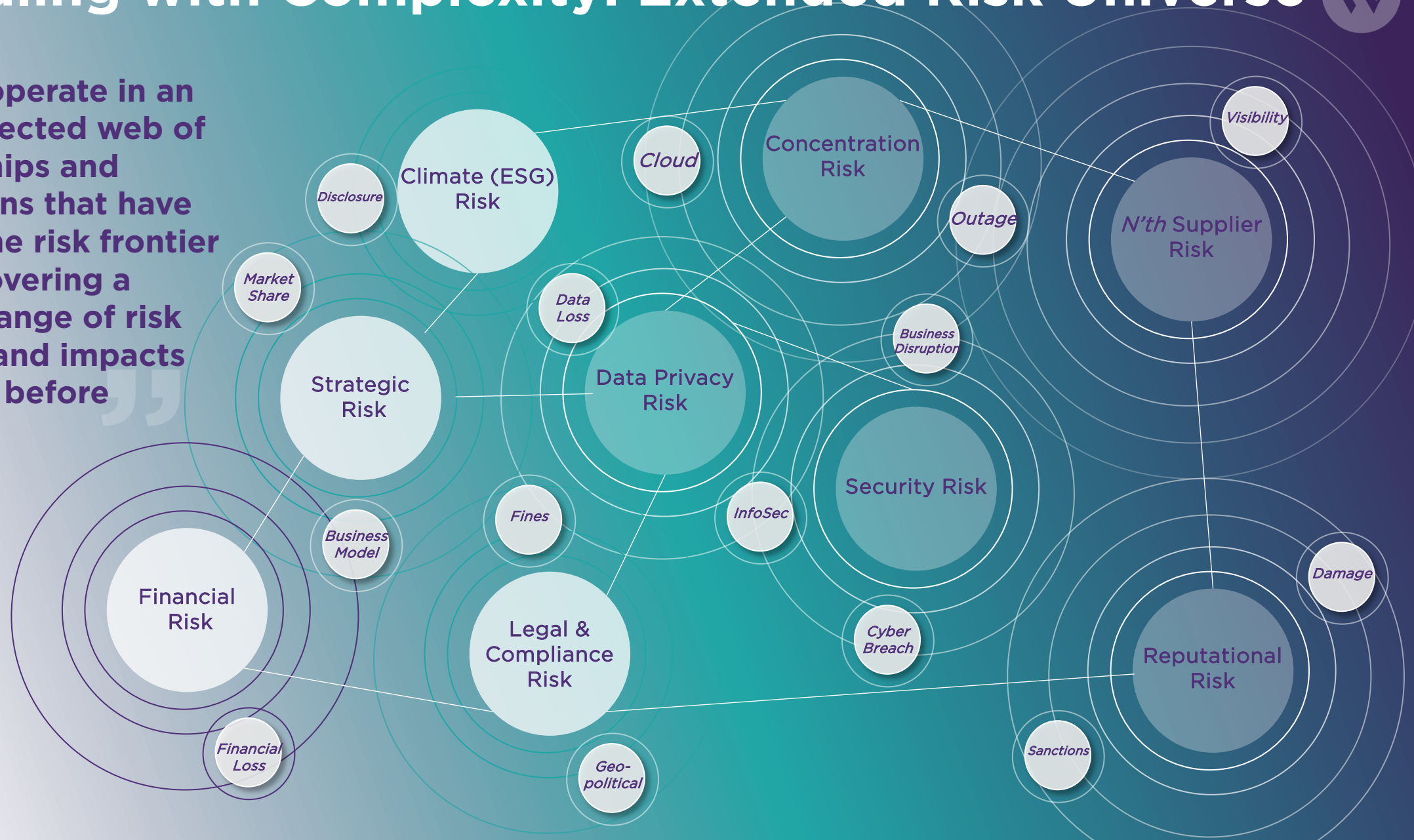
- The Digital Operational Resilience Act (DORA) sets out expectations on firms to address ICT Third Party risks as well as establishing a framework on pan-European ICT service providers (CTPPs).
- Third parties can present additional systemic risks with an expectation that further guidance could be forthcoming on the future Artificial Intelligence Act; Markets in Critical Assets Regulation (MICA); and Cybersecurity Certification Scheme for Cloud Services (Non-EU domiciled entities).

- The federal banking regulators formally recognised the reliance on third party service providers to deliver products and services stating that *'systems, policies, procedures and controls would need to ensure risks are identified, monitored and managed to the same extent as if the designated FMU were performing the service itself".*
- Interagency Guidance on Third Party Relationships expected later in 2023.
- Federal consultation on Regulation HH highlights the need for firms' effectiveness in third parties.

"Globally we are seeing a trend in increased regulator scrutiny on broader management, governance and control expectations for third party arrangements, which requires looking at the obligations holistically."

Dealing with Complexity: Extended Risk Universe

We now operate in an interconnected web of relationships and interactions that have pushed the risk frontier further covering a broader range of risk domains and impacts than ever before



Dealing with Complexity: The 'Unlucky' Bank

Scenario #1: Financial Risk + Strategic Risk + Reputational Risk

Big Bank's Board approved a new business strategy to respond to market disruption from newer challenger banks that were eroding its market share, especially among the 18-45 age category. The strategy centred on creating a new app-based banking brand relying wholly on a digital and modular architecture for its new retail banking app sharing none of the legacy infrastructure from the existing retail brand. A tech start-up provided a new revolutionary data analytics engine that would provide insight into customer's banking habits and usage to inform future marketing of retail banking services. The start-up was small but had a revolutionary product with a lot of market interest. Big Bank could see the potential possibilities. The start-up's financial health passed the due diligence processes (with management waivers) and, despite its small size and largely untested service, was green-lit. 12-months on, and unknown to Big Bank, the start-up suffered during a sudden sharp down-turn in the financial markets, which resulted in credit issues and very little operating cash. Big Bank failed to reassess the financial health following its initial due diligence. Big Bank had also spent a fortune on a slick new nation-wide marketing campaign promoting their new bank app and knowing the data analytics was dependent on the start-up, Big Bank had to resort to acquiring the start-up and its IP, incurring significant financial impact during a downturn market that was unaccounted for in order to mitigate wider strategic and reputational risks.

Scenario #2: Concentration Risk + Operational Risk + Reputational Risk + Resilience Risk

Big Bank relies on a large number of third party partners that provides IT services to its legacy retail bank and support functions. Little did the bank know that one of their partners was on an acquisition spree, acquiring other smaller suppliers within the bank's wider service ecosystem which meant that 75% of the bank's core IT infrastructure serving 8 million depositors was now from one provider. The growing partner experienced a catastrophic global IT outage due to integrating infrastructure, resulting in a complete loss of service to most of the bank's 8 million customers over a weekend.

"The scenarios that can manifest a third party-related risk can seem infinite at times. A typical third-party related risk, when realised, can expect to trigger between 3 and 4 additional risk domains from one single risk event."

Scenario#3: Information Risk + Operational Risk + Reputational Risk + Governance Risk

During the Covid Pandemic a critical third party that Big Bank relies on for the management of its IAM solution implemented a mostly remote working policy in-line with government guidelines. However, the third party failed to update its policies and processes to reflect this shift in remote working, and neither did Big Bank insist on downstream updates to align to the bank's changes in their own Information security policy. This resulted in vulnerabilities in the management of Big Bank's customer password data leading to significant breaches and theft of customer data. Big Bank suffered widespread negative press coverage as well business and systems disruption.

Scenario #4: Legal & Compliance Risk + Data & Privacy Risk + Operational Risk

Another of Big Bank's third parties recently moved a loan processing team outside of the European Union into a low cost jurisdiction with weak infrastructure and data laws. It transpired that Big Bank was not notified of the changes to the third party's internal organisation and the processing team continued to transfer and process Big Bank's customer data in breach of the GDPR leaving Big Bank open to compliance breaches. The exposure was only noticed when Big Bank opted to restructure its loan products and the matter went unnoticed for a long time.

Dealing with Complexity: 2023 Pressure Points

The need to focus on third party risk in 2023 has reached a natural market inflection point across several areas driven by the pressure on firms to:

1. Increase Board oversight of risk and compliance matters relating to third parties
2. Centralised view of all third party arrangements within a single source inventory
3. Establish a comprehensive and effective TPRM framework, appetite setting, and policy suite
4. Improve visibility and understanding of the end-to-end risk profile
5. Cascade third party risk appetite statements and aggregate risk metrics through the enterprise
6. Design and embed effective risk reporting frameworks so that the Board, risk committees, and senior management can make informed decisions
7. Improve management and control capabilities of the most critical and highly dependent third parties within a firm's third party population
8. Assess and understand the full extent of the risks associated with third parties through robust risk identification and assessment processes, as well as embedding dynamic risk adjustment activities
9. Address TPRM weaknesses in the internal risk engagement and governance model across the three lines of defence
10. Define Senior Manager accountabilities to ensure it is clear where overall accountability lies and where delegated responsibilities are needed

02

How to Establish a sustainable TPRM capability

A failure to properly identify, assess, manage, and control risk throughout the lifecycle of a relationship can expose firms to potential and significant damage covering operational, reputational, regulatory & compliance, as well as financial risks. All relationships come with inherent risk, but the increased use of third parties and the provision of increasingly reliant critical services introduces additional elements of risk that may not have been properly considered within existing risk frameworks. 2023 is the year to establish a comprehensive and effective TPRM capability.

Common Barriers to Adopting TPRM

1

Securing board support and appropriate investment:

Historically, there has been an under-appreciation of the value in establishing a holistic TPRM capability by firm's Boards – combined with the competing demands to prioritise other activities and budgets – meant that TPRM is often not considered a top priority. TPRM cannot be implemented successfully and sustainably without a Board-approved mandate and support, accountability from Senior Management, and sufficient levels of investment. However, we are seeing positive changes in re-addressing this focus, primarily due to recent high-profile third party related incidents and regulatory expectations on robust oversight and governance.

2

Addressing the expanded risk frontier:

The risks presented by third party relationships have extended significantly, so much so, that firms need to address organisationally how they oversee and manage third party risk. This involves working closely and collaboratively with third parties to identify, understand, and control risks throughout the value chain, as well as addressing the lifecycle risk culture and governance maturity gaps.

3

Overcoming institutional siloes:

Firms often struggle to implement the right TPRM capabilities where there are operational siloes and barriers to change to overcome. Embedding governance, accountability, and a risk-based lifecycle-driven approach with clear linkages to enterprise risk frameworks will drive an integrated approach to TPRM. This requires significant cross-stakeholder collaboration and looking at third party risk across many different prisms spanning Risk, Legal & Compliance, ICT/ Technology, Operations, Information Security and Cyber Security, Disaster Recovery & Business Continuity, and Operational Resilience.

4

Aligning framework fragmentation:

The typical approach to third party-related management capabilities are historically fragmented across differing frameworks, processes and procedures, and managed primarily under arrangements that predate TPRM principles. To build a holistic TPRM capability firms will need to determine the current coverage of third-party risk related activities across all pre-existing frameworks and internal practices to identify gaps and weaknesses.

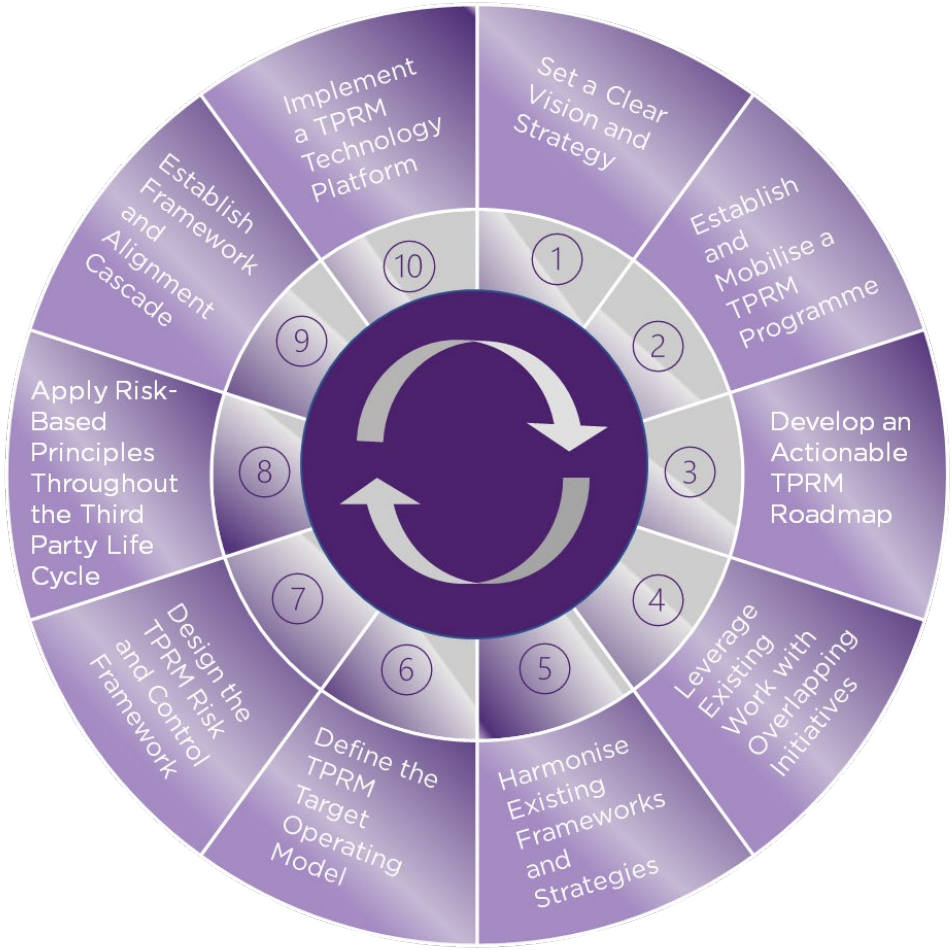
5

Developing a sustainable operating model:

The above challenges can compound issues, preventing a focussed and strategic approach to the target operating model design for TPRM. Firms' have tended to focus more on tactical 'quick-wins' that present the least amount of friction. Long-term it is unlikely to be sustainable given the level of focus on sound and robust risk management and governance expected by Supervisory Authorities.

10 Practical Steps to Establishing TPRM Capabilities

"Based on our learnings and perspectives gained during 2022, we have identified the following **10 Practical Steps** to take in 2023 to guarantee successful outcomes."



It is time for firms to move away from legacy practices and depending on the level of risk maturity, these practical steps can prioritise focus for 2023. It is essential to tackle the issue strategically, yet proportionally and sustainably for your firm.

10 Practical Steps to Establishing TPRM Capabilities

A TPRM Programme cannot succeed without a clear vision and strategy that sets the overall direction – a 'north-star'

1 SET A CLEAR VISION & STRATEGY

Developing a clear Vision & Strategy will be a firm's guiding north-star. TPRM is a relatively new risk principle, but one that is evolving and maturing rapidly. Establishing the Vision & Strategy requires a coordinated set of top-down efforts and actions including, a Board-established mandate, senior management support, appropriate investment, and cross-stakeholder engagement.

Depending on how third-party management activities have evolved in your firm, functions such as: Risk, Operational Resilience, IT/ Technology, Information Security, Legal & Compliance, and Sourcing & Procurement may be responsible for specific elements of the design and organisational alignment of TPRM supported by a network of incumbent frameworks and processes.

Therefore, due to the transversal coverage of TPRM there will likely be several key stakeholder groups involved in contributing to and setting the overall Vision and Strategy. Implementing TPRM can be a time and resource intensive exercise and for complex and large firms can often span a multi-year effort to define, design, and deploy the TPRM capability to a sustainable state. Therefore, setting a clear Vision and Strategy will be essential to laying the right foundations.

2 ESTABLISH & MOBILISE A TPRM PROGRAMME

A TPRM programme will need to be established to *effect* the Vision and Strategy as well as coordinate the activities to define, design, and deploy the necessary TPRM capabilities.

The programme will be better placed to support overcoming any barriers to change and drive efforts in addressing organisational, cultural, technological and data barriers that could impact the ability to determine, assess, manage and control third party risk.

The primary focus at the beginning must be to review and assess how third party-related risks are managed today before defining, designing, and implementing the target state capability. This early approach will identify and bring together the various stakeholder groups, focus minds, and also ascertain the extent of the challenge in order to plan effectively.

10 Practical Steps to Establishing TPRM Capabilities

3 DEVELOP AN ACTIONABLE ROADMAP ALIGNED TO THE VISION & STRATEGY

To arrive at the target end point, the TPRM programme must establish and document an actionable roadmap to act as a 'compass' and provide directional pull to the implementation process from aspiration to delivery mode – supporting the 'north star' approach set by the Vision and Strategy.

Having in a place a clear roadmap will ensure that programme governance, execution oversight, and the right programme accountabilities are in place, as well as demonstrating to the Board how the investment in TPRM will be delivered against the Vision and Strategy.

4 LEVERAGE WORK ALREADY COMPLETED WITHIN OVERLAPPING STRATEGIC INITIATIVES

In recent years, attention has been focussed on initiatives such as Operational Resilience and Outsourcing Compliance programmes. As a result, most firms by now should have a clear idea of their most critical and dependent third-party relationships, 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. We have observed Operational Resilience programmes calling for more TPRM focus and capabilities to be deployed, as key dependencies and gaps are highlighted on the transversal oversight and governance required to manage end-to-end services.

Therefore, it's important to utilise and work closely with Operational Resilience and Outsourcing Compliance programmes to understand how to fast-track, accelerate and co-ordinate activities when defining their TPRM capabilities.

Once a clear vision and TPRM Programme has been established, a target operating model should be developed. The transversal and pervasive nature of third-party risk can lead to functional change, in order to address and manage third party risk holistically.

10 Practical Steps to Establishing TPRM Capabilities

5 REVIEW AND HARMONISE EXISTING FRAMEWORKS, POLICIES AND PROCEDURES

Many firms are not always fully aware of the capabilities and resources that might already be in place that – either focusses or have touchpoints to specific elements of TPRM – because TPRM is not formalised or harmonised in a holistic manner today. It is simply that current internal capabilities and resources are fragmented.

As a result, firms should undertake a company-wide review to build a full picture of all resources and artefacts currently deployed.

determine the right level of effort needed to harmonise disparate or fragmented frameworks under a consolidated TPRM framework, as well as identify areas of weakness or gaps to be addressed within the existing skills and capabilities.

6 DEVELOP A SUSTAINABLE ENTERPRISE-WIDE TPRM OPERATING MODEL

The shift towards centralisation is driven by the fragmented and pervasive nature of third-party risk environments today – together with pressures (internal and external) of developing integrated company-wide oversight capabilities to assess, manage, and control a TPRM risk posture.

Various models and structures can be deployed depending on the organisational and legal entity set up. These range from *decentralised* – with an emphasis on local or entity ownership for managing third party relationships and their risk – to *centralised* where the responsibility and management of third party risk oversight is harmonised across the organisation – to a *hybrid* model taking the best of both worlds of maintaining a decentralised organisational ownership of the relationship complimented by centralised oversight, reporting and governance requirements.

> During the last 12-months we have seen our clients progressively shifting towards centralisation to manage and control TPRM capabilities across the enterprise, starting with the most critical and important arrangements.

10 Practical Steps to establishing TPRM capabilities

The number of third-party risks that firms face is ever growing and pervasive, covering: strategic, reputational, operational & resilience, legal & compliance and security risks.

These risk domains are becoming much more interconnected through third party risk events, often in subtle nuanced ways, which requires a structured and careful set of framework-driven processes to understand the causes and impacts of the risks emanating from your third party population.

All too often we see best efforts towards TPRM stifled and stymied by incumbent organisational siloes and stakeholder 'turf-warfare' over ownership and accountabilities which can prevent a TPRM programme from really succeeding and achieving the outcomes established early on.

The TPRM framework must be underpinned by the risk management processes of identification, assessment, monitoring and control, along with a number of enablers including documented TPRM policy suite, technology and tooling, and the capacity and capability of resources.

> **The overall effectiveness of a TPRM capability will require a great deal of coordination and collaboration horizontally – among departments and support functions – and vertically within organisational and governance structures.**

10 Practical Steps to Establishing TPRM Capabilities

7 DEVELOP AN EFFECTIVE TPRM RISK & CONTROL FRAMEWORK ACROSS THE 3 LINES OF DEFENCE

Organisational complexity, unclear roles and responsibilities, and fragmented governance structures are clear obstacles that can negatively impact the effectiveness of the TPRM engagement model across the three-lines of defence – preventing vertical and horizontal alignment.

We often observe multiple business units, legal entities and control functions have a degree of involvement in third party management. In going through the exercises in 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 & Control Framework.

This will ensure clarity, consistency, and, above all, effectiveness of the target state TPRM engagement model across the three lines.

- An integrated TPRM Risk & Control Framework will help support horizontal and vertical stakeholder groups to understand their involvement and role within TPRM by establishing a common set of risk and control standards for evaluating and managing the firm's third-party risk and control expectations across the three-lines.
- The specific design and implementation of a TPRM Risk & Control Framework will vary according to your risk management and control maturity and culture, together with the nature, scale and complexity of the third-party population and the services they provide as well as internal intricacies.

"The TPRM Framework must be underpinned by a robust third party lifecycle model which will help establish and enforce a risk-based approach to each relationship with the simple premise, as in life, that there is a start, middle, and end to any relationship and the level of risk needs to be fully understood and managed throughout the relationship lifecycle."

10 Practical Steps to Establishing TPRM Capabilities

8 IMPLEMENT RISK-BASED PRINCIPLES THROUGHOUT THE THIRD-PARTY LIFECYCLE

Risk assessments should be an ongoing activity throughout the lifecycle model starting with a full assessment from the outset of the relationship – by applying a set of tiered risk factors depending on the type of third party and nature of the services or products provided.

It will be important to apply the appropriate risk segmentation set out in the TPRM Framework according to the tiered levels of inherent risk from low-risk relationships to moderate risk that should be monitored, to the most critical and complex relationships that represent higher levels of risk to the firm that require the strongest levels of management, oversight, and control.

Implementing a lifecycle approach within the TPRM framework will support firms to take a workflow approach to TPRM as well as implement a comprehensive and effective framework that is risk-centric and risk-adjusted throughout. Therefore, risk management principles should be embedded within each component of the third-party lifecycle covering risk-based processes to identify, assess, and rate risk.

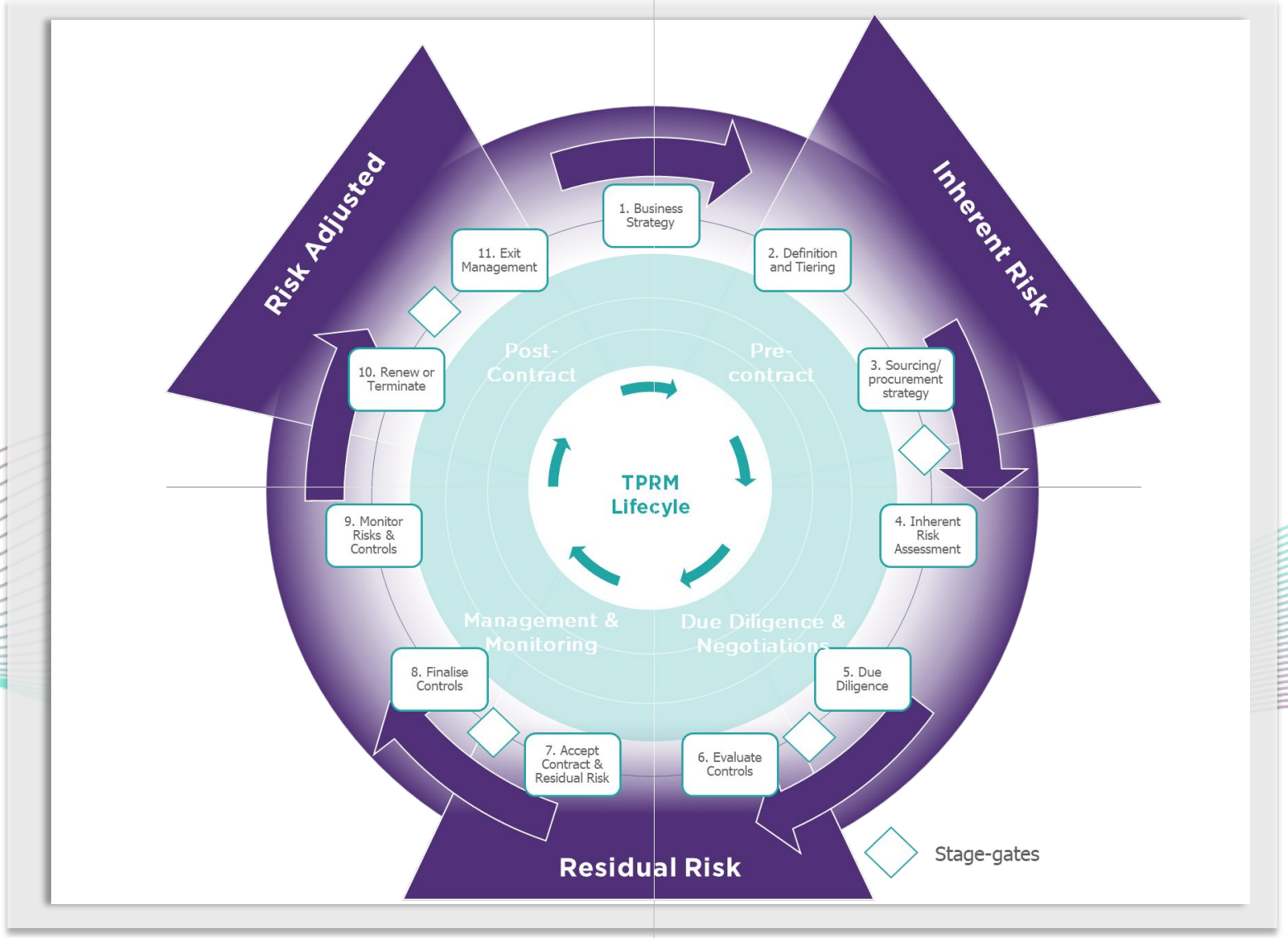
Implementing a transversal risk-based lifecycle does come with a number of barriers and challenges. The most common challenge we see relates to risk fragmentation and inconsistent risk taxonomies across the TPRM stakeholder groups, especially with risk ratings and criticality assessments which makes it difficult (in the absence of a centralised TPRM capability) to aggregate the risk to create, manage, monitor, and control a third-party risk profile for senior decision making.

“Having visibility into your third parties’ risk is fundamental but this should not be a ‘one time’ exercise, there needs to be dynamic ‘risk adjustment’ throughout the lifecycle”

10

Practical Steps to Establishing TPRM Capabilities

"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."

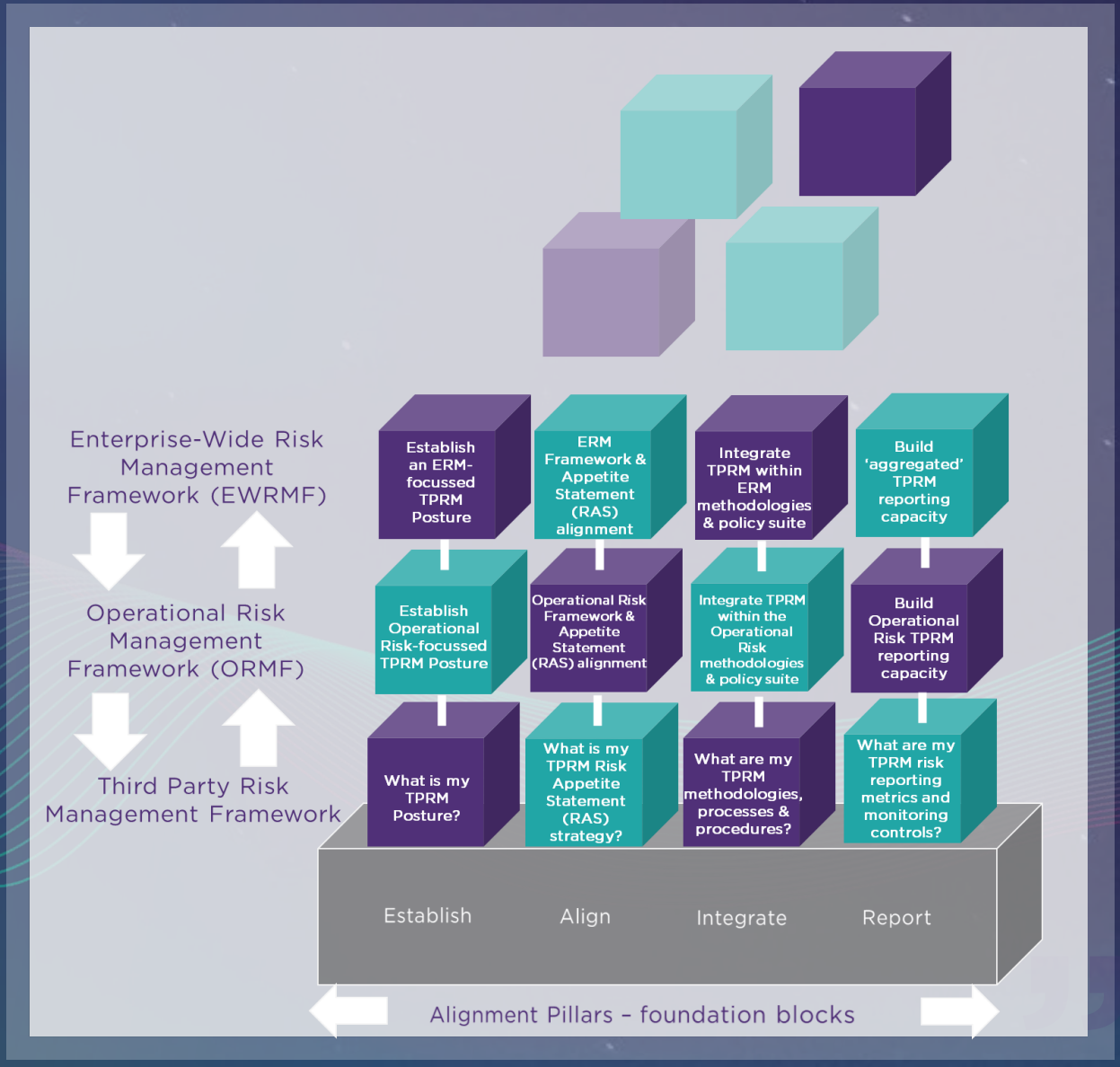


10 Practical Steps to Establishing TPRM Capabilities

9 ESTABLISH FRAMEWORK ALIGNMENT AND CASCADE MATRIX TO FULLY EMBED THE TPRM FRAMEWORK

Firms can often struggle to integrate the right foundation blocks into their strategic frameworks. Focus should be on strategic alignment and a functional cascade of the Enterprise-wide Risk Management Framework and Operational Risk Management Framework to 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. In doing so, this will ensure a clear demarcation between the three lines of defence as well as oversight, governance, reporting, and transparency.

"A framework alignment and cascade model will enhance and drive a level of embeddedness and standardisation throughout the firm. But firms' often struggle to align and stack the right foundation blocks to enable effective alignment."



10 Practical Steps to Establishing TPRM Capabilities

10 IMPLEMENT A TPRM TECHNOLOGY PLATFORM TO AUTOMATE RISK REPORTING AND MANAGEMENT INFORMATION

There is still heavy reliance on fragmented manual processes with a myriad of documents, spreadsheets, and duplicative reporting information leading to a genuine 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 aggregation of risk and provide robust intelligence. But 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; and secondly reading across the 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, firms' will be in a better place to oversee and govern their third party risk environments.

Look to utilise technology to help automate and streamline processes and establish a technology and data architecture that delivers the right level of agility, which will aid senior decision making by integrating and connecting oversight, risk management, and governance processes that will vastly improve the accuracy of risk intelligence.

8 Core TPRM Operating Model Design Components

At Wavestone, we recognise that not all firms are at the same level of TPRM maturity, our operating model framework takes a modular approach to be adapted to your environment to tailor your outcomes.

	Phase #1 DEFINE	Phase #2 DESIGN	Phase #3 DEPLOY	Outcome
1. Vision, Strategy & Design Principles	• Establish TPRM Working Group & facilitate workshops • Finalise TPRM operating model Vision, Scope & strategic inputs and design Principles. • Socialise the Vision & Scope to the function and business stakeholders.	• Incorporate strategic principles into all component 'design' stages. • Alignment to strategic vision • Collate risks and issues, assign owners and manage escalations	• Confirm & sign-off on detailed TPRM TOM designs & deployment model • Begin the deploy phase of the under-pinning TPRM organisation structure	✓ Holistic Vision & Strategy document and roadmap ✓ Full strategic alignment to Group strategy and the function's business strategy
2. TPRM Team Model	• Define target TPRM team requirements, accountability, and responsibility matrix. • Assess the level of integration with other functional risk teams & business lines.	• Design of TPRM team structure • Define consistent, effective interfaces with lines of business and any external parties • FTE gaps and design recruitment strategy	• Deploy and establish an optimum TPRM team to reduce duplication and complexity • Assign FTEs / resources / accountability / reporting lines to target structure • Advertise new roles and deal with displacement	✓ Integrated TPRM team structure within each functional area to support efficient and effective delivery of TPRM services and activities.
3. Capabilities Map	• Initial capability assessment of current skills and an analysis of the TPRM Framework matrix across your firm. • Define the broad capabilities required for each TPRM technology risk & controls roles.	• Undertake RACI exercise • Collate skills and capabilities required by functional area • Assess the gap and build a plan to remove the gaps • Understand where a skills uplift/ resourcing is required	• Build and deliver the capabilities training and development programme • Cross-functional capability requirements are deployed and delivered within each TOM component.	✓ Holistic capabilities mapped to functional TPRM teams and role requirements to ensure integrated management of all relevant risk management & control processes.
4. TPRM Risk Management Framework	• Document the as-is e2e TPRM risk management processes against the target and your firm's Operational Risk Management Framework. • Define function's strategic requirements & ownership against each of the framework pillars 1, 2 & 3.	• Design the underlying risk management process capabilities (covering: risk identification, assessment, evaluation, treatment and response). • Alignment to ERM & OpsRisk Framework & Taxonomy	• Deploy risk and control assessment & align to the TPRM risk register • Embed risk management processes (risk identification, assessment, evaluation, treatment and response).	✓ A fully integrated risk management framework for TPRM. Fully aligned to your firm's requirements and aligned to the ERM & Operational Risk Management Frameworks & metric based reporting. Managing risk within a sound and robust manner.

8 Core TPRM Operating Model Design Components

	Phase #1 DEFINE	Phase #2 DESIGN	Phase #3 DEPLOY	Outcome
5. TPRM Controls Framework	• Facilitate planning workshops to define the target controls framework for the function. • Define the target internal process requirements for the different control processes (identification, assessment, testing)	• Design the target controls framework for the function • Validate control framework RACI. • Design controls processes (identification, assessment, testing) / linkage to control owners / control reporting design	• Deploy and embed target control environment processes / ownership / reporting lines • Embed integrated control catalogue • Deploy control testing regime / consolidation reporting.	✓ Holistic and consolidated TPRM Controls environment, removing duplication and gaps to ensure that the function is controlling the risk profile in a supporting and effective manner.
6. Tooling, Systems, and Data	• Review current technology risk & controls related tooling, systems and data resources. • Document our findings to establish a full baseline of the current technology risk platform(s). • Document agreed improvements for Phase 2 and 3.	• Undertake technology/ systems strategy development (aligned to target end state operating model) • Facilitate workshops & agreements for Technology Platform / tooling utilisation approach (internal v's external)	• Deploy target technology platform / strategic improvements. • GRC integrated capabilities underpinned by advanced data analytics	✓ A holistic TPRM Risk and data architecture underpinned by automation and real -time data insight. A strategic TPRM risk/ GRC platform to support TPRM processes.
7. Governance & Reporting	• Review the current TPRM governance processes. • Identify current governance forums and structure • Set out opportunities for incorporating policy requirements and standards. • Define the requirements for target governance.	• Assess the suitability and decision making control for existing governance forums • Develop new governance framework and layers of control	• Establish integrated governance / forums / test for potential layer risks and issues • Establish 'one -way' governance and reduce duplication and complexity.	✓ Governance framework mapped out to support all levels of an integrated TPRM operating model. ✓ Integrated policy suite management and governance reporting across the TPRM .
8. Culture & Awareness	• Define a risk culture framework & continuous improvement process. • Identify role -based training requirements .	• Design and build risk culture platform including technical risk training artefacts, SharePoint portal materials, and guided video instructions • Build mandatory training requirements for role based training	• Deploy technical training plans • Role based awareness / Risk Champion structure • Deploy TPRM Risk awareness landing Portal site	✓ An holistic risk culture and awareness platform to enable risk to be embedded into the way of working for the function. ✓ A mature and evolving platform for ensuring consistent and effective risk empowerment.

The TPRM operating model should act as a blueprint for your firm to increase the maturity and establish a sustainable approach to managing third parties and risk holistically.

03

Joining the Dots to Effective Governance

There are a number of regulatory requirements that have a bearing on how firms' manage their third-party environments ranging from Outsourcing Arrangements to Critical Third Parties to Important Business Services to Critically Important Functions and so on. A coordinated approach to regulatory & compliance issues is needed when addressing third party risk

Joining the Dots

Firms that establish an ‘enterprise governance framework’ will be better placed to oversee their dynamic risk profile and ensuring regulatory & compliance developments are dealt with holistically across all types of arrangements.

Effective governance means being proactive and adapting to fast-changing environments. Third party dependencies represent a significant threat to a firm’s risk profile and resilience capabilities. Establishing the right holistic approach to the risk governance of third parties, in particular Critical Third Parties, will improve the level of visibility, oversight and management information to sufficiently govern and assure the risks presented by third-party relationships are controlled effectively.

Organisations must invest in greater alignment and scale their enterprise risk management and governance models to ‘join the dots’ of regulatory expectations and compliance issues, as well as streamlining approaches to governance across the organisation.

Firms’ can often struggle to demonstrate and provide evidence of the true visibility of their risk profile arising from their third-party relationships at a sufficient level of detail to satisfy differing governance expectations. Typical issues relate to historical organisational and operational siloes, decentralised inventories, databases and data integrity issues and systems, make it extremely difficult to provide an enterprise-wide view of Third-Party Risk and manage it effectively. On occasion, confirming or locating a copy of a signed contract can still prove difficult for many especially where the relationship has lasted for a long time.

It is important to address the regulatory requirements through a unified strategy that illustrates the core elements of Outsourcing & Third Party Risk, Operational Resilience and DORA requirements when planning your TPRM Programme, as well as other established rules and requirements relating to different regulated activity.

In the long run, it will be inefficient and overly burdensome to establish different risk management and governance models for each regulatory-driven initiative separately (with no linkage or organisational alignment) especially where they overlap on achieving the same principles and outcomes that the corresponding regulators are seeking. This is certainly not the expectation that Supervisory Authorities want either, as this will create unnecessary governance risk by having to manage internal oversight complexity.

In the complex and fast-changing world of third party risk where new types of risks are emerging frequently, being able to quickly obtain accurate management information throughout the organisation will be critical as well as addressing underlying third party data quality and integrity issues which may impact regulatory compliance reporting.

Joining the Dots: Senior Managers' Beware

The recent TSB incident highlighted the need to understand the full extent of governance risks. The IT migration involved 85 sub-contractors and 11 'critical' subcontractors of critical services & functions (*as per PRA Outsourcing Rules*)

The Prudential Regulatory Authority (PRA) in its Final Notice issued on 14 April 2023 and the Financial Conduct Authority's (FCA) fine of £27.6 million on 22 December 2022 relating to the highly public failed IT migration emphasised that senior manager decisions relating to outsourcings and sub-contractor arrangements should be considered careful and making ill-informed judgements on the level of attention firm's management should take on arrangements are critical. It is not enough to assume that a contract is all that is needed to conform with and satisfy rules on Outsourcing arrangements. The Final Notice went further by reiterating that Senior Managers must be fully informed of relevant governance risks depending on the magnitude of the risk.

The TSB incident relates to a failed intra-group migration. The PRA's Final Notice states that firm's should apply the rules on Outsourcings in a proportionate manner to intra-group arrangements. There must be "*careful assessment of whether the service provider has the ability, capacity, resources and appropriate organisational structure to support the performance of the outsourced functions, and for this assessment to be revisited*".

The PRA Final Notice states that the TSB CIO did not take reasonable steps in relation to the readiness of the intra-group provider to operate the IT platform. Instead reliance on the premise that there was an intra-group agreement entered into and the service provider was part of the wider Group structure did not satisfy the level of reasonableness.

It is clear given the interconnectedness of third parties and their services now that the Supervisory Authorities expect Senior Manager's to apply robust assessment, oversight, and governance of intra-group arrangements where the level of risk requires. By holding to account and fining the ex-CIO sends a clear message that simply relying on having an intra-group contract in place but not testing the capabilities or challenging intra-group assurances will not be enough.

> **The events in the TSB IT migration and the decision to fine the ex-CIO sends a clear message that senior managers need to fully understand, evaluate, and challenge the inherent risk in their third party partners irrespective of whether they are external or internal service providers.**


04
How to Adapt to an Ever-expanding Technological Environment and Risk Landscape

Technology is constantly evolving and changing at such a rate that it is not always easy for risk and governance teams to keep pace. Andrew Marvell famously immortalised the phrase, "*Time's wingèd chariot hurrying near*", which provides an appropriate metaphor for where we are today with TPRM. But much can be done to ensure a more proactive stance.

> To establish a forward-looking approach to third party risk management, understanding what is on the horizon is essential, as it informs strategic and operational decisions.

3 Tips to Adapt to Technological Environment and Risk Landscape

1 CONTINUOUS SCANNING AND MONITORING

External factors that impact firms are constantly changing and evolving, whether it is changes in regulatory obligations, subtleties in approaches, changes in underlying customer base and products and market conditions, to innovative and untested technologies (e.g. ChatGPT and generative AI capabilities). These wide-ranging external factors can carry an equally wide array of risks that have the potential to cause significant impact if they materialise or are not managed or controlled effectively in a risk-based way. However, no one firm can manage and control everything (the Covid Pandemic is a prime example) therefore, it is vital to have oversight of potential risks that could arise via these changes and be agile to adapt your strategy and operations accordingly – in order to become truly 'risk-adjusted'.

Implement mechanisms to continuously scan for changes in external factors that could impact your business and monitor their evolution over time. Timing is key - identifying a change in its early stages, or better yet, before it occurs can buy you time to understand the associated risks and impacts to plan, adapt and respond accordingly.

In establishing a TPRM Technology Platform you can also embed horizon scanning mechanisms and tactics to draw out horizon risks or trending indicators for risk. With many advancements in the tooling space, there are a variety of tools that can scan your risk landscape. Close collaboration with technology teams is essential to ensure alignment of requirements and that the chosen solution continues to deliver what is needed.

3 Tips to Adapt to Technological Environment and Risk Landscape

2 UNDERSTANDING AND INTERPRETING THE ASSOCIATED RISKS AND IMPACT

Once a change in an external factor has been identified that could impact your firm, the next stage is to understand what the associated emerging risks are. For each associated risk, you need to understand what the impact is, should it materialise, how and where would it materialise, and who needs to be informed. It will be important to deploy a data-driven approach using the risk indicators under the TPRM Risk & Controls Framework to communicate to senior stakeholders the level of trending cadence, as well as potential impact.

With the risk landscape constantly evolving, the skills needed to understand and manage these risks also needs to evolve. Carry out regular capability assessments to ensure the right skills within your firm exist and are suitable for the future. We know that digitalisation will continue to transform and change business models, driving newer ways to govern and manage risk where certain SME knowledge and capabilities will be needed. Capabilities such as the ability to interact with Artificial Intelligence teams, cloud SMEs, and machine learning, to name a few, will be critical to be able to advise business functions to incorporate a risk-based approach to strategic planning and technology roll-out.

> **The skills and capabilities in the future will be very different to the skills and capabilities today . You will need to adapt and supplement teams with the skills and capabilities necessary to understand and manage risks from new, evolving and emerging technologies as we become more digitally-reliant.**

3 Tips to adapt to technological environment and risk landscape

3 ADAPT AND RESPOND

Once you have a clear understanding of the impact associated with the change, what is left is to adapt your strategy or operations accordingly. This is not a "one off" response, but a continuous cycle of adapting and responding to new information and insight.

Instilling a 'risk-adjustment' methodology will ensure that there is continual improvement and that risk considerations are fully understood and capable of being incorporated into the way of working for teams as well as within your third party partners. Examples include:

- In undertaking a continuous scan of the critical third-party population, you can identify whether a critical third party is in the middle of court proceedings that may introduce reputational risk.
- In undertaking continuous monitoring of a Third Party, you learn that they have now decided to slash their dividends. As a result, you begin to assess the associated risks and the impact that this might bring. For instance, the risk that a Third Party goes bankrupt has increased (even if it is still overall low), which if materialised means that they cannot continue to deliver the service that you rely on. As a response, you take the action of to review and update your contingency plans for that critical third party to be prepared should the risks and corresponding impact materialise.

Final Thoughts

HOW CAN WAVESTONE SUPPORT?

The reality of business has changed. The interconnectedness of internal and external interactions as well as the transversal nature of third-party risk represents a distinct need for firm-wide collaboration and coordination to identify and mitigate existing and future risks, underpinned by a holistic TPRM oversight, governance, risk management, and compliance capability.

To adopt and embed a holistic TPRM capability and be fully equipped to address third party risk, firms can follow the 10 Practical Steps detailed in this Insight Paper.

Your current maturity level will determine what your first step looks like, however, in beginning to take these steps, the journey towards an embedded holistic TPRM model is in sight.

Third Party Risk Management: The Ultimate Guide

WAVESTONE

Business , Technology and Sustainability

15 offices
9 countries

4,000+
Employees

Contact our experts

Mathew Wells
Senior Manager
Mathew.Wells@wavestone.com

Megan Bolland
Senior Consultant
Megan.Bolland@wavestone.com

Zakie Chebbo
Consultant
Zakie.Chebbo@wavestone.com

Anna Meehan
Analyst
Anna.Meehan@wavestone.com