payments and crypto network

Operational Resilience

A series of guides addressing the subject of Operational Resilience for UK authorised Electronic Money Institutions ("EMI") and Payment Institutions ("PI").

Guidance is provided for firms and is not intended as legal advice.

Guide 1: Operational Resilience - Overview

Background

UK authorised EMI and PI businesses must adhere to the regulatory requirements defined in the Electronic Money Regulations 2011 ("EMR") and the Payment Service Regulations 2017 ("PSR") as well as and associated guidance from the UK's Financial Conduct Authority ("FCA") and relevant EBA Guidelines.

In March 2021 the FCA published their Policy Statement on Building Operational Resilience (PS21/3) which provides feedback on their previous consultation and the final operational resilience rules.

Firms should note that the FCA's rules and guidance on Operational Resilience came into force on 31 March 2022. The final implementation deadline is 31 March 2025 meaning that firms *"must be able to remain within their impact tolerances"* before that date.

This first guide provides an overview of the operational resilience requirements. Subsequent guides address specific areas of the requirements.

Background to Operational Resilience

The FCA introduce the concept of Operational Resilience in PS21/3, stating: *"Ensuring the UK financial sector is operationally resilient is important for consumers, firms and financial markets. It ensures firms and the sector can prevent, adapt, respond to, recover and learn from operational disruptions".*

Essentially the objective is to reduce the potential *"harm to consumers and risk to market integrity".* Whilst these definitions use the term "consumer" the requirements relate to the customers of the firm's services (not just individual consumers).

The FCA's Operational Resilience rules are a high-level, principles-based framework designed to provide sufficient flexibility to firms when implementing an approach to operational

resilience. The key stages in implementing the operational resilience requirements are described in this guide.

What is Operational Resilience?

An operationally resilient firm is able to minimise the impact of disruptions, enabling it to recover and learn from disruptions, continue service provision and thereby minimise adverse impacts on customers and the integrity of the financial system. The FCA define Operational Resilience as the ability of financial services firms and the financial services sector to *"prevent, adapt, respond to, recover, and learn from operational disruptions"*.

Recognising that disruptive events will occur, that they will impact the business and must therefore be managed in an effective manner, is the first step in recognising the importance of operational resilience work and implementing an appropriate approach.

Responsibility for Operational Resilience

The Board of the firm will be responsible for ensuring that the business is resilient and that the firm implements an approach towards operational resilience that meets regulatory requirements. Operational resilience is closely related to risk management and should be incorporated into the enterprise-wide risk management framework for which the Board similarly has responsibility.

Day to day responsibility may be allocated to a role such as the Compliance Manager, or similar senior management role (typically operating at the second line of defence), that would have a direct reporting line into the Board.

What outcomes do the FCA expect?

The FCA states that in implementing operational resilience they expect both firms and the financial sector to *"better prevent, adapt, respond to, recover and learn from operational disruptions"*. The stated outcome of improved operational resilience is the reduction in *"harm to consumers and risk to market integrity"* that may be caused through disruptions.

The FCA's supervisory work is designed to ensure that the operational resilience requirements drive changes within firms that work to minimise harm. As a result, the FCA expect to see a positive change in the number and type of major operational or security incidents reported to the FCA as well as improved audit findings reported in the REP018 (Operational and Security Risk Report).

The FCA's Policy Statement is not intended to conflict with, or supersede, existing requirements on firms to manage operational risk or business continuity planning, but rather to set new requirements that enhance the resilience of firms.

Timing of implementation of requirements

As soon as possible after 31 March 2022, and by no later than 31 March 2025, firms must have performed mapping and testing so that they are able to remain within impact tolerances for each important business service. Firms must also have made the necessary investments to enable them to operate consistently within their impact tolerances. Operational resilience is likely to be a key area of focus for the FCA in their supervisory work.

What approach does the FCA expect?

The FCA's Policy Statement outlines the approach that firms should take towards implementing operational resilience. The approach comprises a number of key steps, as detailed below and illustrated in the diagram in Appendix I:

- Identify **important business services** - Firms should already have completed this exercise by 31 March 2022. An important business service must be clearly identifiable as a separate service. The process of identifying the important business services can be undertaken in a manner that management consider most appropriate. The FCA have also published a number of "*factors*" that are helpful to be considered when identifying important business services.
- Set **impact tolerances** – These represent the maximum level of disruption that is acceptable whilst still being able to provide the important business services. Beyond this point any disruption to the important business services would cause "*intolerable harm*" to consumers or market integrity.
- Perform a **mapping exercise** – Identifying and documenting the resources (e.g. people, processes, technology, facilities and information) that are necessary to deliver each important business service. This mapping exercise should enable the firm identify vulnerabilities such that they can be remedied and/or used to facilitate the development of scenarios to be used during scenario testing (see below).
- **Scenario testing** – testing based on a range of "*severe but plausible*" scenarios to help identify areas where operational resilience needs to be improved, i.e. whether they can remain within the impact tolerances that have been defined for each of the important business services.
- **Communication** – Firms must have internal and external communications plans ready in the event that their important business services are disrupted.
- **Self-assessment** – The FCA also require firms to self-assess their operational resilience arrangements and document their assessments.

The above steps are addressed in more detail in subsequent guides.

Appendix I – Overview of the Operational Resilience process