TheCityUK

Recommendations for the implementation of third-party operational resilience

Introduction

Operational resilience is the ability of a firm - or the financial sector as a whole - to prepare for, adapt to and overcome disruption while continuing to deliver core services. This in turn protects the safety and security of customers and provides confidence in the market. The increasing use of technology across the financial and related professional services (FRPS) and associated growing cyber security risks make strong operational resilience capabilities more crucial than ever before.

The operational resilience policy regulations from the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) have been in place since March 2022. The end of the transitional period is 31 March 2025. By this deadline, firms must have:

- Performed mapping and testing to ensure they can remain within impact tolerances for each important business service.
- Made the necessary investments to enable them to operate consistently within those impact tolerances.

Building operational resilience advances organisations from a narrow focus on risk, controls, governance, and reporting to a longer-term strategic view of the total environment, in which operational resilience becomes a competitive advantage in times of disruption. However, there are several challenges that firms face in implementing these requirements, in particular with regard to managing third-party risk. As financial firms increasingly rely on third-party services to support their operations, any disruption in these may have far reaching consequences for the stability of the entire financial ecosystem.

This paper identifies a number of considerations for both firms and regulators **to ensure that implementation of these requirements not only minimises the impact of disruption, but also supports innovation and growth**. This will be paramount to the long-term competitiveness of the UK as a financial centre.

Definitions

In the context of this paper, the following definitions apply:[1]

- 'Firms' includes all firms authorised by the PRA and/or the FCA (both on a dual-regulated and FCA solo regulated basis). The definition includes UK authorised branches of third-country firms.
- A 'third-party' is 'a person who provides services to one or more firms or FMIs'.

[1] Taken from 'DP3/22 – Operational resilience: Critical third parties to the UK financial sector', PRA, available at: DP3/22 – Operational resilience: Critical third parties to the UK financial sector | Bank of England

- A 'critical third-party' (CTP) is a third-party that HM Treasury (HMT) would designate as 'critical' using its proposed powers under the Financial Services and Markets Act (FSMA) 2023. Under FSMA 2023, HMT will be able to designate a third-party as 'critical' if it is satisfied that a failure in, or disruption to, the provision of the services that it provides to firms and financial market infrastructures (FMIs) - either individually or where more than one service is provided, taken together - could threaten the stability of, or confidence in, the financial system of the UK.

Challenges facing the implementation of third-party operational resilience requirements

Third-party risk

FSMA 2023 establishes a new suite of powers for regulators to directly regulate CTP service suppliers. However, regulation of CTPs does not replace any requirement for a firm's own assurance over the resilience of its providers**.** Even where a service provider is authorised and regulated (as would be the case with CTPs designated under the new rules), this does not reduce the level of attention to be paid to them where a failure of, or disruption to, the service provided could lead to a failure of or disruption to an important function. Nevertheless, bringing CTPs under shared regulatory oversight will hopefully support firms' own assurance processes, given the alignment of terminology and approach.

One of the significant challenges faced by financial firms in the pursuit of assurance is the lack of transparency and information sharing from certain third-party providers, particularly those that are global players - in particular global custodians, web service (including cloud) providers, Big Tech firms and market data providers. This lack of transparency can range from, at best, minimal information provided - such as excerpts from a manual – to, at worst, no information at all.

Assurance in the context of CTPs refers to the confidence that financial firms have in the ability of their CTP providers to deliver services without causing a failure or disruption to important business functions.

There is also concern about the increasing burden of due diligence, where industry parties are often enquiring as to each other's resilience, at huge cost in terms of time and resources.

International Alignment and Competitiveness

There are a growing number of operational resilience regulations worldwide. In 2021, The Basel Committee on Banking Supervision (BCBS) published global principles for operational resilience which signalled greater regulatory scrutiny around firms' resilience globally and the risk of divergence in the requirements this scrutiny will set. In January 2023, the European Digital Operational Resilience Act (DORA) entered into force, establishing

technical standards that financial entities and their critical third-party technology service providers must implement by 2025[2] to ensure that Europe is able to stay resilient in the event of a severe operational disruption.

These regulations share common themes of identifying what is important, putting tolerances around that, and comprehensively testing the recovery capability. However, there are always differences and nuances. In the aggregate, the picture is getting increasingly complex and challenging for global firms in particular. Even for UK firms where the bulk of their business takes place domestically, some of the organisations that are likely to be considered to be CTPs will not be UK-based.

Firms in the UK are tasked with the delicate balance of adhering to rigorous operational resilience rules while remaining competitive. The UK's commitment to being "open for business" necessitates a competitive edge, but strict regulations may hinder this goal. In some cases, other jurisdictions (e.g. Japan, Singapore, Hong Kong, Ireland) do not impose operational resilience requirements as stringently as those in the UK. This places firms in the UK at a potential disadvantage when competing with some offshore counterparts, especially in attracting international business.

Regulatory arbitrage opportunities may arise when firms not based in the UK can exploit differences in operational resilience requirements, potentially gaining an unfair competitive advantage. Such situations can undermine the integrity of the financial system. Eliminating regulatory arbitrage opportunities should be a matter (in the UK) for the regulators' competition mandate.

Recommendations for firms

We recommend that **firms** pursue the following:

1. **Industry Collaboration**
   - Establish synergies across the industry to share best practice and optimise the efficiency of assurance exercises. Close engagement with The Cross Market Operational Resilience Group (CMORG) will help oversee assurance efforts effectively.
   - Drive communication and information sharing between firms, third-party providers and regulators to create a streamlined and consistent approach.
   - Explore opportunities to simplify the assurance process without compromising on operational resilience, based on International Organization for Standardisation (ISO) 20022. For example, industry coordination to support testing. Industry has a good track record in this area, having implemented relevant requirements in the Markets in Financial Instruments Directive, Regulatory Technical Standards 6 (MiFID II RTS 6)

[2] The implementation period is 2 years, making DORA enforceable from 17 January 2025.

on self-assessments and attestations to third parties undertaken by the Futures Industry Association (FIA) and others.

- Use industry bodies to pursue collaboration between industry, regulators and government to deliver pragmatic, proportionate and – where possible – interoperable standards. For example, on assessment methodologies and resilience requirements. Existing resources such as the Standardized Information Gathering (SIG) questionnaire should be leveraged to share best practices, solutions and tools to align assurance procedures.
- Utilise existing industry resources to better signpost to existing industry guidance such as that from the CMORG or industry trade bodies (see annex).

2. Continuous engagement with regulators

- Keep abreast of regulatory developments, as these may improve access to assurance information for certain third-party providers.
- Persistently seek regulatory guidance and support. Suggest subject matters for regulatory thematic reviews. Escalate issues to regulators as needed, and document these interactions. This proactive approach will demonstrate to regulators that the firm is taking steps to ensure the resilience of its CTPs.
- Ask regulators, business groups and overseas authorities for support in producing guidance for firms.
    - This is important for large offshore firms which are not start-ups and where the competition for similar services is limited.
    - This is even more important, although for different reasons, for start-ups or scale-ups which may not have the resources to ensure that their products and services are as resilient as their potential customers need. We should not ask for forbearance from the operational resilience rules to engage with start-ups, but instead ask for governmental support here. For example, tax breaks, grants, collective purchase agreements, Competition Act 1998 (CA98) exemptions or waivers.

3. Independent due diligence and classification

- Push ahead with their own third-party due diligence exercises, and not rely on anything from the CTP regulation, to ensure they are ready by March 2025. Firms must integrate operational resilience assurance into other lifecycle management processes. Once the CTP regulation is in place, firms can review their third-party due diligence work and determine the scope of the due diligence work they still need to carry out, over and above the CTP regulation, to satisfy themselves that their third parties are resilient. This includes assessing the operational resilience considerations in new product governance and approval processes.
- Develop a prioritised list of whom they consider to be their critical third-party providers through a defined methodology. This will vary from firm to firm, depending on the nature of their business. This documentation will prove valuable when aligning with regulatory requirements and reporting to authorities.

- Firms should identity their own impact tolerances and be clear about which 'severe but plausible' (SBP) scenarios fit within these. For those where the level of risk is not manageable, additional consideration must be given to identify what steps would be needed.

4. **Alignment within Firms**
   - Firms operating across multiple jurisdictions should prioritise an internally aligned approach to operational resilience. This will promote consistency, reduce compliance risks, and enhance operational resilience across the organisation.

5. **Two-Step Approach**
   - Implement a two-step approach comprising verification (does the third-party product or service comply) and validation (is it fit for purpose) to assess third-party products and services, and structure their testing accordingly. It is important to look beyond contractual commitments to ensure that firms are able to provide evidence for resilience.

6. **Due Diligence:**
   - There is concern about the increasing burden of due diligence, where industry parties are often enquiring as to each other's resilience, at disproportionate cost in terms of time and resources.
   - A potential solution is reliance on external assurance or some other innovations, to ease the burden and deal with the requirements more efficiently and proportionately to execute due diligence questionnaires (DDQs).

Recommendations for regulators

We recommend that regulators consider operational resilience requirements through the lens of international competitiveness implications, to ensure that increased resilience assurance increases the competitiveness of the UK, rather than impedes it. This should be considered as fundamental to the regulators' new secondary competitiveness and growth objective.

In light of this, we ask **regulators** to consider the following:

1. **A proportionate and dynamic approach**
   - Acknowledge the tension between the pace of consolidation and maturity of advancements in technologies, and the ever-evolving landscape of risks. A flexible and proportionate approach is needed to balance resilience expectations with the need to remain competitive and meet rapidly changing consumer expectations.
   - Apply principles consistently and proportionately, aligned with the risk profile of the firms they supervise.

2. **Continuous engagement with the industry**
    - Share information with individual firms or groups of firms on concentration risks (where these are not considered CTPs).
    - Conduct regular thematic reviews – on a non-enforcement, information-gathering basis only – to provide the market with data with which to update its methodologies and approach.
    - Explore opportunities to simplify the assurance process for firms without compromising on operational resilience.
    - Provide industry guidance on the implementation of operational resilience requirements, including clearer guidelines on the "plausible" element of SBP scenarios.
    - Maintain up-to-date market and threat reviews in order to support policy updates, robust SBP scenarios, and enhanced testing and simulation methodologies.
    - Work with industry to highlight and promote the commercial benefits of operational resilience, such as:
        a. Improved understanding of services
        b. Better prioritisation of investment
        c. Reduced disruption to clients/customers
        d. Improved client trust.

3. **Global Regulatory Alignment**
    - Identify and understand the common themes and differences in operational resilience regulations between the UK and other jurisdictions. This knowledge will support consistent implementation of approaches that focus on the risks to be addressed and potential strategies to address misalignments.
    - Seek collaboration with other jurisdictions to establish a single baseline set of operational resilience regulations. This would reduce compliance complexities, eliminate regulatory arbitrage opportunities, and ensure uniformity in standards.

Conclusion

As the deadline of 31 March 2025 approaches, industry collaboration and engagement with regulators will be imperative to navigate the path to third-party assurance. Regulators must adopt a proportionate and dynamic approach to operational resilience requirements, recognising the evolving landscape of risks and technological advancements. Operational resilience will support future financial stability and the safety and security of customers. However continuous engagement between regulators and the industry, global regulatory alignment, and the promotion of commercial benefits will be essential to effectively support the long-term competitiveness of the UK FRPS industry. We look forward to continuing to work with firms and regulators to get this balance right.

Annex: Existing Industry Resources

Title	Organisation	Description	Link	Date
Guidance for Firm Operational Resilience	Cross Market Operational Resilience Group (CMORG)	The guidance incorporates the key requirements set out by the UK regulators for implementing operational resilience into firms. The content should be considered as high-level principles that can be used proportionately by a firm accordingly to their size, scale and complexity. It is not intended to be prescriptive or mandatory, but rather to support completion of individual firm documentation that aligns to the organisation's specific corporate governance requirements and templates. Chapters: • Identifying Important Business Services • Impact Tolerances • Mapping and assessments • Scenario testing • Self-Assessment.	Guidance for Firm Operational resilience - TLP Clear - CMORG.pdf	03.11.23
Third-party Lifecycle Management Guidance	Cross Market Operational Resilience Group (CMORG)	Industry expertise on managing resilience risks through the lifecycle of a third-party engagement, optimising the approaches undertaken by larger firms and supporting capability building across the wider sector. The guidance considers each stage of engagement from supplier selection and due diligence, classification to support supplier management approach, governance and assurance through to exit.	CMORG Third-party Lifecycle Management Guidance - TLP Clear.pdf	