Outsourcing and third party risk management -

Building resilience in supply chains and meeting regulatory expectations

April 2021

kpmg.com/uk

contents

01 Introduction

Outsourcing and Third Party Risk Management ('TPRM') has become one of the key areas of focus for financial services organisations. In the latest global KPMG Third Party Risk Management Outlook survey, over 75% of respondents stated that TPRM was a strategic priority for their business.

This is reflective of the rapidly changing landscape the industry finds itself in; more than ever before companies are using third parties to deliver technology-driven services to customers, migrating to cloud-based solutions and transform their business.

Businesses are encountering challenges in the effective management of third party risks

— Insufficient resources and capabilities to manage all the third-party risks they face, against a backdrop of evolving risks and threats

— Inconsistent and ineffective approaches to identifying and managing risks across the lifecycle of a relationship or service

— Failure to harness the automation benefits from using technology and data for decisioning, monitoring and workflow

— Sustaining a complex operating model that spans multiple parts of the business

High up on the risk agenda for Executives and Board members, regulators across the globe have started to issue new guidance and raise the bar in terms of on how financial services institutions should manage third party risks.

In the UK, the Prudential Regulation Authority ('PRA') published its Policy and Supervisory Statements on Outsourcing and Third Party Risk Management on 29th March 2021.

The PRA is modernising its expectations on how firms should manage outsourcing and third party risks.

Specifically, the PRA is seeking to:

— Align this topic with the implementation of Operational Resilience and complement the stated regulatory requirements

— Facilitate the adoption of Cloud and other new technologies in a consistent way across the industry

— Implement the EBA's "Guidelines on outsourcing arrangements" and "ICT and security risk management"

— Ultimately, drive greater resilience in the financial services supply chain

Timelines:

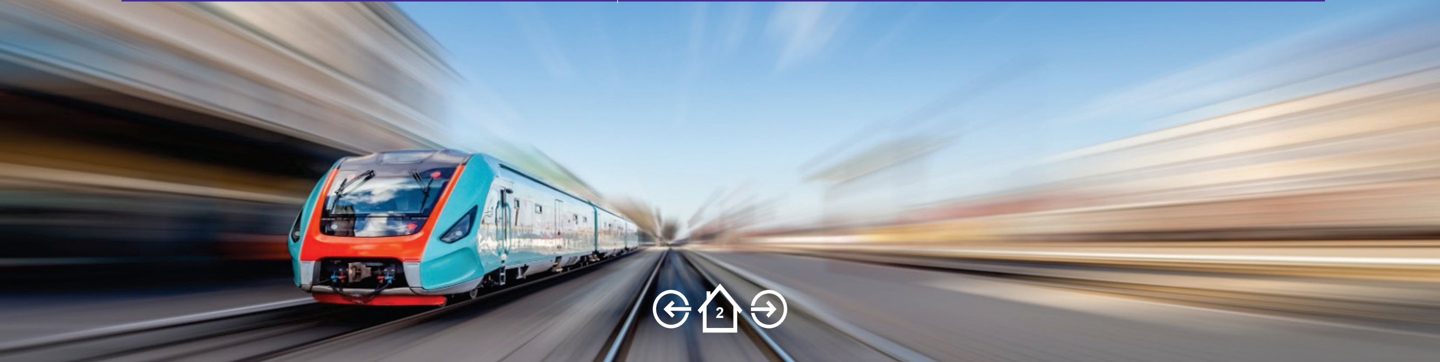
The PRA has set the following timelines for implementation:

31 March 2022

Firms have less than a year to comply with the expectations set out in the Supervisory Statement.

As soon as possible

Firms should review and update legacy outsourcing agreements entered into before 31 March 2021 at the first appropriate contractual renewal or as soon as possible on or after 31 March 2022.



02 Summary of new regulatory requirements

Board engagement and involvement	Board is to 'set the control environment' and specifically approve, review and implement a written outsourcing policy. The Board is to be furnished with the right level of MI to be able discharge its oversight responsibilities.
Senior Management accountability	Expectation that responsibility to be allocated to the SMF24. SMF24 is accountable for overall framework, policy, and systems and controls. Includes defining the outsourcing policy in line with expectations stated by the regulators.
Materiality and risk	Develop processes for assessing materiality and risk on an ongoing basis. Firms are expected to assess *all third party arrangements*, irrespective of whether they fall within the definition of outsourcing.
Due diligence	'Appropriate and proportionate' due diligence to be conducted on all potential service providers. For material outsourcing, wide array of areas to be covered including business model, financial situation, ownership structure, and scale; capability, expertise, and reputation; financial, human, and technology resources; IT controls and security.
Contracts	Expected minimum contract requirements included with firms also expected to consider various additional contract requirements - some new requirements on exit plans included which could be challenging.
Risk assessment and monitoring	Risk assessment and monitoring to cover financial risks and operational risks based on severe but plausible scenarios. Risk mitigations / controls to be assessed.
Data security controls	Requirement to define, document, and understand own and service provider's respective responsibilities in respect of data and take appropriate measures to protect them. Robust controls to be implemented across 13 data security control areas. Expectation that the service provider's security controls are, at least, as effective as the in-house security environment.
Continuity and exit plans	For each material outsourcing arrangement, should develop, maintain, and test a business continuity plan and exit strategy. Latter to cover stressed and managed exits. Testing to align to scenario testing under Operational Resilience regime.
Concentration risk and 4th parties	Requirement to assess and manage concentration risk, including third party dependencies in a close geographical location and 4th parties.
Cloud	All forms of cloud arrangements are subject to the expectations. Cloud arrangements should not automatically be considered outsourcing, but require materiality and risk assessment to determine commensurate level of control required.
Intragroup arrangements	Subject to the same requirements as external outsourcing and should not be treated as being less risky. Proportionality applies re: level of 'control and influence' that can be exerted over the provider, which enables reliance on group policies, standards and controls – providing they are adequate.

The requirements effectively broaden and deepen the scope of existing TPRM programmes, focusing in on materiality and risk assessment processes, data security controls and assurance; as well as early and enhanced development of BCP and exit plans.

Most firms will need to enhance existing frameworks and approaches, and look at the capabilities required to meet and sustain these going forwards.

03 Meeting the new regulatory requirements

To achieve compliance and to build a more resilient supply chain, we have set out key actions firms should undertake. KPMG has developed a set of accelerators designed to get you there quickly and robustly.

Governance

Key Client Actions to Achieve Compliance

- Engage and involve the Board, by presenting current TPRM framework including TPRM policy, appetite and tolerance levels, and risk management approach
- Carry out Board and Executive training
- Allocate accountability for TPRM to the SMF24 (expected) or another appropriate SMF
- Agree / explain SMF24 accountability for overall framework, policy, and systems and controls. Define the TPRM policy in line with expectations documented by the regulators
- Identify / establish the governance body responsible for TPRM and reporting
- Assess / define MI reporting needs of governance bodies including Board, Board Risk Committee, Executive / Management Committees
- Board to approve, review, and implement documented TPRM policy
- Establish processes to notify the regulator in advance of undertaking any material third party arrangements
- Establish clear and formal links and dependencies to the Operational Resilience programme
- Uplift record keeping to extend the outsourcing register to include other material third party arrangements and meet concentration risk assessment requirements

KPMG Accelerators:

- Executive and Board Training
- MI and reporting templates
- Outsourcing policy
- Pre-defined KPIs and KRIs
- Third Party Inventory Template
- TPRM Governance Body terms of reference

Materiality and risk assessment

Key Client Actions to Achieve Compliance

- Refresh processes for assessing materiality, include criteria stated in Supervisory Statement
- Materiality assessment (and segmentation approach) to reflect “important business services” and link in with Operational Resilience programme
- Refresh processes for assessing risk (entity and service level), include operational and financial risks, and risk mitigations
- Execute process to assess the materiality and risks of all third party arrangements, irrespective of whether they fall within the definition of outsourcing
- Assess suitability of control framework for material or high risk arrangements to ensure it is effective and risk-based (and as equally robust as for outsourcing arrangements)
- Ensure risk assessment methodologies include assessment of concentration risk

KPMG Accelerators:

- Third Party Materiality Assessment model
- Third Party Inherent Risk Assessment tool
- Third Party Risk Assessment as a Service (TPRAaS)
- Third Party Risk – Managed Services

Pre-contract due diligence

Key Client Actions to Achieve Compliance

- Enhance due diligence scope, approach and processes to ensure they are ‘appropriate and proportionate’
- Align due diligence approach to reflect the materiality and risk assessment, and the subsequent segmentation approach
- For material outsourcing, due diligence scope and process is required to address: business model, complexity, financial situation, nature, ownership structure, and scale; capability, expertise, and reputation; financial, human, and technology resources; ICT controls and security; and sub-outsourced service providers
- Consider whether the breadth of domains required to be covered under due diligence is matched with in-house skills, resources and data sources
- Ensure due diligence process documents any 4th parties or sub-outsourcing arrangements and assesses that the third party has appropriate governance and controls of oversight of those 4th parties
- Implement process to track issues and actions and feed into contracting and monitoring

KPMG Accelerators:

- Risk-based due diligence methodology
- Pre-defined domain-specific due diligence questionnaires
- Risk scoring methodology
- Residual risk methodology

Contractual Clauses

Key Client Actions to Achieve Compliance

- Establish processes to feed due diligence and risk assessment results into contractual clauses
- Build assets required to ensure regulatory compliant material outsourcing contracts (both third party and intra-group) – templates & checklists
- Develop contract framework for material non-outsourced third parties to achieve equivalent contractual controls to those that apply to material outsourced third parties
- Review and identify material outsourcing contracts that require remediation and develop a remediation plan
- Ensure material contracts post March 2021 incorporates the stated requirements.
- Establish a process to notify the regulators where material outsource parties don't agree to meet the regulatory requirements

KPMG Accelerators:

- Contract risk framework for non-outsourced material third parties
- Contract assets for material outsourcing third parties – templates & checklists
- Contract remediation methodology
- Technology assisted contract reviews using KPMG's proprietary Ignite CCM tool

Intragroup arrangements

Key Client Actions to Achieve Compliance

- Identify all intragroup arrangements and assess their materiality and risks
- Assess the governance structure and internal control functions including - allocation of senior management functions and responsibilities; ability to alter intragroup arrangements and/or influence terms and conditions to meet UK regulatory obligations and manage relevant UK-specific risks; consistency and robustness of group wide standards controls, policies, and procedures
- Create due diligence and monitoring approach for intragroup arrangements based on:
  - proportionality, level of control, and influence
  - robustness of centralised processes and oversight and the extent they can be relied upon
  - adequacy and coverage of group wide standards, continuity plans, and controls and whether they effectively safeguard operational resilience
- Validate existence and quality of written agreements, including any memorandum of understandings (MoUs), and ensure it appropriately articulates the services that are being delivered, SLAs, obligations to notify on incidents, and key controls to monitor the delivery of the service
- Build in requirements on the service provider to share KPIs, KRIs and RCSAs to support monitoring

KPMG Accelerators:

- Intra-group current state assessment model
- Assessment framework for intra-group agreements
- Approach to governance of intra-group services
- Templates for intra-group agreements
- Framework for monitoring Intra-group Arrangements
- KPI Framework for intra-group arrangements

KPMG TPRM team works together with KPMG Law to help clients on enhancing their contractual risk management process. For more information see KPMG Law: Contracts and Third Party Risk

Ongoing monitoring

Key Client Actions to Achieve Compliance

- Develop processes that use access, audit, and information rights in order to drive identification, assessment, management, and mitigation of risks
- Adapt monitoring processes to be outcomes-focused, to assess whether the service provider is providing the relevant service effectively and in compliance with the firm's legal and regulatory obligations, including operational resilience
- Enhance monitoring process to reflect proportionality (i.e. whether the firm is significant), materiality, and risk of the arrangement
- Implement approach and processes to monitor risks and controls on an ongoing basis throughout the duration of the arrangement. Processes should include tracking and follow-up on actions and issues
- Ensure monitoring covers areas that could impact the firm's own business continuity, operational resilience, and operational risk, including: conduct risk; IT risk, legal risk, reputational risk, GDPR and data protection
- Ensure concentration risk is assessed on a regular basis and is part of the ongoing monitoring framework
- Assess the third party's risk assessment and controls framework for oversight of any material fourth parties are robust and proportionate to the service being provided
- Enhance operational risk monitoring such that it is based on severe but plausible scenarios, e.g. a breach or outage affecting data confidentiality or service availability
- Assess where a failure in performance could materially impair financial resilience (i.e. assets, capital, funding, and liquidity); or operational resilience (i.e. ability to continue providing important business services)
- Expand monitoring scope to include devices, information, systems, and networks used for providing the outsourced service or monitoring its performance. Include where appropriate the service provider's policies, processes, and controls on data ethics, data governance, and data security
- Ensure monitoring includes the results of security penetration testing to assess the effectiveness of implemented cyber and internal IT security measures and processes

KPMG Accelerators:

- Ongoing monitoring methodologies
- Domain-specific ongoing monitoring questionnaires
- K3PID – continuous risk screening tool
- Third Party Risk Assessment as a Service (TPRAaS)
- Third Party Risk – Managed Services

Data Security

Key Client Actions to Achieve Compliance

- Define approach and documentation for Data Security requirements with the objective of understanding in-house and service provider's respective responsibilities
- Develop documentation to include:
  - data classification based on confidentiality and sensitivity
  - potential risks, such as unauthorised access, loss, unavailability, and theft
  - agreed levels of availability, confidentiality, and integrity
  - assurance from third parties on the provenance or lineage of data
- Implement robust controls for data-in-transit, data-in-memory, and data-at-rest, including a range of preventative and detective measures
- Develop assurance process to validate effectiveness of service provider's security environment
- Ensure scope of assurance covers 13 data security control areas - configuration management; encryption & key management; identity & access management (especially privileged access); monitoring of 'insider threats' (incl. contractors, secondees, and sub-outsourced service providers); access & activity logging; incident detection & response; loss prevention & recovery; data segregation; operating system, network, and firewall configuration; staff training; control monitoring; policies & procedures; data deletion
- Assess whether service provider is at least as effective as the in-house security environment

KPMG Accelerators:

- Third Party Security Maturity Assessment and Benchmarking tool
- KACEYTM – AI powered digital task manager
- Continuous security assessment solution

Cloud

Key Client Actions to Achieve Compliance

- Incorporate all forms of cloud arrangement (i.e. SAAS, PAAS etc) within the TPRM framework
- Assess the materiality and risks of the cloud arrangements
- Assess the resilience requirements of the service and data hosted in the cloud and develop resilience options
- Apply due diligence and monitoring regime, and BCP and exit planning requirements stated on previous pages

KPMG Accelerators:

- Cloud risk and control framework
- Cloud regulatory reporting templates
- Insights from cloud regulatory reviews across the sector.

Exit and contingency planning

Key Client Actions to Achieve Compliance

- For new material outsourcing arrangements, prior to onboarding, develop a business continuity plan ('BCP'), and documented exit strategy for stressed exit and managed exits
- For existing material third party arrangement develop or enhance existing business continuity and exit plans aligned to the regulatory requirements
- Ensure the BCPs are primarily focused on the ability of firms to deliver important business services, that are supported by third parties, in line with their impact tolerances in the event of disruption
- Develop scenarios to test stressed exit plans
- Define a plan to carry out BCP testing and scenario testing exercises for all exit plans for material third parties
- Ensure exit plans and scenarios are aligned to the impact tolerances defined through your Operational Resilience programme
- Ensure that for material arrangements, service providers implement appropriate BCPs to anticipate, withstand, respond to, and recover from severe but plausible operational disruption

KPMG Accelerators:

- Exit and Contingency Plan Standards and Templates
- Exit triggers
- Scenario Testing Plan and Templates

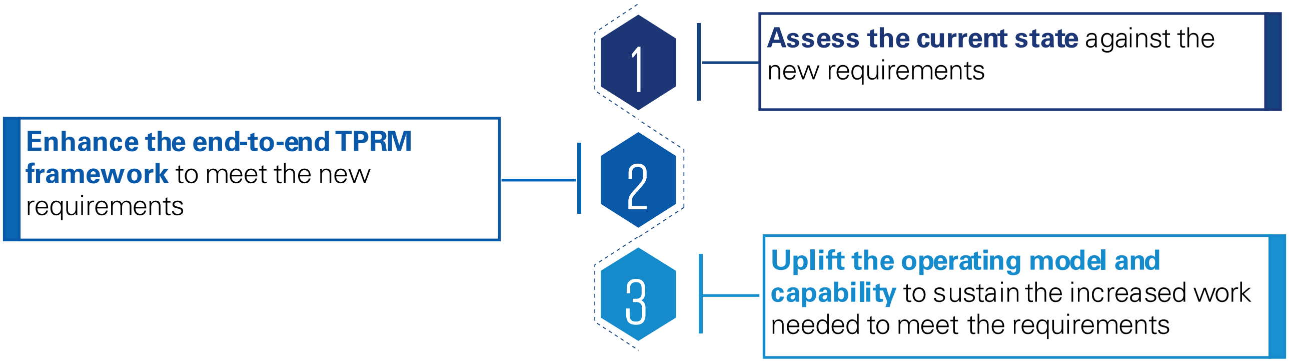
04 Next steps and further insights

Financial services organisations are at different levels of maturity when it comes to TPRM.

For more mature organisations meeting the regulatory requirements will mean enhancements to existing policies, frameworks and artefacts, and potentially an increase in the scope of third parties that are material or high risk.

Less mature organisations will need a more fundamental uplift, delivered through a co-ordinated set of activities, to ensure the requirements are met.

Whatever your current position, KPMG recommends that all organisations should:



1 **Assess the current state** against the new requirements

2 **Enhance the end-to-end TPRM framework** to meet the new requirements

3 **Uplift the operating model and capability** to sustain the increased work needed to meet the requirements

KPMG's technology enabled TPRM solutions can help clients in their journey to build a more resilient and sustainable supply chain.

Powered Enterprise I Risk I Third Party Risk
Build Trust by Harnessing Risk

Assess

Perform **rapid assessments of your TPRM current state** and develop **recommendations and roadmap** for enhancing your TPRM **capability and maturity.**

Enhance

Using KPMG's **global leading practice accelerators** and partnering with **industry leading TPRM technology platform**, enhance **automation, efficiencies and sustainability** of your TPRM capability.

Run

Operate **end-to-end TPRM processes** and **perform risk assessments** using **KPMG's TPRM Managed Service solution.**

To find out more about KPMG's Powered Solution and arrange a demo please get in touch with the Key Contacts listed on the next page.

Contacts

We would welcome the opportunity to share our views and further insights on the new regulatory requirements, as well as offer advice as to the practical steps that you should be taking.
If you have any questions or would like to discuss the implications of this important regulatory development, please contact:

Jon Dowie

Partner
Third Party Risk Management
Financial Services

M: +44 (0)7799 065532
E: jon.dowie@kpmg.co.uk

Rohit Nag

TPRM Lead
Financial Services
Risk Consulting

M: +44 (0)7774 337810
E: rohit.nag@kpmg.co.uk

KPMG

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Legal services may not be offered to SEC registrant audit clients or where otherwise prohibited by law.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Law is part of KPMG LLP, a multi-disciplinary practice authorised and regulated by the Solicitors Regulation Authority. SRA ID: 615423. For full details of our professional regulation please refer to 'Regulatory information' under 'About' at www.kpmg.com/uk