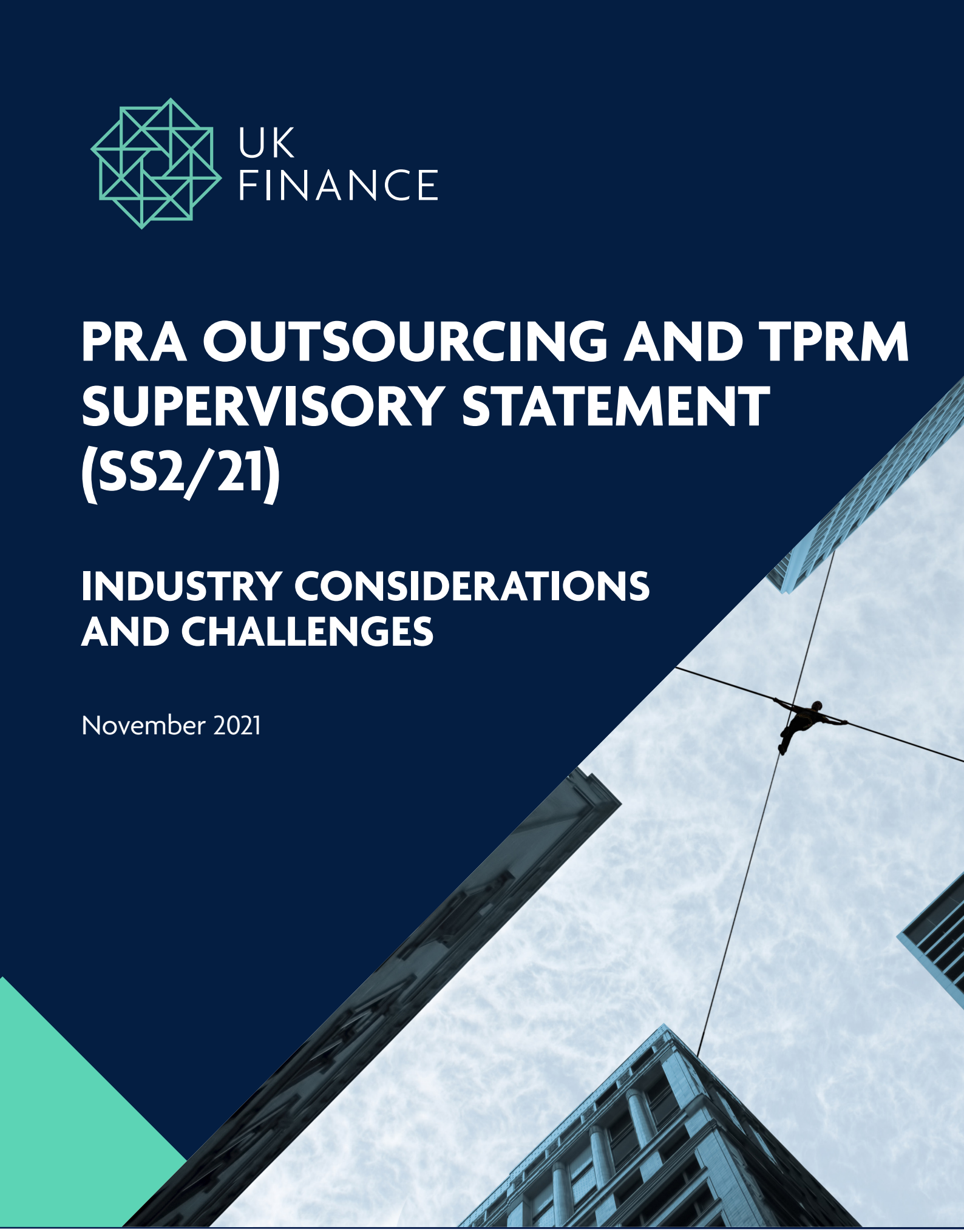
UK FINANCE

PRA OUTSOURCING AND TPRM SUPERVISORY STATEMENT (SS2/21)

INDUSTRY CONSIDERATIONS AND CHALLENGES

November 2021



UK FINANCE

EY
Building a better working world

AUTHORS

Oge Udensi, Principal, Cyber and Third Party Risk, UK Finance
Oge is an experienced Cyber Security Resilience Lead working within the UK Finance's Cyber and Third Party risk team where she engages with key stakeholders within Financial Services to ensure the collective voice of the financial sector on Cyber and resilience policies are maintained. She is also currently leading the cloud initiative, cloud adoption practices and the definition of a standardised cloud security and risk framework, while she continues to play a key role in the expansion of the Financial Sector Cyber Collaboration Centre (FSCCC), an industry utility designed to promote cyber intelligence sharing amongst financial institutions.

Zelfau Rauof, Analyst, Cyber and Third Party Risk, UK Finance
Zelfau holds a master's in International Health Policy and Health Economics with previous experience working within Private Equity as a Depositary Analyst. In her role at UK Finance, she engages with key stakeholders across the sector on relevant cyber and third party policies to ensure the collective voice of the Financial Sector is maintained. She also continues to support the development of the Financial Sector Cyber Collaboration Centre (FSCCC), an industry utility designed to promote cyber intelligence sharing amongst financial institutions.

Kanika Seth, Partner, EY EMEIA Financial Services Third-Party Risk Management (TPRM) Solution Leader and Cybersecurity Leader
Kanika is the EY EMEIA Financial Services Cybersecurity Leader. She also leads the EMEIA Third-Party Risk Management (TPRM) and Outsourcing solution. She has 20+ years of experience in delivering TPRM and Cyber engagements and working closely with regulators to provide thought leadership and market insights to the industry. Kanika has significant experience in working with Boards and Executive Committees, bringing deep expertise in understanding evolving Cybersecurity regulatory expectations.

Shriparna Ghosh, Director, EY Financial Services, Third Party Risk Management (TPRM)
Shriparna is a Director in the Cybersecurity practice (focussing on TPRM) within EY. She leads the Cyber Consulting team in Scotland. She has circa 12+ years' experience in financial services and IT consulting services internationally. She has led multiple large scale transformation and remediation programmes focussing on Third-Party Risk Management (TPRM), Information Security and data privacy. She is passionate about enhancing diversity in the workplace and creating exciting careers for the next generation of digital talent.

Marta Wolinska, Consultant, EY Financial Services, Third Party Risk Management (TPRM)
Marta is a Cybersecurity Consultant in the UK Financial Services practice and has previously worked in financial risk analytics. She has experience delivering various third-party risk management engagements including risk and controls mapping, framework reviews and regulatory remediation work against EBA and PRA guidelines. As an engineer by training, Marta applies a scientific approach to problem solving and is passionate about the use of technology to streamline business processes to bring efficiency gains.

OVERVIEW

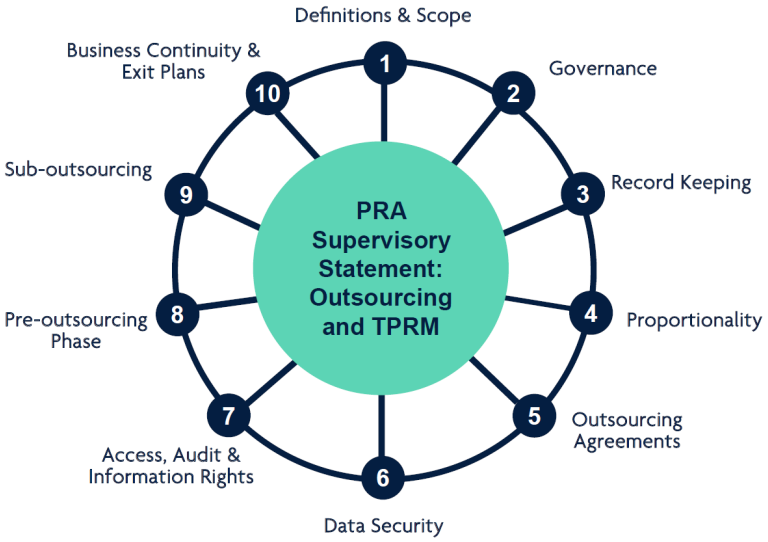
Following months of consultation responses and industry engagement, the Supervisory Statement (SS) on outsourcing and third-party risk management (TPRM) was released by the Prudential Regulation Authority (PRA) in March 2021 with a need to comply with these requirements by 31 March 2022.

The SS, which applies to banks, insurers, building societies, designated investment firms, and third-country branches, does not significantly diverge from the consultation paper published in 2019, and should be considered in conjunction with the operational resilience policy statements.

This SS seeks to modernise the PRA's expectations by clarifying existing requirements on outsourcing and third-party risk management. It also enables the firms to comply with these expectations throughout the lifecycle of an outsourcing and third-party arrangement.

The elements covered in the SS are outlined in the associated graphic.

This paper summarises the key elements in each chapter of the Supervisory Statement and then provides a spotlight view on specific aspects of implementation. It also highlights four key challenges identified across the industry.



KEY TIMELINE TO BE AWARE OF

CONSULTATION

The UK regulators consulted on these rules from December 2019 through 2020.

IMPLEMENTATION

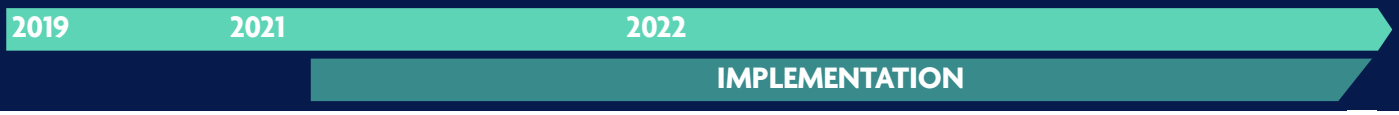
Implementation is required for both legacy agreements and agreements entered into on or after the 31 March 2021.

LEGACY AGREEMENTS (BEFORE 31 MARCH 2021)

Remediation should take place at the first available contractual renewal or revision point. Agreements should be reviewed and updated to the expectations of the SS as soon as possible on or after 31 March 2022.

NEW AGREEMENTS (ENTERED ON OR AFTER 31 MARCH 2021)

Agreements entered into on or after 31 March 2021 should meet expectations by 31 March 2022.



CHAPTER SUMMARY AND INDUSTRY PERSPECTIVES

PRA CHAPTER SUMMARY

Definition and scope

- The PRA's overarching aim is for firms to apply adequate governance and controls to all (both outsourcing and non-outsourcing) third-party dependencies that can impact PRA's statutory objectives.
- The definition of 'outsourcing' was expanded beyond that of the PRA Rulebook (which derives from EU law) to capture all relevant arrangements between firms and third parties not already covered e.g. hardware purchases.
- The materiality and risk of all third-party arrangements should be assessed, even those which do not fall under the definition of outsourcing.
- Third-party arrangements falling under "material" or "high risk" categories should have proportionate risk-based control.

Proportionality

- Proportionality and materiality are separate but complementary concepts; links between these two need to be understood in order to determine appropriate treatment strategies.
- Intragroup agreements are not inherently less risky.
- Although intragroups are subject to similar requirements, firms may comply with some of the requirements proportionately, depending on their level of 'control and influence' over the entity that is providing the outsourced service.
- There is a need to apply proportionate minimum expectations to third-country branches.
- Non-significant firms may outsource certain functions (e.g. internal audit). Their outsourcing policy should reflect complexity, materiality, and the number of outsourcing arrangements.

IMPLEMENTATION SPOTLIGHT

Defining and applying materiality to all third parties

- Firms need to quickly establish their 'house view' of key definitions – e.g. 'outsourcing', 'materiality'.
- Plans need to be clearly set out for the re-assessment of existing suppliers, based on materiality.
- Treatment strategy for 'material non-outsourcing' arrangement needs to be established rapidly.
- Most organisations are looking into proactive solutions to reduce legacy remediation of contracts entered into after 31 March 2021.

Demonstrating control and influence

- Firms are reviewing intragroup agreements to ensure the scope of the relationship is clearly articulated.
- Organisations are updating their policies and processes (where applicable) to ensure they are fit for use by all sub-entities (or intragroup entities).
- Appropriate connectivity and understanding of services will underpin the ability to demonstrate appropriate levels of controls and influence, as without it firms might not be aware of their key dependencies.
- From a sub-entity's point of view, defining KPIs / KRIs and appropriate risk appetite will aid with monitoring. of relationships.

PRA CHAPTER SUMMARY

Governance

- The PRA expects management information provided to the board to be clear, consistent, robust, timely, well-targeted and contain an appropriate level of technical detail to facilitate effective oversight and challenge by the board.
- Firms entering outsourcing arrangements remain accountable for complying with regulatory obligations.

Pre-outsourcing phase

- Firms should assess the materiality of all outsourcing and third-party arrangements using the criteria in the SS and reassess it at defined points in the supplier lifecycle.
- Firms are expected to notify of material outsourcing and third-party arrangements.
- The expectation is to carry out a proportionate risk assessment for material vs non-material arrangements.
- Firms' risk assessments must consider operational, financial as well as group-wide concentration risk.

Outsourcing agreements

- The contractual agreement should not impede or limit the regulator's ability to effectively supervise the firm's outsourcing ability, function, or services.
- Where a material outsourcer or third-party is unable or unwilling to include certain terms within the agreement which reflect the firm's obligations, the firm is required to make the PRA aware of this issue.
- Contracts for third parties (specifically material non-outsourcing arrangements) might require revisiting to meet operational resilience requirements such as including impact tolerances for important business services.

Data security

- Where an outsourcing agreement involves the transfer of data, the PRA expects firms to classify relevant data based on their confidentiality and sensitivity, identify potential risks relating to outsourced data and their impact and agree an appropriate level of data availability, confidentiality and integrity.
- Security requirements are also particularly relevant for cloud providers.
- Firms needs to be aware of cross border regulations and risk-based approach should be applied in this context.

Access, audit and information rights

- Access audit and information rights should be exercised in an outcome-focused way. Pooled audits and third-party certifications can be used only where it is sufficient for firms to meet their obligations.
- Risk-based approach to access, audit and information rights should be applied to all providers (material or non-material).
- Alternative methods of assurance can be agreed

IMPLEMENTATION SPOTLIGHT

Board-level approval and reporting

- Firms need to be clear on where the responsibility for the approval or sign-off of the outsourcing policy and procedures lay. Where this is not a board level expectation, clarity on the relevant committees responsible, should be documented.
- For effective board-level reporting firms need to understand what data they have available and what limitations this poses in providing a clear view of the firm's third-party estate. This understanding should aid the creation of a roadmap to achieve consistent informative reporting across any firm.
- Detailed reporting on holistic third-party portfolios – covering aspects of concentration risk, BCP/exits, inherent and residual risk position etc is as important as granular reporting on individual third parties or outsourcers.

Expanding scope of notification

- Firms might consider developing a single internal framework for notifying the PRA of material outsourcing and material non-outsourcing arrangements. In the first instance, firms may opt to submit a single blanket notification for all legacy material arrangements.
- Firms who are already introducing technology solutions to meet notification requirements will continue to gain value from these investments, as they form a foundation for additional considerations such as operational continuity in resolution (OCIR), impact tolerances etc.

Contract remediation

- This activity needs to be underpinned by an understanding of all existing material contracts.
- Many firms are continuing to follow the timelines that are set out for remediation of outsourcing contracts as per the EBA deadline. However, the increase in scope beyond outsourcing contracts (to material contracts) warrants the design of an additional roadmap.

Cloud considerations

- If a cloud environment is properly configured and responsibilities understood, firms might see a benefit to its resilience, as the overall infrastructure could be more robust. However, when engaging with third parties, firms need to understand if their use of cloud (where applicable) is aligned to the firm's own strategy and resilience considerations. Cloud resiliency options should be considered as part of firms' business continuity and exit planning. This needs to be considered by firms on a case by case basis.
- A detailed understanding of the cloud service providers used by the firm's outsourced and non-outsourced third parties is also necessary in order to understand whether an aggregate risk exists from one provider.

between the service provider and client, where onsite visits would create an unmanageable risk for either party.
- For material outsourcing arrangements, firms need to inform their supervisor if alternative means of assurance have been agreed.

Sub-outsourcing
- Firms should have the right to approve or object sub-outsourcing of material outsourcing arrangements.
- Firms should monitor such sub-outsourced service providers' involvement in the provision of important business service.
- There is emphasis on critically assessing the risk of sub-outsourcing (or 4th party providers) and the firms are expected to take into account (where applicable) the complex chain of sub-outsourcing and assess their operational resilience.

Business continuity and exit plan
- Firms should develop and maintain business continuity plans and documented exit strategies for both stressed and non-stressed exits.
- Business Continuity Plans (BCP) should consider options to withstand/recover from an outage at a service provider.
- Business continuity and exit plans should be tested on a periodic basis.
- Consider the implications of deliberately destructive scenarios (e.g. cyber-attacks) and effective crisis communication measures in place.
- Firms should include conditions enabling the regulators to assess the effectiveness of service providers' business continuity plans.

Outcome-focused approach in audit
- The level of assurance required from a third party to meet all their obligations will vary based on risk profile.
- This should be defined by the firm as part of their proportional risk based approach. Treatment strategies should outline the outcome-focussed and risk based approach towards managing outsourcing and third party providers.

BCP / Exit testing methodology
- Firms should be able to understand how they can continue delivering services in case of an outage (for all types of providers, including cloud providers). The ultimate goal is to ensure resilience and there is no prescriptive approach mandated.
- Exit scenarios (for stressed and non-stressed exits) and continuity measures need to be considered prior to signing contracts.
- Testing of BCP and exit plans should include an assessment of possible scenarios and consider what suitable (and practical) testing options are available.
- Firms need to take a risk-based approach when selecting testing options. Tabletop exercises could be a potential cost-effective methodology for lower-risk suppliers. In the future, as the requirements become more engrained, large suppliers might offer testing options as part of the due diligence or supplier assurance activity.

KEY INDUSTRY CHALLENGES

In order to become compliant against PRA SS 2/21, firms are using various implementation strategies, depending on their level of maturity. Some of the key industry challenges and associated insights are captured in the below section:

INTERDEPENDENCIES BETWEEN OPERATIONAL RESILIENCE AND TPRM

- A significant volume of work needs to be delivered in an efficient manner across the outsourcing and TPRM and operational resilience agenda, to ensure that the compliance activities are completed as per regulatory deadlines. Clear linkages must be established between the operational resilience and TPRM programmes upfront.
- Business continuity planning and scenario testing: Business continuity for third parties needs to incorporate scenario testing and the impact tolerances of important business services (IBS). The impact of third parties on IBSs needs to be considered as part of business service mapping; with exit planning and substitutability considerations accounted for in the pre-contract stage.
- Impact tolerance: The definition of impact tolerances has a large downstream impact on the TPRM programme(s). It needs to be considered in the context of business continuity planning, scenario testing, contractual terms as well as to drive due diligence and treatment of third parties.
- Governance: Clear and aligned roles and responsibilities are required across operational resilience and TPRM. Governance processes should be reviewed to clarify ownership, accountabilities and activities relating to important business services and third parties.
- Aligned documentation: Evolving regulatory requirements have led to a complex framework landscape which is not always fully aligned. A simple to follow, consistent, suite of documents is required to address all stakeholder needs and allow future-proofing of end-to-end processes in relation to resilience and outsourcing / TPRM.
- Prioritisation: Use of agreed and established taxonomies through both programmes is essential for consistent and effective prioritisation as well as proportionate resilience activities. These priorities should feed into TPRM tools such as inherent risk assessments.

Across the industry, various implementation approaches are being employed and overall there is a recognition of the need for further collaboration and alignment in relation to governance, taxonomy, policy, consideration of impact tolerances as part of the firm wide approach (including intra-groups). It is important to identify synergies between the TPRM and resilience programmes, specifically in the identification, review and monitoring for critical / material / high risk-third party services.

VIEWS ON BROADER CONTRACT REMEDIATION

- Contracts entered into after 31 March 2021 need to be fully compliant (including the presence of business continuity plans and exit strategies) by 31 March 2022.
- To effectively remediate, firms will need to have an understanding of the materiality of their suppliers, therefore the definition of materiality should be agreed upfront and materiality assessments should be applied to all arrangements as soon as possible.
- Firms should perform a review of their contractual terms with a resilience lens to assess whether current terms are sufficient or whether further resilience considerations need to be included in contracts (specifically for all material ones). Note - impact tolerance needs to be included in contractual terms.
- Once remediation effort has been estimated, firms need to take a risk-based approach in prioritising activities.

Depending on the firm's level of maturity, their contractual terms might already include robust resilience considerations. However, firms need to review their contractual terms to ensure alignment with PRA expectations. The success of the contractual remediation activity is dependent on the firm's ability to identify material arrangements and effectively execute the implementation of compliance activities such as the inclusion of business continuity and exit plans pre-contract. A plan should be developed to tackle legacy remediation of all other contracts at minimum at their point of renewal.

SUB-OUTSOURCING

- The PRA expects a detailed understanding and consideration of fourth parties and sub-outsources by firms across their supplier population. This includes understanding of risk levels, concentration risk and resilience considerations.
- Firms should look to develop an understanding of their fourth party or sub-outsourcing population through methods such as inclusion in the due diligence process or supplementary steps in supplier assurance.

Understanding of complex supply chains across the sector is still in its nascent stages, however the direction of travel in the coming years will enable better understanding of the supply chains. In particular, a careful understanding of cloud service providers should be explicitly addressed in firms' strategies. Firms needs to be aware of cross border regulations and a risk based approach should be applied in this context as well, specifically when looking at long complex chains of service providers.

Current fourth party monitoring across the industry relies on contractual terms established with the third party, the third party's risk assessment of the fourth party or on contractual terms between the third and fourth parties, with the first two being more prevalent. Very few firms perform independent reviews on fourth parties but current methodologies, such as inclusion in risk assessment, could be enhanced through use of automated threat intelligence tools for more insightful reviews of fourth parties.

APPROPRIATE LEVEL OF ASSURANCE ON THIRD PARTIES

- PRA has statutory information-gathering powers that applies to third-party service providers (S.165A of FSMA) as well.
- Firms are exercising their audit and access rights in a risk-based manner. Pooled audits and third-party certifications are also being considered as an input into the risk assessment exercise. Firms need to make sure that appropriate review of the risk position is conducted in order to be able to understand their exposure.
- Receiving appropriate assurance from cloud service providers is challenging for all firms regardless of size.
- There is a recognition that certain types of onsite audit may create an unmanageable risk for the environment of the provider and/or another client of the service provider. In such cases, the firm and the service provider are agreeing on alternative ways to provide an equivalent level of assurance, e.g. via the inclusion of specific controls to be tested in a report or certification.

One of the key challenges firms are facing in relation to outsourcing and TPRM is the availability of resources as well as availability of required knowledge and skills to undertake assurance exercises. There is also an uptake in organisations using external frameworks such as NIST, ISO and COBIT to baseline their risk assessment of third parties. There is a lot of pressure to deliver due diligence or assurance outcomes faster, across a broader and deeper scope. To do this, organisations are turning to market utilities or managed service propositions more often to decrease cycle times and increase the quality of data going into due diligence and ongoing oversight decisions. For these solutions to be effective however, they need to be embedded into the firm's operating model, with agreed control framework and risk thresholds. Firms are gradually shifting the internal headcount that traditionally supported TPRM functions to more value-adding risk management activities, and engaging external parties to handle the variable nature of assessment volumes.