THE INVESTMENT ASSOCIATION

MEMBER GUIDANCE

OPERATIONAL RESILIENCE AND THIRD PARTY PROVIDERS

July 2023

ABOUT THE INVESTMENT ASSOCIATION (IA):

The IA champions UK investment management, supporting British savers, investors and businesses. Our 250 members manage £10.0 trillion of assets and the investment management industry supports 122,000 jobs across the UK.

Our mission is to make investment better. Better for clients, so they achieve their financial goals. Better for companies, so they get the capital they need to grow. And better for the economy, so everyone prospers.

Our purpose is to ensure investment managers are in the best possible position to:

- Build people's resilience to financial adversity
- Help people achieve their financial aspirations
- Enable people to maintain a decent standard of living as they grow older
- Contribute to economic growth through the efficient allocation of capital

The money our members manage is in a wide variety of investment vehicles including authorised investment funds, pension funds and stocks and shares ISAs. The UK is the second largest investment management centre in the world, after the US and manages over a third (37%) of all assets managed in Europe.

CONTENTS

1. INTRODUCTION

The UK Operational Resilience Rules published in March 2021 in PS21/3: Building Operational Resilience apply to: banks; building societies; PRA-designated investment firms; insurers; Recognised Investment Exchanges; enhanced scope SM&CR firms; and entities authorised and registered under the Payment Services Regulations 2017 or Electronic Money Regulations 2011. They introduced a new regulatory expectation that ***'when a firm is using a third-party provider in the provision of important business services, it should work effectively with that provider to set and remain within impact tolerances. Ultimately, the requirements to set and remain within impact tolerances remain the responsibility of the firm, regardless of whether it uses external parties for the provision of important business services'.***

Investment management firms which are not subject to the most extensive requirements under these rules must still comply with SYSC 8 requirements on outsourcing and can take a proportionate approach to implementation using the rules as guidance for best practice where applicable.

The nature of outsourcing and third party service provision in the investment management industry and the wider financial sector is extensive. There are numerous benefits, as well as risks, inherent to such arrangements. From an operational resilience perspective, outsourcing and third-party service provision changes the firm's risk profile, and in many cases results in greater resilience. At the same time, it can pose risks that need to be managed.

Firms relying on third parties need to be able to demonstrate that they are effectively managing the risk of disruption and harm to their customers and end consumers. This guide aims to help firms do just that.

The IA Operational Resilience Third Parties Working Group (Working Group), set up in conjunction with Macfarlanes LLP and EY, was launched in 2022 to address the requirements of the UK Operational Resilience Rules in relation to third party service provision. The group, made up of around 25 member firms of various sizes and business models, including some firms who are themselves third parties for others, met several times to discuss the subject. This guide represents the final output of the Working Group and has been informed by the discussions held.

This guide builds on the IA's earlier operational resilience guidance on governance, important business services, impact tolerances, scenario testing and self-assessment documents. Readers are encouraged to refer to these accompanying guides alongside the insights contained within this document.

We would like to thank Macfarlanes and EY for their help with facilitating this Working Group and members of the Working Group for sharing their insights.

HOW TO USE THIS GUIDE

This document represents optional industry guidance. Firms referring to this guide will need to assess the proportionality of what is suggested for their firm's specific circumstances, and be mindful that not every suggestion will be relevant for every firm.

The suggestions and any lists provided within the document may be non-exhaustive, and should be seen as a guide, rather than a definitive catalogue.

2. DEFINITIONS

Third Party Provider (TPP): An external service provider that performs a process, service or activity on behalf of a firm.

Key Third Party Provider: A TPP which the firm determines as critical to the firm. In this guide we adopt the term Key Third Party Provider in order to avoid confusion with the concept of Critical Third Parties to the Finance Sector, as introduced in DP3-22: Critical Third Parties to the Finance Sector (see Section 6.1 for more detail on these proposals).

Critical Third Party: Entities designated by HM Treasury as Critical Third Parties to the UK finance sector. See Section 6.1 for more details.

Critical Third Party Provider: Entities designated as Critical ICT Third Party Providers under the EU DORA. See Sections 3 and 6.2 for more details.

Outsourcing: In this guide we follow the *FCA's definition of outsourcing*. Essentially, a firm is outsourcing when it has 'an arrangement where a service provider performs a process, service or activity on behalf of a firm which the firm would otherwise carry out itself. So, for example, a firm can outsource the hosting of a data centre or business process to a third party'.

Third Party Service Provision: Not all services provided by third party providers are considered outsourcing. If the service performed by a third party is something the firm would not typically do itself, then this would not be classed as outsourcing. For example, firms relying on email and software applications/ services which they buy from third parties would not be considered outsourcing, because firm would not typically build these in house.

Important Business Service (IBS)[1]: A service provided by a firm, or by another person on behalf of the firm, to one or more clients of the firm which, if disrupted, could:

1. cause intolerable levels of harm to any one or more of the firm's clients; or
2. pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets.

Impact tolerance: An impact tolerance reflects the first point at which a disruption to an important business service would cause intolerable levels of harm to consumers or risk to market integrity.

Vulnerabilities: Weaknesses in the firm's operational resilience that threaten the firm's ability to deliver its important business services within the impact tolerances set.

[1] https://www.handbook.fca.org.uk/handbook/glossary/G3505i.html?date=2022-03-31

3. REGULATORY REQUIREMENTS

This section aims to signpost to the main regulatory responsibilities firms need to be aware of regarding third parties and outsourcing in the context of operational resilience. This guidance document is chiefly centred on firms' responsibilities under FCA PS21/3: Building Operational Resilience. However, there are many other regulatory requirements concerning third-party service provision and outsourcing that the Working Group has considered, and these are reflected where appropriate in this guide.

3.1 SUMMARY OF RELEVANT REGULATIONS AND GUIDELINES

FCA PS21/3: Building Operational Resilience[2]

The publication of the FCA's policy statement in March 2021 outlined their final rules and expectations for firms triggered the start of a 12-month implementation period for firms. By 31 March 2022 firms were required to have carried out mapping and scenario testing to a level of sophistication necessary to accurately identify their important business services, set impact tolerances and identify any vulnerabilities in their operational resilience and review once a year whenever there is a material change to their business or the market in which they operate. Although firms have until 31 March 2025 to continue developing mapping and testing to a more sophisticated level with a view to being able to consistently remain within impact tolerances for each important business service, the FCA has made clear that firms should not wait until the end of the 3 year transitional period and should remain within their tolerances as soon as reasonably practicable.

The mapping exercise includes identifying where third-party providers are present in supply chains. The policy expects firms to be responsible for accurately mapping any relationship outsourced to an external third-party. If a firm outsources to a third party, the regulatory expectation is that the firm still needs to be able to understand the potential vulnerabilities by mapping where those vulnerabilities occur, whether they sit with the third party or beyond. If the firm is unable to obtain sufficient information from the third party to satisfy them that they can operate within tolerance, then it should review and where necessary change their arrangements.

[As will be discussed in more detail in Section 4: Key challenges, obtaining sufficient information from third parties has proven difficult in practice, and there are frictions to changing suppliers.]

By actively capturing and maintaining relationships with third-party providers, the FCA expects firms to satisfy themselves of that third party's resilience.

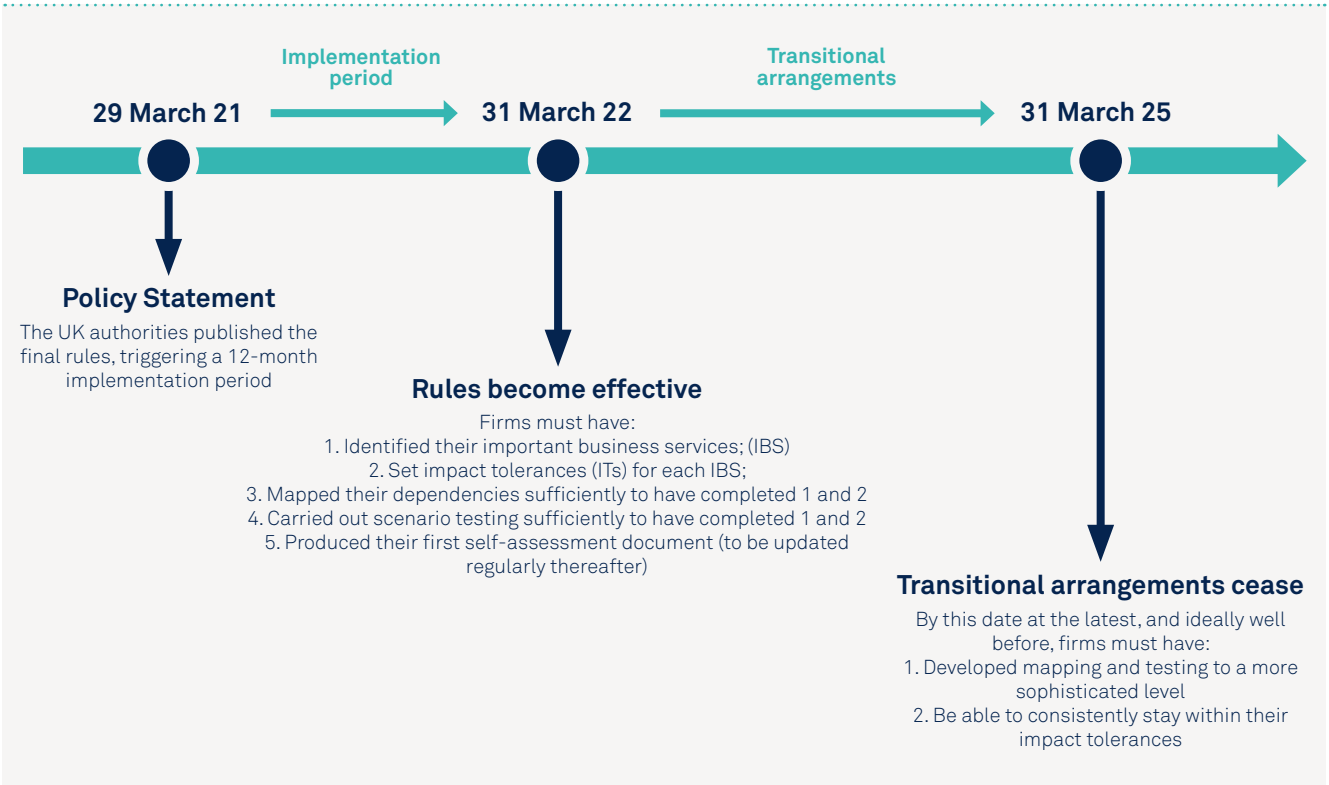
With respect to where a firm uses a third-party provider in the provision of important business services, the policy says the firm should work effectively with that provider to set and remain within impact tolerances. Ultimately, the requirements to set and remain within impact tolerances remain the responsibility of the firm, regardless of whether it uses external parties for the provision of important business services.

On testing, the policy statement says firms should approach testing with third parties in the same way as they approach the mapping exercise, working as effectively as possible with third parties to facilitate testing. This could mean that either the firm or the third party carries out testing. Firms in scope of the policy

will need to satisfy themselves, if the third party is going to carry out any testing, of the methodologies, scenarios and considerations of the third party in doing so. The firm is ultimately responsible for the quality and accuracy of any testing carried out, be that by themselves or by an external party.

See SYSC 15A for the specific applicable rules on mapping and testing[3].

[2] PS21/3: Building operational resilience: Feedback to CP19/32 and final rules (fca.org.uk)
[3] SYSC 15A - FCA Handbook



PRA Statement of Policy: Operational Resilience[4]

Dual regulated firms also have to comply with the PRA's operational resilience rules, in addition to the FCA's rules.

The PRA's statement clarifies how the PRA's operational resilience policy affects its approach to four key areas of the regulatory framework in particular: governance; operational risk management; business continuity planning (BCP); and the management of outsourced relationships. The PRA emphasised the importance of accountability and the need for senior management leadership to prioritise the investment and cultural change required to improve operational resilience.

The PRA expects in scope firms to understand how their outsourcing and third party dependencies support important business services. They also expect firms to be able to remain within impact tolerances for important business services, irrespective of whether or not they use third parties in the delivery of these services. This means that firms should effectively manage their use of third parties to ensure they can meet the required standard of operational resilience.

In addition, *SS1/21* addresses the operational resilience of firms' important business services.

SYSC 8.1 General outsourcing requirements[5]

These are the FCA's fundamental expectations for firms with respect to outsourcing.

At the cornerstone of these requirements is the expectation that where a firm relies on a third party for the performance of operational functions that are critical to regulated activities, by doing so the firm does not materially impair the quality of its internal control or the ability of the FCA to monitor the firm's compliance with relevant regulations.

[4] SoP 'Operational resilience' (bankofengland.co.uk)
[5] SYSC 8.1 General outsourcing requirements – FCA Handbook

PRA SS2/21 Outsourcing and third party risk management[6] and PS7/21[7]

Chapters 5 to 10 of SS2/21 set out detailed expectations on how firms should perform due diligence and obtain effective and proportionate assurance from third parties, including through scenario testing.

The PRA expects contractual agreements for material outsourcing arrangements to include 'requirements for both parties to implement and test business contingency plans. For the firm, these should take account of firms' impact tolerances for important business services. Where appropriate, both parties should commit to take reasonable steps to support the testing of such plans.

Firms' business continuity and exit plans for material outsourcing arrangements should 'where possible and relevant ... align to, support, or even be a component of firms' scenario testing for operational resilience.

The PRA also clarified its approach to EU Guidance. Consistent with the PRA approach set out in the Statement of Policy 'Interpretation of EU Guidelines and Recommendations: Bank of England and PRA approach after the UK's withdrawal from the EU' the PRA does not expect PRA-regulated firms to make every effort to comply with any ESA Guidelines that came into effect after the end of the Brexit implementation period, including the ESMA Guidelines on outsourcing to cloud service providers.

Notwithstanding this approach, the PRA has confirmed that the final Supervisory Statement does implement the EBA Outsourcing Guidelines. The Supervisory Statement should however be the primary source of reference for in-scope UK firms when interpreting and complying with PRA requirements on outsourcing and third party risk management. In particular, there is additional guidance in the Supervisory Statement that elaborates on the EBA Outsourcing Guidelines.

For UK firms with European operations, all relevant ESA Guidelines will continue to apply to their European operations and to the activities undertaken in the EU.

September 2019: EBA Outsourcing guidelines[8]

The guidelines set out specific provisions for firms' governance frameworks with regard to their outsourcing arrangements and the related supervisory expectations and processes. Outsourcing to cloud service providers is also covered.

The Guidelines have in practice generated many questions on flow down to sub-contractors, particularly around audit rights and penetration testing rights.

There are some issues with implementation of the Guidelines where firms have taken a group wide approach. It can be challenging for providers who as a result are dealing with parties to whom the rules do not apply.

In accordance with the FCA's approach to non-legislative materials, these guidelines continue to be relevant to UK firms.[9]

EBA Guidelines on ICT and security risk management

Although not specifically focused on operational resilience, ICT and security risks form part of a firm's approach to operational resilience. The EBA Guidelines on ICT and security risk management include steps to be undertaken by firms on a regular and ongoing basis to identify their supporting processes and assets, to establish and implement preventive security measures, to test and assess their resilience plans against a range of scenarios, and to prioritise business continuity actions using a risk-based approach. As above for the EBA Outsourcing guidelines, the FCA's approach is that these guidelines continue to be relevant to UK firms.[10]

[6] SS2/21 Outsourcing and third party risk management | Bank of England
[7] PS7/21 | CP30/19 Outsourcing and third party risk management | Bank of England
[8] EBA BS 2019 xxx (EBA Draft Guidelines on outsourcing arrangements).docx (europa.eu)
[9] Brexit: our approach to EU non-legislative materials (fca.org.uk)
[10] Brexit: our approach to EU non-legislative materials (fca.org.uk)

EU Digital Operational Resilience Act (DORA)[11]

The European Commission's Digital Operational Resilience Act Regulation and Directive (DORA) focus on the ICT risks that can pose a challenge to the operational resilience of the EU financial system.

DORA regulations will most likely have a direct impact on certain ICT third party service providers.

DORA's five key proposals include requirements relating to:

- ICT risk management
- ICT-related incident reporting
- Establishing EU-wide standards for digital operational resilience testing
- Harmonising firms' management of third-party risk
- Creating a regulatory framework for Critical ICT Third Party Providers (CTPPs).

Critical ICT Third Party Provider oversight

Similar to the UK CTP proposals outlined in Section 6.1, contained within the EU DORA are provisions relating to regulatory oversight of Critical ICT Third Party Providers (CTPPs).

There will likely be a large degree of overlap between the entities designated as CTPs in the UK and CTPPs in the EU. Cloud Service Providers, in particular, have explicitly been signalled as likely falling within scope of both sets of rules.

Designated CTPPs will be expected to demonstrate their resilience to the European Supervisory Authorities (ESAs). The ESAs will have the power to assess CTPPs and issue recommendations for them to make improvements to their resilience. If these are not heeded, the ESAs will have the power to issue fines and also to direct FS firms to pause or cancel their contracts with CTPPs.

The related technical standards for the CTPP oversight framework are yet to be issued, but should be published by 17 July 2024 at the latest, 18 months after the DORA officially came into force.

Next steps

It should be noted that DORA is a regulatory framework in and of itself. It sets out legislative requirements at a high level (though both a regulation which has direct effect in member states and a directive (amending certain other EU directives) which EU member states will need to implement through national law). European Supervisory Authorities (ESAs) will need to translate the requirements into a common supervisory framework (regulatory technical standards) prior to the final compliance deadline. These regulatory technical standards will specify much of the technical and practical detail.

Timeline:

- DORA adopted by EU on 16 January 2023 commencing a two year implementation period.
- June 2023: Public consultation on the regulatory technical standards for an industry-wide ICT risk management framework.
- November 2023: Public consultation on the regulatory technical standards for third-party ICT risk management and sub-contracting.
- 17 January 2025: Implementation period ends. DORA takes effect in the EU.

[11] Regulation of the European Parliament and of the Council on digital operational resilience for the finance sector

3.2 CLOUD SERVICE PROVISION

The main regulations and related consultations firms need to be aware of regarding cloud service provision are:

September 2019: EBA Outsourcing guidelines[12]

These guidelines set out specific provisions for firms' governance frameworks with regard to their outsourcing arrangements and the related supervisory expectations and processes. Outsourcing to cloud service providers is also covered.

July 2016: FG 16/5 Cloud Outsourcing Guidance[13]

This guidance was initially applicable to all firms; however it was updated to remove institutions such as credit institutions in September 2019 due to the application of the EBA Guidelines from 30 September 2019.

December 2020: ESMA Final Report Guidelines on outsourcing to cloud service providers[14]

Sectorial guidelines on outsourcing to the cloud. The paper takes the EBA and EIOPA guidelines into account. It was also mindful of the European Commission's Digital Operational Resilience Act Regulation (DORA). The Final ESMA guidelines were published in May 2021 (after the Brexit transition) so do not apply to the UK, though do apply to those firms with a pan European model. However, the FCA confirms that firms should continue to have regard to ESMA's Final report: Guidelines on outsourcing to cloud service providers published in December 2020 (prior to the end of the Brexit implementation period).

October 2021: IOSCO Principles on Outsourcing[15]

These principles address wider issues with outsourcing and seven principles along with guidance. It includes an annex on outsourcing and cloud computing for credit rating agencies; executive summary notes that those basic approaches to cloud computing span the financial services sector.

[12] EBA BS 2019 xxx (EBA Draft Guidelines on outsourcing arrangements).docx (europa.eu)
[13] FG16/5: Guidance for firms outsourcing to the 'cloud' and other third party IT services | FCA
[14] Guidelines On outsourcing to cloud service providers (europa.eu)
[15] FR07/2021 Principles on Outsourcing (iosco.org)

4. KEY CHALLENGES

The process of obtaining the necessary information required from third parties in order to form an adequate assessment is frequently cited as one of the biggest obstacles currently being faced by firms in terms of implementing the UK Operational Resilience Rules. There can be a disconnect in some cases between firms' expectations of what others should disclose to them, versus what TPPs are willing to disclose.

Under the UK Operational Resilience Rules for firms, the onus is solely on customer firms to obtain adequate assurance over their third-party arrangements and outsourcing. There is no corresponding requirement on third parties to accommodate their customers' efforts to gain assurances, and therefore the extent to which TTPs are willing to engage with their financial services customers on operational resilience can be dependent on the balance of incentives they face for doing so. In the table below we summarise the incentives in play from the perspective of TPPs. In certain cases, the balance of incentives can be weighed against sharing sufficient information with customer firms.

The UK Operational Resilience Rules state that if firms are unable to obtain sufficient information from the third party to satisfying them that they can operate within tolerance, then they should review and where necessary change their arrangements. However, experience in practice reveals that frictions exist which make changing TPPs difficult. Ending a supplier relationship can be complex and require significant time to exit. In some cases, there may be a lack of suitable alternative providers to substitute to. As a result, firms can find themselves to some extent 'locked-in' to their relationships with TPPs.

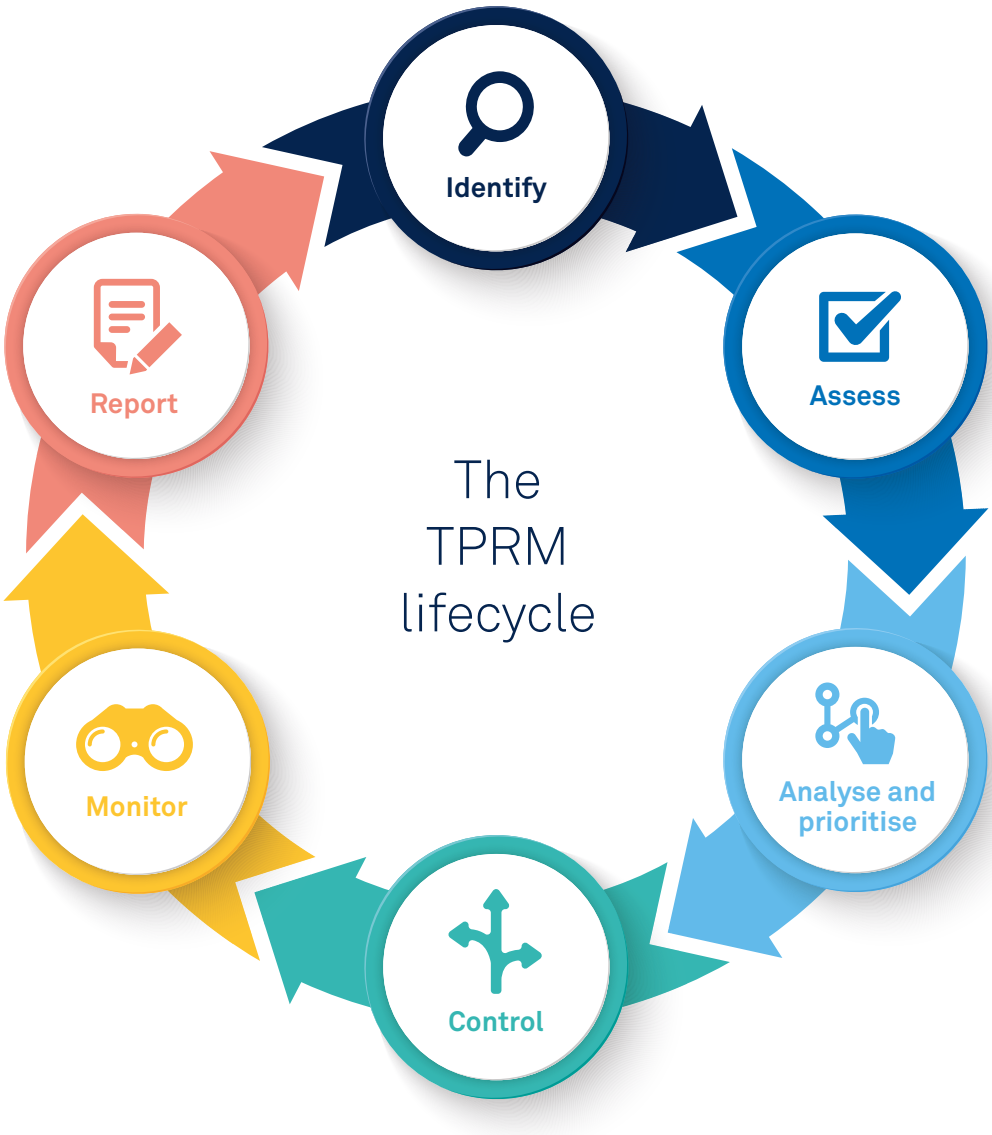
Recovery from a loss of a key third party provider represents another significant challenge. Such a recovery will likely be difficult and time consuming. In certain scenarios, it could also lead to the breach of impact tolerances.

Incentives for engagement / disclosures	Incentives against engagement / disclosures
Commercial: Ultimately, where a firm is unable to obtain satisfactory evidence of their TPP's resilience or ability to support their IBSs, the firm will have to consider taking their business elsewhere.	**Commercial:** In practice, it may be quite drastic, complicated, drawn out, costly and risky for a customer firm to end the relationship. Some customer firms may be more likely to tolerate a level of risk acceptance before taking such a step. Also, a firm may be unlikely to terminate a relationship simply because disclosures cannot be elicited if all other indicators do not suggest there is a problem. Moreover, in some markets, there is a lack of viable alternative providers for customers to switch to, which further weakens the commercial imperative to help firms with disclosures to help them satisfy their regulatory obligations.
Relationships: Where a good working relationship has been fostered between the firm and the TPP, the TPP may be inclined to preserve the relationship by satisfying information requests.	**Disclosure is optional:** TPPs are not mandated to make disclosures to firms where contractual provisions are not in place
Demonstrate resilience: Where the resilience of a TPP is evidenced through robust processes and controls, information disclosures may offer TPPs the opportunity to demonstrate their resilience to their clients, including at the outset of the relationship. Some may consider it to be a commercial advantage.	**Risk:** TPPs may be uncomfortable about disclosing information to clients. This could be because of the potential correlation between disclosure and contractual commitment, risk, and liability. TPPs may also be wary of divulging any competitive or confidential information.
	Information and power asymmetries: As the HMT ***Critical third parties to the finance sector policy statement*** states: *"There may also be significant information and power asymmetries between certain third parties and firms, which may prevent firms from obtaining adequate assurances that their contractual arrangements achieve an appropriate level of operational resilience".*

5. A FRAMEWORK FOR THIRD PARTY RISK MANAGEMENT IN THE CONTEXT OF OPERATIONAL RESILIENCE

This section of the guidance provides a high-level framework for the management of third parties in the context of operational resilience.

The framework consists of six categories, each addressing a segment of the TPRM lifecycle.



Please note that all lists presented in this document are not exhaustive, nor applicable to all member firms, but have been provided as an illustrative guide.

High level category	Sub-topics
Identify	• Mechanism for identifying third parties key to IBS (needs to be done proportionately) • Mapping (identifying who is providing the service) • 4th parties, nth parties • Categories of third parties (e.g., transfer agents, custody banks, etc) • How to determine if a TPP is critical • Regulated vs unregulated TPPs
Assess	• Due Diligence Questionnaires • Further due diligence/ engagement, e.g., follow up questions, live meetings, site visits, checklists (including sub outsourcers) • How can firms engage effectively with TPPs? • Audits (physical and virtual) • Shared assurance models • External assurance / audit • Assessment methodology – Creation of a TPP risk profile • Intragroup oversight • Oversight model
Analyse and prioritise	• Testing – internal testing / contingency testing for loss of TPPs • Testing – testing the business continuity arrangements of TPPs • Testing – joint scenario testing • Testing – exit plan testing (stressed and non-stressed) • Mapping vendor concentration risk (location and usage) – Including whether or not the supplier understands their own concentration risk • Impact tolerance vs third party RTO
Control	• Controls • Contract updates • Exit plans • Recovery, resolution, wind down planning • Service substitution
Monitor	• Tooling • Intra-group oversight • Governance • Oversight models for material outsourcing, IBS and non-IBS
Report	• Management information • What to document in the Self-Assessment

5.1 IDENTIFY

Identifying third parties supporting important business services

The current financial regulatory frameworks require firms to manage risks to their individual Operational Resilience, including where these risks stem from their reliance on third parties for the provision of important business services (IBS). Thus, the identification of all TPPs supporting the firm's important business services is an essential starting point for the effective management of third-party resilience.

Firms (per PS 2/21 and SYSC 15 A) are expected to identify and document the resources essential for the delivery of an IBS. These resources/ assets may be categorised across the following:

- Process
- People
- Technology
- Data
- Premises
- Third-party

Each of these resources, in the context of each firm's IBS, these may be:

- delivered internally (by the firm),
- delivered by using a TPP service.

The delivery by TPP may be external or intra-group.

As firms look to identify TPP relevant to IBS, they can leverage existing data sources which include, but are not limited to:

- Service mapping from the prior year's Operational Resilience Programme (the mapping that has been done in the lead-up to the first Operational Resilience implementation regulatory milestone in March 2022);
- Process, risk and control mapping;
- Third Party Risk Management / Vendor Management Programme;
- Process mapping from Business Continuity Planning, Operational Continuity in Resolution (OCIR); and/or
- Central Securities Depositories Regulation (CSDR), Consumer Duty.

If gaps are found within these existing programmes after leveraging existing data sources to identify TPPs, then this presents a potential opportunity for the firm to consider undertaking new business mapping activities, a vendor refresh/ evaluation programme and/ or a material spend analysis.

Determining the criticality of third parties supporting important business services

Once all the TPPs supporting IBSs have been identified, firms should determine whether each TPP is critical or not. In this guide, we refer to TPPs deemed critical to the firm as 'Key Third-Party Providers' (KTPPs). This is to avoid confusion with the concept of Critical Third Parties to the finance sector more broadly, as introduced in DP3-22: Critical Third Parties to the Finance Sector (see 4.3 for more detail on these proposals).

Firms should be able to identify the IBSs supported by each TPP and establish whether each TPP has the potential if disrupted, to materially impact and/ or halt the IBS, ultimately resulting in harm to the consumer, firm or market. This, therefore, requires that firms understand the elements of each IBS that each TPP supports.

Additionally, firms should investigate whether each third party supports important internal processes (or group services) and whether they have the potential to affect service quality and, ultimately, the IBS. Firms should also consider if there is a need to develop an exit strategy and how easy it is to substitute the supplier with an alternative.

Key factors that firms should consider in determining the criticality of its TPP include, but are not limited to:

- The number of IBSs that the TPP supports;
- Whether the TPP has the potential if disrupted, to materially impact service quality and/ or halt an IBS;
- Whether the TPP supports critical processes or critical elements of an IBS;
- Whether the TPP is a material supplier / supports critical internal processes;
- Specific services provided;
- Uptime requirements;
- Regulatory Requirements; and
- Substitutability of the service provider.

There is no one set way of approaching the task, and firms may wish to utilise scoring models or tiering systems to help determine the criticality of their TPP. Such models may be helpful when there is a large volume of TPPs to work through. However, it is important to keep the key aim in mind which is to Identify what is truly critical and what has the potential to disrupt the functioning of IBSs and ultimately cause intolerable harm.

Following this logic, different naming patterns may be utilised to capture the different suppliers in accordance with the firm's risk taxonomy, e.g.:

- IBS Third party and Material Outsourcer
- Material Outsourcer
- IBS Supplier
- Essential Supplier
- Non-essential Supplier

Mapping of Key Third-Party Providers

Where a firm relies on a third party for the delivery of an IBS, SYSC 15 A notes that the firm should have a sufficient understanding of the resources the third party utilises to support the provision of its service to and on behalf of the firm.

In carrying out the mapping of TPP, the information captured should cover the key regulatory headings: People, Processes, Technology, Facilities and Information as applicable.

While we note the current difficulty in capturing mapping information outside the organisation, we expect the more mature organisation will continue to develop. Potentially; more firms will be in position to demonstrate compliance with Para 5.5 of SS1/21 "The PRA expects firms to map the resources necessary to deliver important business services irrespective of whether the resources are being provided wholly or in part by a third party, which may be an intragroup or external service provider. Firms should understand how their outsourcing and third party dependencies support important business services".

The principles of proportionality should be applied as only IBS activities (processes and sub-processes that underpin the delivery of the service) need to be mapped.

Identifying fourth and n^{th} parties

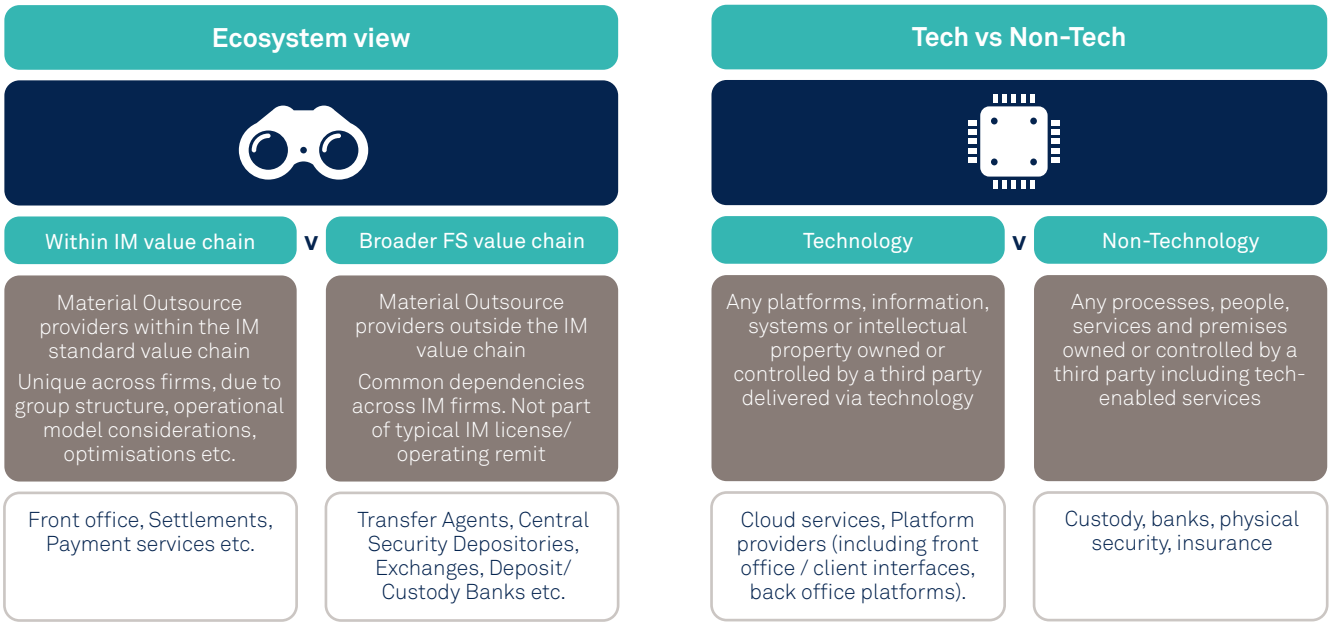
There is no consensus on the best methods to capture fourth-party information. It is likely that emerging privacy, resilience and global inventory expectations will increase the collection of fourth-party data.

While firms have begun asking questions about fourth parties, some firms rely on the third-party firm's Third Party Risk Management (TPRM) programme to gain confidence in fourth-party "material outsourcer" risks.

Firms will need to have visibility of the risks posed by fourth parties. The recent regulatory enforcement actions against TSB Bank Plc and its Senior Manager, Carlos Abarca, due to failings in their oversight of outsourcing arrangements relating to fourth parties further underline the need for firms to understand the material outsourcers of third parties for each IBS, as these pose an indirect, yet pertinent threat, to their Operational Resilience. Such efforts are usually challenging due to the absence of a direct contractual link and lack of transparency of the value chain. However, insights from such analysis would help firms refine the understanding of their concentration risks and implications for their resilience posture.

Categorisation of third parties

There are many ways firms can categorise TPPs, based on the services they purchase from such vendor. These categorisations prove useful in helping firms to be pragmatic, proportionate, and implement a coherent risk-based approach to the management of resilience dependencies on third parties. Some examples are noted below:



Regulated vs non-regulated third parties

Another lens for the categorisation of third parties is by firms understanding the regulatory regime that its TPP subscribe to. Whilst firms can expect that all third parties within the regulatory capture of PS 2/21 are also working to enhance their resilience and address vulnerabilities within the March 2025 regulatory deadline, this should not be assumed and an independent assessment of the third party must still be undertaken. It is also expected that firms which may be in the scope of the HM Treasury's Critical Third-party regime/ EU DORA are also likely to make progress in enhancing their resilience.

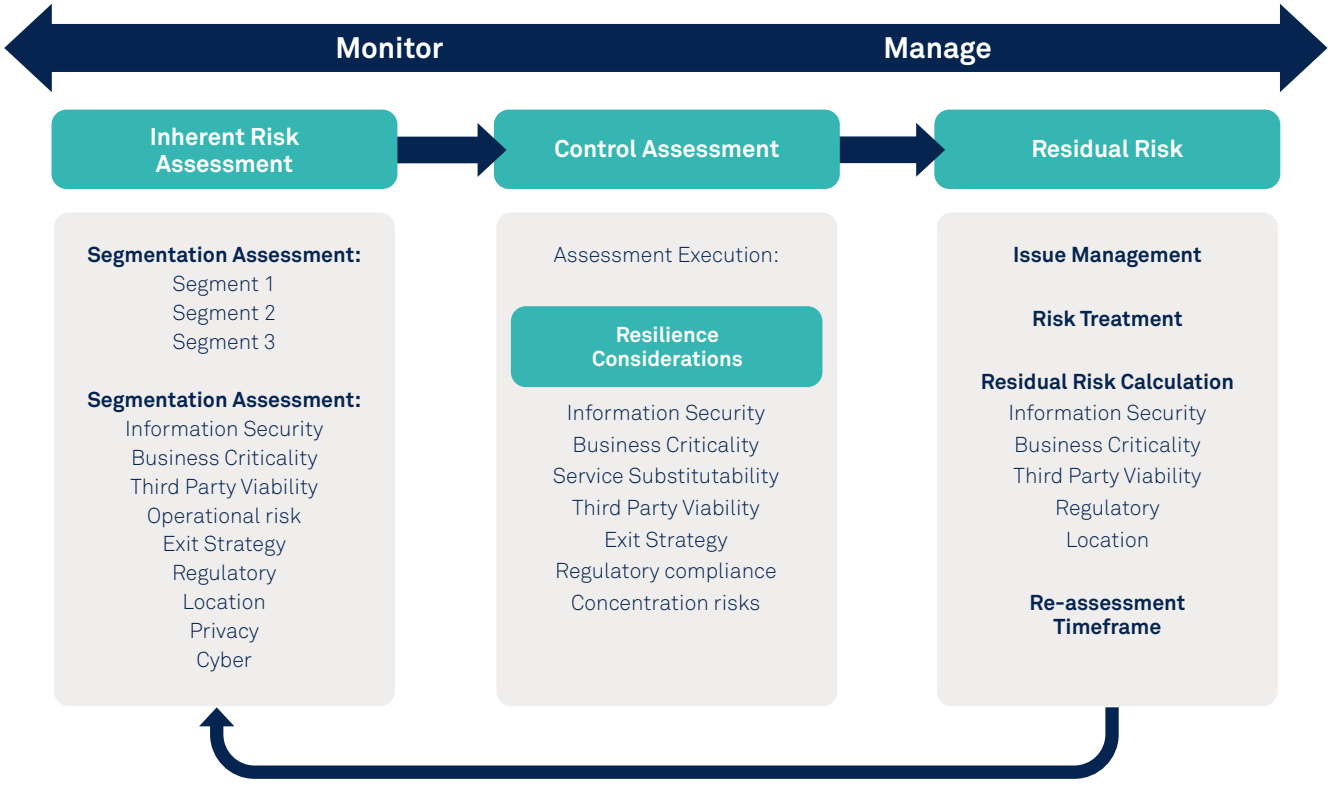
There is an opportunity for firms to leverage the general framework that financial institutions are working to comply with (per regulator regime) as a basis to understand and drive enhancements in the oversight and risk management of significant third-party relationships. This regulatory coverage lens should be considered as firms develop strategies to prioritise and engage critical third parties supporting IBS.

5.2 ASSESS

The methodological assessment of identified critical third parties which a firm relies on for the delivery of an important business service.

Incorporating Resilience into Third Party Provider's risk profile:

Firms should look to embed Operational Resilience considerations in their existing risk models, which allow for the qualitative and quantitative assessment of resilience risk. Hence risk models will enable an organisation to focus efforts on monitoring higher levels of inherent risk and manage higher levels of residual risk. Firms should also focus on modifying and enhancing their TPRM Programmes to augment them with Operational Resilience considerations.



As the organisation matures, it should move towards real-time management and monitoring of risks whilst leveraging on residual risk or control effectiveness ratings to determine the frequency of reviews as opposed to inherent risk and transactional events, for example, contracting and invoicing.

It is important that firms get an integrated view of third parties covering both risk and resilience across the TPP.

For 'material outsourcers,' SS 2/21 sets out the regulatory expectations for firms to have an understanding and clarity of the resilience, incident handling and crisis management procedures and capabilities of the TPP.

Firms should also examine and scrutinise the contingency plans of third parties and engage with third parties to articulate joint goals and outcomes.

Engaging with Third Party Providers – key considerations:

The engagement of TPP on Operational Resilience should emphasise desired outcomes and joint goals. Firms should consider the following when engaging with TPPs:

- The opportunity to drive changes through contract renewals, SLAs and other forums, particularly on KPIs and metrics.
- Prioritise an integrated review (and view) of third parties to reduce organisational effort and time committed by both the firm and third parties.
- Engagement should facilitate third-party assessment, monitoring and reporting with clarity and an appropriate level of detail to facilitate oversight and challenge.
- Roles, responsibilities and broader expectations (e.g. resilience, incident handling/ crisis management) should be well articulated and understood.
- Use Resilience SME engagement with third parties to emphasise key resilience messages, i.e. beyond compliance.

Engaging with Third Party Providers – Typical Methods:

Depending upon a firm's characterisation of its TPPs, some or all of the methods listed below can be used to engage effectively with third-party providers. Effective engagement enables firms to monitor and manage the risks associated with third parties and contracts.

- **Due Diligence Questionnaires:** TPRM questionnaires updated to gain required and desired resilience information in order to support the firm's understanding of how third parties provide the services required by important business services. See Appendix 1 for example due diligence questions on operational resilience.
- **Enhanced Due diligence:** Including follow-up questions, live meetings, and site visits as required to augment the firm's understanding of how a third party delivers service to the important business service and stated capabilities to remain within the defined impact tolerances.
- **Focused Audits:** Physical / virtual audits of the TPPs noted capabilities (should be integrated within TPRM audits to minimise compliance efforts). These may be performed on behalf of the firm (per contractual agreements). Resilience audits may prioritise mapping information and key resilience capabilities across incident management, critical workarounds, failover capabilities etc.
- **Joint Bi-lateral Resilience testing:** Joint resilience planning and testing to improve the firm's assurance of the TPP's capabilities to remain within the defined impact tolerance while improving crisis coordination, information sharing and other linked capabilities.
- **Multiple firm or cross-market testing:** A firm may wish to participate in a TPPs testing for multiple client firms.

Joint testing poses an important opportunity for firms to understand resilience practices and capabilities at third parties and is the subject of discussion later in this document.

Intra-group oversight

Critical inter-group arrangements should meet the same levels of Governance and risk management as external third parties. Firms should aim for sufficient insight into the capacity of the "group" service provider to support entity-level IBS to the same level as it would for external third parties.

Some practices firms should consider include:

1. Request and receive data mapping data on the delivery of services to support the firm's IBS to the extent it supports their understanding of how key services are delivered.

2. Utilise the firm's understanding of identified resilience vulnerabilities to influence "group" remediation prioritisation and investment plans.

3. Engage in leveraging relationships, aligned strategic objectives and regulatory messages to promote information sharing.

4. Leverage OCIR and Recovery and Resolution plans in exit planning considerations.

5. Leverage group approaches and group governance processes where appropriate to get assurance over controls applied across the group's operations in order to limit the amount of explicit oversight activity where duplicative.

Assurance Models

Firms should aim to carry out more resilience assessments and Scenario Testing, as assurance models are still immature. Current external assurance/ audits which can be leveraged include SOC 2 Reports, ISO 22301, 27000 Certifications and other linked standards. The Cross Markets Operational Resilience Group (CMORG) are currently working on future state industry-standard resilience external assurance models. Firms should not rely solely on external assurance reports; rather, these should remain as one data point in the firm's assessment of its critical TPPs.

Joint testing/ exercising will be key in enabling a firm to understand and gain assurance of how its key third parties can support its IBS and impact tolerance.

5.3 ANALYSE AND PRIORITISE

Resilience prioritisation, assessments, and risk mapping of third parties identified as critical for the delivery of an important business service.

A risk-based approach to the management of third parties impacting resilience enables firms to pay the most attention where the potential impact and likelihood of disruption is highest. At the analysis and prioritisation stage of managing key third-party providers, firms should consider the following examples:

- Risk-based approach to defining and selecting scenarios for testing.
- Internal Testing/ contingency testing (firm only).
- Testing the Business Continuity of third-party providers (TPP only).
- Joint Scenario Testing (firm and TPP).
- Exit testing.

It is recognised by members that more guidance needs to be provided around the definition of severe but plausible scenarios. The IA will aim to provide further guidance on this topic via a separate working group paper.

Risk-based approach to defining and selecting scenarios for testing

Firms should prioritise scenarios based on the likelihood of scenarios and the duration and impact of the scenario on the important business service. Firms can utilise resource mapping to understand the impact the scenario would have on each of their important business services' processes, critical resources and key points of failure.

Firms should sort scenarios by the total scenario priority, with high being the most prioritised scenario. Where multiple scenarios have the same scenario priority, additional focus drivers for testing should be analysed, e.g. Concentration risks, key dependencies, recent incidents, recent near misses, known vulnerabilities, and prevalent threats.

Total Scenario Priority				
Likelihood of scenario	High	High	High	High
	Medium	Medium	Medium	High
	Low	Low	Medium	High
		Low	Medium	High
	Duration and Impact on Important Business Service			

Some factors which can be considered for the scenario likelihood are:

- Threat scores/ ratings provided through a due diligence report
- Cyber assessment programme
- Mapping output/ single points of failure
- Low-scoring KPIs/ periodic reviews
- Operating events, disruption and near misses
- Concentration risks
- Multiple IBS affected
- Increased media coverage of incidents.
- Other emerging risk factors, e.g. sustainability

While multiple types of testing are mentioned in this document, they all rely on the high-level approach below. See the IA's previous guidance on scenario testing for further information.[16] The key steps are:

1. Test design and planning
2. Test execution
3. Analysis and remediation

Internal Testing/ contingency testing (Firm only Testing)

Internal Scenario tests aim to assess the firm's ability to remain within its impact tolerance for each of its IBS in the event of a severe but plausible disruption of its operations resulting from the failure of a third party.

Risk-based principles should be applied to determine the priority for testing scenarios and third parties.

The assumption should be that preventative controls have failed, and the third party has failed, and the onus is on how the firm detects and responds to the failure of the third party. Firms should identify workarounds which aim to provide services at minimum levels that prevent/ deter intolerable harm.

Scenario Tests should be conducted using confirmed/ historical data and capabilities rather than control designs and theoretical data.

In addition to top-down IBS focused testing, tests of the underlying business continuity plan workaround/ contingency tests for loss of third party augment the firm's understanding of their resilience in the event of a TPP outage.

Firms should consider the scale and volume of what workarounds are required to do, i.e. a workaround may work for a small test sample but not for millions of transactions. Firms must demonstrate and provide a rationale in their self-assessment or due diligence if it is implausible for a TPP to fail for a specific length of time.

[16] https://www.theia.org/sites/default/files/2021-12/IA%20Scenario%20Testing%20Severe%20but%20Plausible%20Dec21.pdf

Testing the business continuity of third-party providers (TPP-only testing)

Firms should seek assurance that their critical TPPs have performed resilience testing to ensure that they can provide services supporting IBS in the event of a severe but plausible scenario and test their ability to recover the business services before breaching the impact tolerance. As the mapping of TPPs increases in sophistication, there should be increasing assurance that TPPs can continue to deliver services supporting important business services (including consideration for other regulatory influences; e.g. DORA which may not be applicable to all firms).

It is the firm that is ultimately responsible for the quality and accuracy of any testing carried out by the firm or by a Third Party.

The firm should ensure the suitability of methodologies, scenarios and considerations adopted by the third party in carrying out testing. Some example scenarios are:

- Corruption, deletion or manipulation of critical data
- Unavailability of facilities or key people
- Unavailability of critical third-party services
- Loss or provision of the technology underpinning service delivery
- Disruption to other market participants where applicable

Following resilience testing, firms should look to understand the lessons learned and potential remediation plans. The TPP should look to make necessary improvements to address weaknesses identified to improve its resilience.

Joint Scenario testing (Firm and Third Party Provider Testing)

Joint Scenario Testing with TPPs is one approach to "increasing sophistication" firms can look to execute in testing the resilience capabilities of their important business services. Contracts with providers may by updated to encourage joint testing with TPPs; following due process between firm and TPP.

Firms should look to carry out joint resilience testing with KTTPs. For such exercises, the value would be derived by testing scenarios which are severe but plausible and relevant to the firm.

Action and remediation reporting after resilience exercises are critical. Actions and remediations must be managed across the remediation lifecycle, with vulnerabilities escalated to the appropriate level and changes being effectively communicated.

Routine testing of underlying business continuity plans (BCPs) for critical processes is essential to maintain resilience and improve the robustness of internal recovery plans in light of third party failures, i.e. resilience testing does not replace Business Continuity (BC) testing as both have different aims.

Example steps to carry out joint Scenario Testing are as follows:

1. Consider the unavailability of third parties across important business services.
2. Define an inventory of severe but plausible scenarios across important business services considering the following:
   a. Availability
   b. Integrity
   c. Confidentiality
3. Validate that scenarios can cause intolerable harm and how this would manifest at the point of disruption whilst ensuring they are severe but plausible.
4. Carry out joint Scenario Testing with TPPs, testing their recovery capabilities, communications and ability to deliver services during severe but plausible scenarios.
5. Prioritise scenarios by analysing the following:
   a. Concentration and the impact of the scenario on the important business services and across horizontal business services;
   b. Testing capabilities and lead time;
   c. Previous testing completed;
   d. Likelihood of the scenarios occurring; and
   e. Areas of concern/ relative risk.

Multiple firm or cross-market testing

A firm may wish to participate in a TPPs testing for multiple client firms which present an opportunity to learn about the resilience capabilities / operations of KTTPs. One example of such efforts in the market is by Euroclear UK and International which has held a market wide exercise to ensure that market participants know what to do in the event of a CREST system outage.

We recognise the benefit of such exercises to the market and also recognise the amount of co-ordination effort and expertise in executing such multilateral tests.

Exit Testing

Firms may carry out both stressed exit testing (following the failure or insolvency of the service provider) and planned exit testing.

The resilience testing of exit plans allows firms to understand how they can work with third parties, particularly if contingencies need to be utilised.

Whilst stressed exits are a product of unforeseen emergencies, which may render it difficult to remain within impact tolerance, the value of Scenario Testing stressed exits stems from providing firms with an opportunity to understand where vulnerabilities may arise from, what the extent of the threat is; where you can and cannot transfer services in-house; and examples of where adopting a "do-nothing" approach, whereby firms wait for the TPP to recover their services, may render a better outcome than immediately deploying contingencies. SS 1/21 Para 6.12 notes that such test which firms anticipate exceeding their impact tolerance "provide useful information to firms' management and to their supervisors. Boards and senior management will need to judge whether failing to remain within the impact tolerance in specific scenarios is acceptable and be able to explain their reasoning to supervisors"

The scope of testing can include:

1. A full exit
2. A regional exit
3. Service-specific exits of material outsourcers that support IBS

Possible reasons, planning methods and testing methods for each type include the following:

	Stressed Exit	Planned Exit
Possible reason for exit	• Disruption • An outage or failure • Insolvency or liquidation of the third party	• Expiration or satisfaction of contract • Increased risk exposure/ issues • Costs exceed the return on investment • Decision to move service capability "in-house." • Breach of contract
Planning	• Emphasise operational transitions and how workflows can be transitioned • A key objective of stressed exit plans is to provide risk mitigation in the event of a disruption which cannot be managed • Firms must assign clear roles and responsibilities to develop and execute these plans	• Firms should have a plan in place for planned exits, including: – Determining the firm's exposure caused by the exit – Receiving legal confirmation of data destruction – Confirm the repossession of data/ equipment provided to the third party – Implementing previously defined transition plans, including steps for short and long-term transition
Testing	• Firms can use scenario testing as an opportunity to improve the firm's understanding of their third parties and the limitations of contingency planning	• Planned exit testing can be used as an opportunity to review the feasibility and utility of the exit plan.

Cloud Testing

Regulators express clear concerns related to exit planning for cloud-service providers due to the following reasons:

- Threat-testing capabilities are still relatively low across the industry.
- It typically takes 12 months or more for a contractual agreement to be reached.
- The integration of new providers requires colleagues with substantial skills and resources, something which is not always available in abundance.
- There is an optimism bias associated with cloud-service providers, as opposed to non-cloud providers, which may potentially be misplaced unless firms take due diligence when testing the resilience of this service in the first place.

To counteract these risks, the resilience testing of critical third and fourth parties may extend to cloud-service providers to understand the limitations and potential vulnerabilities inherent in how we use, consume, or buy cloud services. We recognise other resilience regulations which may have implications for cloud testing are being established.

Key Testing considerations

Below are key considerations for firms to keep top of mind as they evaluate and enhance their testing capabilities in pursuit of enhanced resilience:

1. Operational Resilience is not a journey that will be finalised overnight, nor is it a consideration solely for resilience colleagues; instead, it is a constant evolutionary process that is fundamental across all aspects of an organisation.
2. In order to undertake effective joint testing, firms must engage TPPs early on and, where possible, prior to contractual arrangements being agreed upon.
3. When testing is undertaken, TPPs ideally need to be involved.
4. Firms should try to leverage their relationships with TPPs, so as to effectively build relationships with and assess the resiliency of nth party providers.
5. Resilience testing should include cloud-service providers. Firms cannot assume resilience in the cloud.
6. Exit testing should be used to reveal strategies that will allow firms to operate beyond merely meeting their impact tolerance.
7. Firms should focus their attention on material outsources and IBSs.
8. Firms should adopt a proportional and risk-based approach towards resilience testing.

5.4 CONTROL

Firms should have in place resilience controls over third parties, which aim to provide reasonable assurance that the third parties the firm relies on are able to remain resilient to the extent that intolerable harm will not occur to the firm's clients, end consumers, the broader market or the firm itself. These controls fall into three categories:

1. Preventative controls
Preventative controls are an attempt to prevent or deter undesirable acts from occurring at the TPP. They are proactive controls designed to prevent a loss, error or omission. For example:

a) Due diligence questionnaires

b) Enhanced due diligence

c) Focused audits

d) Contractual agreements

e) Governance

f) Access Controls

2. Detective controls
Detective controls attempt to detect undesirable acts that have occurred at the TPP. They provide evidence after-the-fact that a loss or error has occurred but do not prevent them from occurring. For example:

a) Management Information and Reporting

b) Financial Statements

c) Audits

d) Supplier Review Committees

e) Reconciliations

f) Intelligence Services

g) Intrusion detection systems

3. Remediation controls
Remediation controls are designed to correct and respond to errors and undesirable acts that have been detected at the TPP as well as minimising the risk of future occurrence. For example:

a) Response/ Remediation Plans

b) Contractual Agreements

c) Implementation of new policies

d) Training programmes

e) Exit plans

Response/Remediation of TPP resilience opportunities for Improvement

Risk response is a cyclical process. As circumstances are constantly changing, continuous monitoring and review of the framework ensure a continual improvement of the framework (Assess, Evaluate, Manage, Measure). These are typically:

Risk response options are not necessarily mutually exclusive or appropriate in all circumstances.

Controlling through Contracts

Firms should update their contracts to consider key regulatory considerations regarding Operational Resilience and outsourcing arrangements. Contracts should be updated to include the following:

- Audit rights
- Compliance
- Business continuity/ disaster recovery
- Subcontracting and oversight of fourth parties
- Termination rights
- Exit requirements (including exit plan)
- IT security/ data protection requirements
- Remediation
- Governance
- SLAs/ reporting /MI
- Regulatory disclosures depending on service (e.g. best execution/client categorisation etc.)

(Please note that this is non-exhaustive, and the agreement terms will depend on (i) the rules that apply to the firm; (ii) market practice; (iii) the services being provided; and (iv) the specific requirements that the firm wants to impose (e.g. as a result of its due diligence on the TPP)).

Contracts should also be updated in the context of the applicable regulation, e.g. the FCA and PRA Operational Resilience rules, PRA SS2/21 Outsourcing and Third Party Risk Management, SYSC 8.1 General outsourcing requirements, EBA Outsourcing guidelines, HM Treasury Critical Third-Party Regime.

Service Substitution

Service substitution is the approach to switching/ changing service in entirety/ in part to achieve specific (e.g. resilience, profitability) outcomes. Service substitution may arise due to some of the following reasons:

1. The TPP stops support for a key service
2. The TPP stops providing the service in a specified country/area
3. Legacy software is no longer compatible with modern hardware

If a third party provider opts to discontinue the provision of a service, firms must have contingency arrangements in place to continue the delivery of the IBS. Some key service substitution considerations are below. These can enable a transition to a new TPP.

- Firms must have up-to-date mapping information in order to fully articulate the impact of the service substitution on the firm's IBSs.
- Firms must have updated Management Information on third-party-provided services so they can effectively implement a transition plan when necessary.
- Firms should have contractual agreements ensuring that support for hardware/ software is provided for the duration of the contract.
- Firms should have a regularly reviewed transition plan to ensure the service substitution has minimal impact on service delivery and clients.

Exit Plans

Exit planning and strategies are necessary to identify possible risks, define potential losses and ensure business service continuity. An exit plan details how to prepare to exit a supplier if required. This may arise due to a number of scenarios. An exit plan should enable the firm to continue providing its important business services and avoid causing harm to clients in the event of a loss of the ability to use a TPP.

Exit strategies should be considered when developing a firm's business service and engaging in contracts with TPP. The exit of a TPP and the execution of the associated exit plan can be planned or unplanned. Possible reasons for an exit are:

- Exit at the end of the agreed contract term.
- Exit during the contract by either party (for convenience or breach of contract).
- Exit due to failure of the TPP.
- Exit due to deterioration of the quality of the service provided or failed provision.
- Exit due to material risks arising from the continuous operation of the service.

For an exit plan to be executable and effective, exit plans should contain:

- The mitigating action to be performed and responsibility for the completion.
- Timeframes within which the actions should be completed.
- Triggers for the implementation of the exit plan.
- Scenarios covered by the plan.
- Service substitutability.
- Roles and responsibilities of the Firm and the TPP. Pre, Intra and Post-Exit.
- Arrangements for maintaining service continuity during the exit.
- Documentation to be transferred.
- Management Information and reporting required.
- Payment arrangements.
- Identification and agreement of exit costs and liability.
- Actions and timescales related to Data, IT Infrastructure, systems, assets, facilities, people & knowledge, sub-contractors and others.

Firms can carry out joint Scenario Testing with TPPs to improve the practicability of exit plans and ensure runbooks are executable and usable.

Recovery and resolution planning within the firm

Firms should minimise the impact of the exit of a critical TPP and ensure that the firm can continue carrying out operations and delivering business services despite the loss of a TPP. When doing this, firms should consider applicable regulations, including:

- The FCA has proposed that as part of the Internal capital adequacy and risk assessment (ICARA) process, firms should identify appropriate recovery actions.
- The firm's recovery planning should be linked with its business model and explain how it would recover from a stressed scenario and prepare processes appropriately.
- The PRA expects firms to undertake recovery planning. Firms should have a number of recovery options and maintain and test their plans regularly.

Below are key recovery and resolution plan considerations which a firm should consider when making and developing its plans:

- Business Impact Analysis
  - Process mapping will enable firms to understand and address important business service impacts caused by an outage. Mapping information should be consistent across organisational use cases.

- Quantitative and Qualitative triggers
  - Firms should have a mix of quantitative and qualitative triggers in their recovery plans. These should consider Operational Resilience implications.

- Scenario Testing
  - Firms should test recovery and resolution plans against multiple stress scenarios to evaluate the effectiveness of the plans. Such scenarios can be leveraged in resilience testing.

- Governance
  - Firms should have a regularly reviewed recovery and resolution plan within established Governance. Opportunities to integrate resilience and recovery frameworks should be leveraged.

- IBS Considerations
  - Firms should consider IBS and consider the compatibility of recovery plans with resilience objectives.

Wind down planning in the event of Third Party Providers

Firms must prepare for the scenario that critical TPP have access to limited resources and need to wind down their business. Firms must be able to continue providing their business services despite the winding down of TPPs.

TPPs may lead to a business winding down due to:

- Loss of key clients.
- Severe economic downturn.
- Strategic exit from a market.
- A firm experiences insolvency.

A firm should consider these key considerations when wind-down planning:

- Identifying a stress
  - Firms must have accurate MI from TPPs to identify and monitor stress which may cause the TPP to wind down.
- Devising a strategy
  - Firms must carry out their exit plan strategy in order to ensure there is minimum disruption caused to the delivery of IBSs.
- Communication
  - Firms must have adequate exit plans, preparatory measures and a communications plan to minimise the disruption.
- Assessment of resources
  - Firms should carry out an assessment of the resources, financial and non-financial, that are needed to support/ transition to maintain resilience in the event of a TPP winding down.
- Regulatory ring-fence capital
  - Firms should consider the regulatory regime of third parties and assess whether such TPP would have cash reserved for orderly wind-down or a potentially accelerated exit.
- Exit testing
  - Firms must regularly test exit plans against a range of severe but plausible disruptive events, e.g. the winding down of critical TPPs.

5.5 MONITOR

PROVIDING OVERSIGHT REGARDING THE ACHIEVEMENT OF OBJECTIVES AND RESILIENCE OF THIRD PARTY PROVIDERS

Metrics and Monitoring – Resilience of Third Party Providers

Operational Resilience monitoring helps you articulate your overall resilience position and should incorporate perspectives of the ability of key TPP to support the firm's resilience requirements. This would inform the Board, Management and other resilience governance forums and drive answers to the holistic POV on the TPP resilience.

Operational Resilience monitoring should:

- Highlight areas of weakness
  - Including early warning of potential impact tolerance breaches. Supports impact assessment of incidents through an understanding of TPP resources required to support important business services and process flows.
- Drive investment decisions
  - Allow Senior Executives to prioritise key decisions and focus on vulnerabilities and TPP dependencies, the potential impact of issues and potential risk reduction implications to drive investment decisions.
- Prove the firm's resilience
  - Meet resilience reporting needs of the Board, Management and other stakeholders by enabling a data-driven ongoing view of the TPP's Operational Resilience.

Resilience Metrics and Monitoring should provide:

1. A real-time resilience snapshot answering the question, 'is the TPP resilient now?'
2. Resilience Governance Reports answering the question 'How resilient was the TPP in the last period?'
3. Programme Metrics answering the question 'What needs to be done by the TPP to be resilient in the future?'

Resilience tooling may be leveraged to help firms embed monitoring of critical third parties with less manual input needed, helping firms embed resilience monitoring into business-as-usual operations.

Governance

Firms must have governance structures in place to enable resilience risks regarding third parties to be escalated and to enable the prioritisation of investment decisions. Third-party Governance and oversight should be integrated within a firm's existing Governance structures.

Some key considerations of the Board should be:

- Understanding the Governance of resilience and how the company leverages TPPs.
- Considering the impact of third parties as it relates to enterprise risk and resilience.
- For governance and monitoring to be reflected in the contracts.
- To assemble and maintain operational manuals to manage exits/ disruptions.
- To establish routine reporting and testing to provide assurance.
- To assess that the Board has the requisite management information to supervise the TPPs.

Oversight of resilience of Intra-Group Third Party Providers

Together with the specific requirements of PS 2/22 on TPRM; on the subject of understanding and demonstrating oversight of an intragroup third party, firms should:

- Apply the same rigour when conducting intragroup assessments as for third party assessments.
- Consider the extent to which the firm is able to exert influence on the group/or parent entity providing the service.
- Consider the prioritisation of any remediation of outsourced services where outages may impact the firm.
- Ensure that the resolution of any potential conflicts of interest is provided for in the governance arrangements.
- Assess if policies and procedures applied at group level are fit for purpose at the local entity.
- Consider local and linked regulations on resilience and TPRM.

5.6 REPORT

Reporting on the achievement of objectives and resilience status of third party providers

Dashboarding and MI reporting support the firm in collecting and collating data required to monitor and report on the resilience of TPP and IBS's ability to continue operating during severe but plausible disruptions and remain within their impact tolerance, highlighting areas of Operational Resilience weakness that require attention for remediation with potential escalation, and further investments to be planned.

Operational Resilience metrics should:

- Be specific, predictive, and easy to quantify through verified numbers, percentages, or ratios.
- Have relevant thresholds and trigger points*.
- Provide actionable information to the right stakeholders at the right time.
- Be outcome-focused and provide insight on resilience trends.
- Allow Senior Executives to prioritise key decisions and focus on key. vulnerabilities, issues, and investment decisions.

** Thresholds and trigger points are business specific and must be agreed by the relevant groups, for example, Technology, Business and 2LoD*

Bottom-Up vs top down: The firm's approach to defining and reporting metrics may take a bottom-up/ top-down approach. Both methods have merit and can be helpful depending on the organisational context. While building out reporting metrics, it is critical that the outcomes must be consistently measurable, actionable and meaningful to end users.

Third party providers resilience gaps in the self-assessment

The Operational Resilience self-assessment document is an opportunity to articulate the firm's understanding of resilience vulnerabilities identified (including those originating from the use of TPPs), and the firm's plan to remediate vulnerabilities ensuring resilient IBSs.

All effort channelled towards understanding third party resilience gaps:

- Once vulnerabilities regarding TPPs have been identified, it is crucial to build a remediation approach to address vulnerabilities.
- The creation of a remediation programme will require some investment and an appropriate governance structure and coordination with the TPP.
- The remediation programme can serve as evidence of remediation of vulnerabilities which is key in the resilience self-assessment.

6. NEXT STEPS – POLICY DEVELOPMENTS / AREAS FOR FUTURE PROGRESS

This section explores future developments and trends in the operational resilience area, including new regulations, innovations, and collective initiatives.

Readers are cautioned that there are unlikely to be any 'silver bullet' solutions that emerge in this space to resolve all of the challenges identified in Section 4: Key challenges. However, incoming regulations, potential developments in assurance and collective industry initiatives may cumulatively, and over time, assuage the difficulties firms currently face.

6.1 SUMMARY OF UK PROPOSALS ON CRITICAL THIRD PARTIES

In July 2022, the FCA, Bank of England and PRA published a Discussion Paper regarding Critical Third Parties (CTPs) to the finance sector. The DP contained proposals that are intended to manage the systemic risks presented by large technology providers to the BoE, PRA and FCA's objectives of UK financial stability, market integrity and consumer projection. The proposals are likely to capture major cloud service providers and other technology providers.

The proposals will complement the regulators' UK Operational Resilience Rules. They are motivated by HMT's assessment[17] that the regulators' current powers are not sufficient to tackle the systemic risk that disruption at a third party providing key services to multiple firms could cause.

Many financial services firms and FMIs rely on a small number of third party providers in order to deliver their services. Some of these third parties reside outside of the regulatory perimeter, limiting the regulators' ability to monitor and manage the risks their disruption or failure would present to the regulators' objectives.

Under the existing UK Operational Resilience Rules, firms relying on third parties to support the delivery of their important business services (IBS) play a role in monitoring and managing the risks presented by those third parties. However, the authorities' discussion paper recognises that no single firm can adequately monitor or manage the systemic risks that certain third parties pose to the regulators' objectives, hence additional policy measures are now being pursued.

Firms will remain accountable for managing the risks to their own operational resilience presented by critical third parties, however, the proposed regime is intended to fill a gap in the regulators' powers by allowing them to directly oversee services that CTPs provide to firms.

At a high level, the proposed measures include:

- A framework for designating certain third parties as critical third parties (CTPs)
- Minimum resilience standards for CTPs in respect of material services they provide to FS firms
- Resilience testing of material services that CTPs provide to firms
- Provision of information by CTPs to the regulators to assess the resilience of material services
- New statutory powers for the regulators to exercise over CTPs
- The regulators will not oversee CTPs in their entirety, only their material services to the FS sector

The regulators' initial thinking for the minimum resilience standards involves:

- Identification of material services provided to FS firms.
- Mapping of resources required for delivering its material services: people, processes.technology, facilities and information.
- Risk management controls.
- Testing and sector-wide exercises.
- Disclosures to regulators on threats and incidents.
- Develop and potentially test financial sector continuity playbook.
- Develop post-incident communication plans to engage with firms and regulators.
- Regularly share lessons learned with firms and regulators.

[17] 2022-06-08_critical_third_parties_policy_statement.pdf (publishing.service.gov.uk)

How the proposed measures might interact with the existing operational resilience policy for firms

Currently unregulated third parties who are designated as CTPs will become subject to minimum resilience standards and regulatory supervision. Firms will take a degree of comfort from these facts despite the risk remaining with the client firms and senior management.

The regulators also assume the measures could strengthen firms' ability (both individually and collectively) to oversee and obtain assurance from CTPs. However, the measures as drafted in the DP are not always specific with respect to how this will come about.

Standards	What CTPs are expected to do /disclose to the regulators	Potential implications for customer firms
Identification and mapping	CTPs will be expected to identify material services to firms and map the resources required for delivering them, including key nth parties	This will likely require engagement with firms. The various parties in the supply chain will start to speak a common language on resilience.
Testing	CTPs will be expected to regularly test the resilience of its material services by • Participating in tests and sector wide exercises convened by the regulators • Performing its own tests • Potentially, testing severe but plausible scenarios in collaboration with firms and industry groups	Regulators will develop ways to share test results with firms that rely on the CTP for material services or are planning to do so in the future.
Engagement with regulators	The CTP proactively and promptly discloses to the supervisory authorities any information of which they would reasonably expect notice. In particular, information relating to incidents or threats that could have a systemic impact on the supervisory authorities' objectives.	In theory, the regulators will step in to manage systemic risks presented by CTPs, which will indirectly benefit the firms that use them. More clarity is needed on how firms will be availed of relevant information arising from this interaction.
Financial sector continuity playbook	The CTP has developed and, to the extent appropriate, tested specific measures to address potential systemic risks to the supervisory authorities' objectives that could arise from its failure, or a severe but plausible disruption to its material services to firms. The CTP has documented these measures in a 'Financial sector continuity playbook', which it regularly updates and submits to the supervisory authorities.	Continuity playbooks cannot be wholly relied on by firms, but they are helpful to have in place in the event of a CTP failing for financial reasons. The DP envisions cooperation between CTPs and firms, industry bodies, etc, to agree continuity playbooks and if necessary, to test them.
Post-incident communication	Develop tailored communication plan to engage with firms, regulators and other relevant stakeholders in the event of its failure or severe disruption to material services. May include appropriate info about measures to recover material services, and estimated timeframe for doing so	CTPs could be required to coordinate with relevant stakeholders in developing plans. Timeframes to recover material services would be helpful to compare against impact tolerances.
Lessons learned	CTPs regularly share lessons learned (from incidents, tests, etc) with regulators and firms	Firms would receive details of lessons learned.
Cyber resilience testing	Cyber resilience testing of certain CTPs, potentially via a requirement for relevant CTPs to actively support the cyber resilience testing of firms, i.e. CBEST or STARFS	Potentially firms will receive support from certain CTPs on their cyber resilience testing.

Next steps

The DP closed for feedback on 23 December 2022. After having considered responses to the DP, the regulators plan to consult on their proposed requirements and expectations for CTPs in H2 2023[18].

6.2 ASSURANCE AND DUE DILIGENCE

Further to Section 5.2: Assess, **shared assurance models** could potentially lead to efficiencies for both customer firms and TPPs. Shared assurance models involve an independent provider conducting shared due diligence assessments on TPPs on behalf of the vendor's clients. In this way the TPP only needs to answer one set of questions, one time, and the findings are disseminated to all. This is an efficient approach but it's efficacy may be limited in that the resulting disclosures can be too generic to fully satisfy the requirements of individual firms.

Centralised due diligence portals are another way to streamline the process of transmitting relevant information between TPPs and customer firms. Such portals allow TPPs to upload information relating to resilience matters in a secure manner that can then be accessed by customer firms. Potential drawbacks of centralised due diligence portals include that the information provided may not always satisfy the requirements of individual firms, requiring bilateral engagement to plug any gaps. Firms may also find themselves having to navigate multiple portals across their TPPs, as well as needing to reformat data for their own systems, which could detract from any efficiency benefits.

Self-assessments and/ or **self-attestations** by third parties over their own resilience can be helpful, but will be of limited value unless they are accompanied by suitable evidence that can be reviewed by customer firms. A risk inherent to self-assessments is that they may not provide the level of robust challenge that firms expect.

In a similar vein to shared assurance models, **external assurance reports**, such as SOC 2 audits, can be valuable sources of assurance over TPPs and represent a more efficient method than duplicative firm-by-firm engagement.

[18] Regulatory Initiatives Grid - February 2023 (fca.org.uk)

SOC 2 audits are assessments carried out by an independent party on a TPP's control environment. The resulting report can be made available by the TPP to their clients. A key benefit of external assurance is the increased level of confidence conferred by the independent nature of the findings.

External assurance reports have their limitations too. Firms must translate the findings of the report into what they mean for their own operational resilience. There may also be misalignment between the firms IBSs, and the IBSs of the TPP, adding further complication. There is also significant cost associated with performing the reports, which may indirectly be passed down to clients, and ultimately to consumers.

Firms should not rely solely on external assurance reports; rather, these should remain as one data point in the firm's assessment of its critical TPPs.

Notwithstanding their limitations, external assurance reports could represent an opportunity area for future innovation in the operational resilience space. SOC 2 audits could potentially serve as a starting point for new versions of assurance reports to emerge that are more tailored to the needs of compliance with operational resilience rules and scenario testing. The Cross Markets Operational Resilience Group (CMORG) are currently working on future state industry-standard resilience external assurance models.

6.3 MULTILATERAL SCENARIO TESTING

Industry forums may be well placed to organise and convene multilateral scenario tests between TPPs and several firms at one time.

Similarly, regulators and industry forums may also be in a good position to facilitate the co-designing of industry-wide scenarios, which may involve disruption of common TPPs, that firms can use to independently, or cooperatively, test the resilience of their IBSs. Relevant TPPs could be invited to contribute to the design of such scenarios, or participate in the tests themselves, to improve the accuracy of the test's assumptions and make them more realistic.

Transfer Agents, specifically, may also be keen to work with their client base to agree an appropriate scenario, perform a test and then share the output with all clients, rather than potentially test several different scenarios bilaterally with different clients.

7. CONCLUSION

Third party oversight is a considerable challenge for firms. It has revealed itself to be perhaps the most difficult aspect of the new UK Operational Resilience Rules for firms to get to grips with. And significant concern remains over firms' ability to gain assurance over their TPPs' resilience in the level of detail expected by regulators. It may take time for the space to mature to the point where firms are able to consistently form adequate assessments.

The trend towards greater outsourcing and third party service provision within the industry highlights the importance of driving improvements in this area. Similarly, technological advances and the growing importance of technology providers from outside of the financial world is creating new systemic risks that firms and supervisory authorities have to manage.

Incoming regulations around critical third parties are a welcome step in the right direction, however, there are unfortunately no 'silver bullets' that will solve all challenges. Incremental progress across the areas of regulation, assurance, collective initiatives and through numerous bilateral engagements, including testing, between firms and their TPPs, will be required going forward.

This guide attempts to contribute to the situation by providing firms in the investment management sector with an overview of the relevant issues and a practical framework with which to guide their interactions with third parties.

We would like to thank the firms and individual representatives who contributed to the Working Group, as well as Macfarlanes and EY for their invaluable assistance.

If you would like to speak further about any aspect of this document, please feel free to get in touch with the IA.

APPENDIX 1

EXAMPLE DUE DILIGENCE QUESTIONS

Firms will already have existing business continuity / business recovery due diligence questionnaires (DDQs) and may wish to supplement them with an additional question set on operational resilience. Alternatively, firms may decide to structure their DDQs in accordance with the pillars of operational resilience, e.g. impact tolerances, mapping, and so on.

Firms should aim to set themselves up for success with the questions that they pose. For each question, it is worth reflecting on how likely it is that the information requested will actually be provided by the TPP. In addition, allowing for a degree of flexibility in how the TTP can respond to the question may yield better results that rigid questions that may elicit non-responses.

Example questions explicit to the Operational Resilience Rules:

- If applicable, what progress have you made on the implementation of your Operational Resilience Programme in relation to the Financial Conduct Authority (FCA)'s, and the Prudential Regulation Authority (PRA)'s Policy Statements?
- Please provide details of the important business services that you have identified and the impact tolerances that have been set for each important business service.
- Does your firm have an operational resilience program in place designed to respond to clients' queries in respect of the Operational Resilience Rules?
- In relation to the Operational Resilience Rules – does your firm have resilience assurance statements, which reflect the principles of the Operational Resilience Rules? If so, please provide them.
- Are there any vulnerabilities in your service (including parties on whom you rely) that could threaten our ability to deliver our X IBS within the impact tolerance of X time duration? If so, please provide details.
- Please provide us with summary details of your firm's most critical assets broken down into groups covering each of the 6 Mapping Items (Critical People, Processes, Technology, Facilities, Information, and Third Parties) – which your firm relies on to provide us with a service.
- We have identified you as a key third party dependency within our important business services. We would like to discuss the impact tolerances we have set for our important business services with you to ensure alignment.

Example questions in relation to 4th parties:

- Do you outsource any critical activities to your own third parties (which are, notionally, 4th parties from our perspective)? I.e.: the ones where you would not be able to provide us with the service if it were to fail.
- For each of the 4th Parties detailed, what plans are in place to ensure continued service to us if they failed or were disabled for significant period of time? How often are the plans reviewed and what level of testing is performed of these plans to ensure that they are feasible and robust?
- Please detail how you are ensuring alignment with any third parties (i.e. 4th Parties from our perspective) who deliver all or part of any important business service on your behalf.

Example questions in relation to testing:

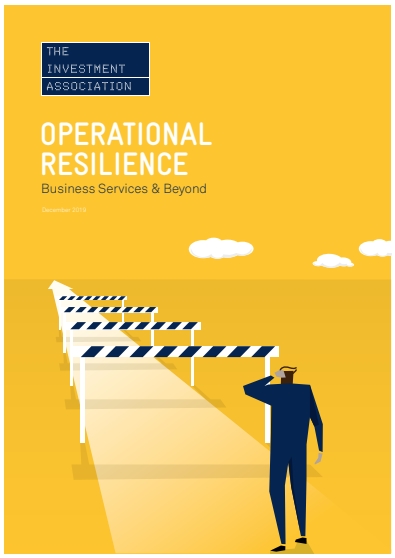
- Does your firm hold results of any testing relevant to the resilience of the service you provide to us? If so, please provide a summary of the testing results.
- Would you be willing to participate in and support our resilience testing and exercising programme in relation to the services you offer to us?

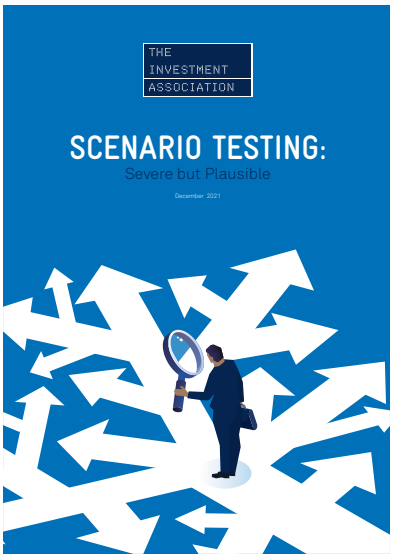
Other example resilience questions:

- Are you currently directly authorised by the FCA or any other relevant body? If yes, what permissions do you currently have?
- Are you registered (certified) to any recognised resilience standard for the services and works you are offering to us? If so, please provide your certification number.
- How do your change management and project management policies and procedures mitigate the risks that changes inadvertently affect the service provided to us?
- Have you identified any key person dependencies to deliver your business services?
- What is the level of operational vulnerability to the physical risks from climate change?
- Have there been any climate-related events in the last 5 to 10 years that have led to prolonged (> 3 days) outages or loss of access to your firm's sites?
- In the last five years has your company had any regulatory inquiries/investigations related to the resilience of any service you provide? If so, please provide details.
- Are there any outstanding material audit findings against your resilience programme. If so, please provide details of your action plan to closure.
- Where does specific accountability for resilience sit within your organisation? (Board, Senior Management etc.)
- Do you have dedicated staff assigned to managing resilience with clearly defined and documented roles and responsibilities?

APPENDIX 2

OTHER IA OPERATIONAL RESILIENCE GUIDANCE





THE
INVESTMENT
ASSOCIATION

The Investment Association
Camomile Court, 23 Camomile Street, London, EC3A 7LL

www.theia.org
@InvAssoc

July 2023