Operational Resilience:

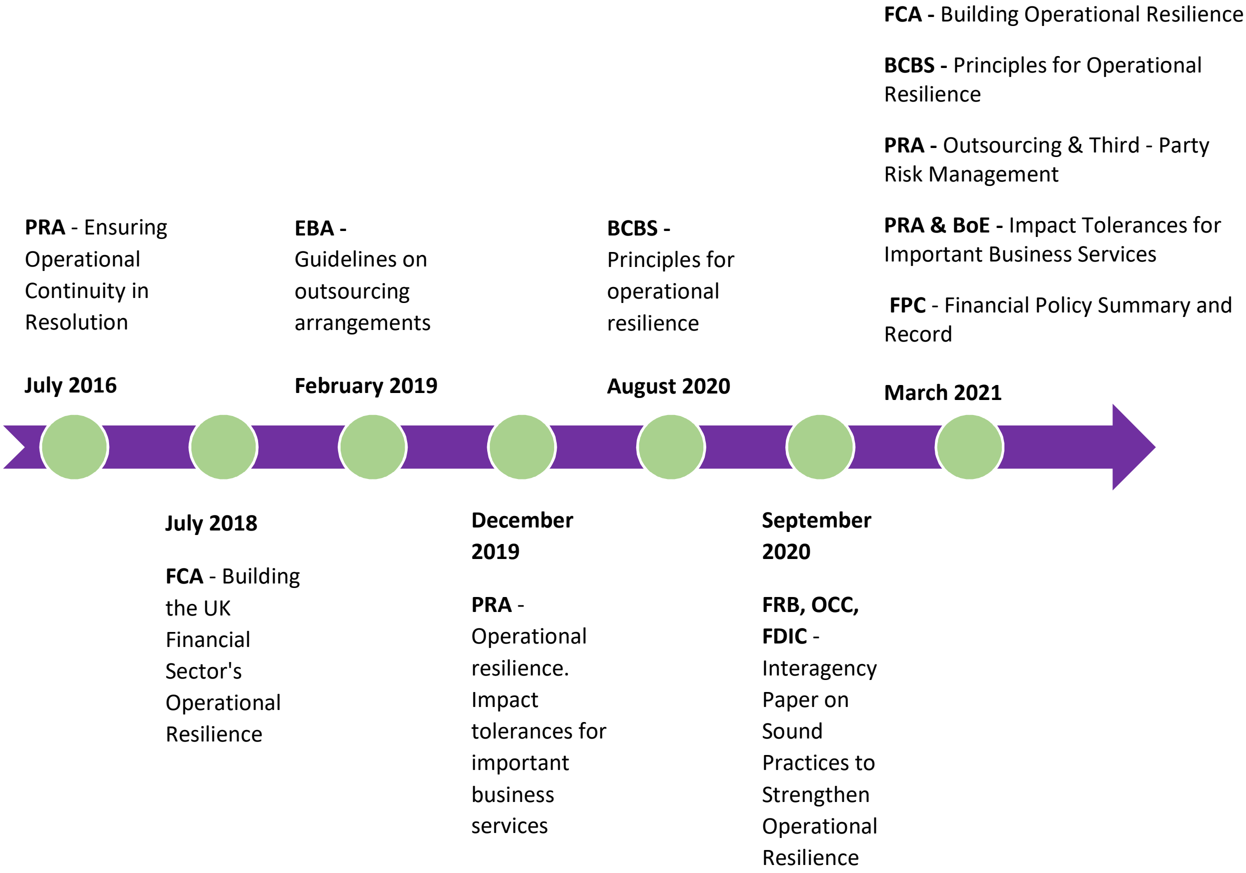
An evolving and challenging landscape

Operational resilience landscape

As the prudential risk framework evolved after the Global Financial Crisis (GFC), regulators noted that better capital and liquidity management are only part of the solution to improve the ability of firms to absorb external shocks.

Operational continuity failures, while firms had robust capital and liquidity levels, could still threaten financial stability. There was a gradual realisation that FS firms needed to be better at responding to operational events – pandemics, cyber incidents and natural disasters (meta risks) – which can significantly impact their ability to continue operating.

This thought process has been reflected through a number of supervisory statements and expectations issued since 2015 and recent PRA and FCA interactions with firms. The Digital Operational Resilience Act (DORA) in the EU is another key regulation that firms in scope are responding to.



In particular, the Bank, PRA, and FCA's operational resilience policy, issued in March 2021, requires firms to identify important business services, set impact tolerances for those services, and act to continue to deliver them during severe but plausible disruptions. Updated policy on outsourcing and third-party risk management complements the wider operational resilience policy, and considers firms' growing dependency on third parties, including cloud service providers.

During 2022, the PRA will assess firms' progress against its policy expectations that came into force on 31 March 2022. This will include an assessment of firms' plans to ensure they will be able to deliver important business services within impact tolerance, no later than 31 March 2025.

The initial findings from this assessment were mentioned in a speech by David Bailey in April 2022[1], in which he discussed the work the PRA does with UK banks and building societies to strengthen their resilience, while mentioning how well these firms have implemented the PRA's policy in this area to date. High-level findings include:

- Firms have generally made positive progress against the PRA's expectations for identifying Important Business Services;
- Setting Impact tolerances has been more challenging for firms; and
- Firms are leveraging existing frameworks and tools for mapping and testing.

Overall, the view is that meaningful progress has been made, however, work still needs to be done in order to meet the regulatory expectations. On the same wavelength is the speech given by Duncan Mackinnon in May 2022[2], in which it is reported that many firms are expected to have further work to do to set impact tolerances relating to safety and soundness and financial stability. Where firms have set tolerances, there has often been a wide range of tolerances across different firms providing the

[1] Operational resilience: next steps on the PRA's supervisory roadmap – speech by David Bailey, April 2022
[2] What will operational resilience look like going forward? An overview of the supervisory regulatory position – speech by Duncan Mackinnon, City & Financial 9th Annual Operational Resilience for Financial Institutions Summit, May 2022

same service. For example, CHAPS payments impact tolerances for safety and soundness varied across some firms from two days to two weeks. The regulator will discuss these variances with firms to understand how they came to the conclusions they have, and how the tolerance they have set will protect safety and soundness and financial stability.

As mentioned in this speech, the PRA will continue to focus on how firms take their work forward to 2025 and beyond. As long as important business services, impact tolerances, mapping and testing are only the start, PRA expects firms' mapping to include all critical resources and consider internal and external dependencies. Mapping should rapidly become more sophisticated, in line with firms' potential impact. It should enable firms to identify vulnerabilities, and inform the development of scenario testing. And testing itself should be evolving so that firms can assure their boards they can deliver important business services within impact tolerances through severe but plausible scenarios by end-March 2025.

Another finding from the speech refers to the utilisation of disaster recovery and business continuity testing to address operational resilience requirements. If existing testing does not provide a firm with an end-to-end view of the resilience of its important business services, the PRA expects that more work will have to be done, including utilising sufficiently severe scenarios.

The PRA, as mentioned in its Business Plan[3], will continue to deliver its priorities around operational resilience through a broad range of industry and sector-based engagements such as the Authorities Response Framework, the Cross Market Operational Resilience Group, the Cyber Expert Group, and the Basel Committee for Banking Supervision Operational Resilience Group.

As indicated by the Financial Policy Committee (FPC) in 2021, the PRA and FCA will publish a joint discussion paper outlining potential additional measures to enhance the oversight of the systemic risks posed by critical third-party service providers. Joint authorities will also co-ordinate work on the longer-term approach to supervising cyber risks, and improving the collection of operational incident and outsourcing data.

In March 2022, the PRA published Policy Statement PS2/22 | CP21/21 - Operational Resilience and Operational Continuity in Resolution[4]. Firms and holding companies are required to take a group level view of operational resilience, guaranteeing risks arising in parts of the group that are not subject to the individual requirements, are considered.

PS2/22 | CP21/21 - Operational Resilience and Operational Continuity

The new policy provides feedback on responses to Consultation Paper (CP) 21/21 on Operational Resilience and Operational Continuity[5], amending the following:

- Operational Resilience Part of the PRA Rulebook, the Insurance – Operational Resilience Part of the PRA Rulebook and the Group Supervision Part of the PRA Rulebook[6];
    - New rules have been introduced to Chapter 8 (Group Arrangements), requiring CRR consolidation entities to comply with the following requirements by no later than 30 June 2022:
        - Assess the ability of group members to remain within impact tolerances for their Important group Business Services; and
        - Ensure the entity's board approves the entity's assessment.

[3] Prudential Regulation Authority Business Plan 2022/23
[4] PS2/22 - Operational Resilience and Operational Continuity in Resolution: CRR firms, Solvency II firms, and Financial Holding Companies (for Operational Resilience), March 2022
[5] CP21/21 'Operational Resilience and Operational Continuity in Resolution: CRR firms, Solvency II firms, and Financial Holding Companies', November 2021
[6] Pra Rulebook: CRR Firms, SII Firms: Operational Resilience Instrument 2022, PRA2022/1

- SS1/21 'Operational resilience: Impact tolerances for important business services'[7];
  - Chapter 9 of SS1/21 has been amended to clarify where the policy applies to a CRR consolidation entity and where the policy applies to an insurer, deleting the reference to the definition of important group business services, providing examples of important group business services and clarifying the PRA's expectations regarding how CRR consolidation entities and insurers should consider important group business services;
  - In addition, paragraph 9.4 of SS1/21 add an expectation that CRR consolidation entities should have a regular dialogue with other members of its group regarding the assessment required under Rule 8.8 of the Operational Resilience Part applicable to CRR firms in order to facilitate the CRR firm's own analysis.
  - a new bullet in paragraph 8.3 of SS1/21 has been inserted to clarify the PRA's expectations regarding the contents of a CRR firm's self-assessment as required under Rule 6.1 of the Operational Resilience Part applicable to CRR firms in respect of additional risks arising elsewhere in the group;
- Operational Continuity Part of the PRA Rulebook[8]:
  - CP21/21 proposed a minor amendment (deleting the word 'other') to the Operational Continuity Part of the PRA Rulebook, in order to clarify the intended scope of application of the rule.

Scope

Regarding operational resilience, this new PS will be relevant for UK banks, building societies, PRA-designated investment firms, CRR consolidation entities, UK Solvency II firms, and the Society of Lloyd's and its managing agents. For the Operational Continuity in Resolution aspects, this PS will be relevant to UK banks, building societies, and PRA-designated UK investment firms. The Operational Resilience Parts of the PRA Rulebook do not directly apply to branches, which are regulated by the SS5/21 policy.

Implementation dates

The implementation dates for the changes set out in the mentioned PS are:

- 31 March 2022 for the Operational Resilience Parts and the Group Supervision Part; and
- 30 June 2022, for CRR consolidation entities to be compliant with the changes introduced to Chapter 8 of the Operational Resilience Part
- 1 January 2023 for the Operational Continuity Part.

Operational Resilience Journey: aspects that firms need to consider

As Avantage Reply, we see the following aspects that firms need to consider in their operational resilience journey:

- **Iterative process:** Once the important business services are defined there is an expectation to perform annual reviews and increase sophistication of mapping and understanding, making necessary progress within the three year period to remediate any vulnerabilities and remain in tolerance.
- **Senior Management accountability and governance**: The statements place firm accountability with the senior management regime. The authorities have made it clear there is no need for extra committees, leverage the SMF24 regime if applicable or board for suitable sign off.
- **Comprehensive approach**: The operational resilience statements should bring together operational risk and the existing response and recovery plans. Firms should drive a culture of operational resilience and not treat it as a side of desk programme.

[7] Supervisory Statement, SS1/21 Operational resilience: Impact tolerances for important business services, March 2022
[8] Pra Rulebook: CRR Firms: Operational Continuity Instrument 2022, PRA2022/2

- **Third Country v Subsidiaries v UK branches:** Align to the spirit and intent of the policy statements irrespective of legal nuances. In the FCA PS 21/3 it states that 3rd country branches are technically out of scope for the FCA. However, there is an expectation of all branches, that they are well regulated and do not pose a risk to the regulatory objectives. A firm operating as a branch in UK should align the UK regime to the greatest extent.
- **Shifting nature of business models:** Risks from the pandemic follow a different rhythm to other types of risk, some of these stem from the technological complexity and cyber-risk. Plans to migrate functions to the Cloud, initially stretched out over 4-5 years, are now considered in terms of a much shorter timeframe.
- **Operational resilience vs Financial resilience:** In contrast to financial resilience, there is no bail out option if firms are unable to function because of an operational incident. On one hand, firms will seek to be self-reliant but at the same time financial services firms are encouraged by the regulators to invest in collective action for addressing many of the common challenges faced
- **Impact tolerances for dual-regulated firms:** The PRA and FCA have different objectives: Disruptions that may impact safety and soundness or financial stability could be different from those that may cause customer harm. For now, only large firms are asked to have set impact tolerances with regard to financial stability
- **Outsourcing and third-party dependencies:** If correctly configured there are clear resilience benefits to firms from Cloud adoption by enabling a scalable IT infrastructure. However, due to their size some firms find it challenging to oversee Cloud Services Providers (CSPs), with a limited ability to implement effective Business Continuity Plan (BCPs), negotiate contractual safeguards and obtain appropriate assurance from CSPs. Satisfactory levels of assurance is required from all third-parties, regardless of outsourcing / non-outsourcing classification

How Avantage can assist

As you implement solutions to meet the regulatory requirements for operational resilience, Avantage Reply can support you in the following ways:

- **Knowledge Sessions:** Educate the Board and senior management on the regulatory requirements and the implications for your firm while providing industry insight and examples of best practices.
- **Regulatory Gap and Self-Assessments:** Review your current status against the regulatory requirements, identify and prioritise the gaps, and devise a remediation plan.
- **Identification or refresh of Important Business Services (IBS):** Conduct an initial assessment of the business services at your firm and identify which are deemed important in the regulatory context, utilising our industry insight and the best practice we see across the market. We can also provide a refresh of your existing IBS assessment to ensure the list of remains up to date.
- **Identification or refresh of Impact Tolerances**: Based on the choice of IBSs, we can support you to determine appropriate impact tolerances, utilising our industry insight and the best practices we see across the market. We can also provide a refresh of existing impact tolerances to ensure they remain appropriate and in line with industry practices.
- **Scenario Testing:** Support you to develop and execute an operational resilience scenario testing plan.
- **Governance Arrangements**: Support you in enhancing your governance arrangements to appropriately capture operational resilience considerations. Specifically, this can involve updating roles and responsibilities, committee terms of reference, and reporting and escalation channels.
- **Framework Implementation and Enhancement**: An effective approach to operational resilience requires a robust and comprehensive framework to be in place covering the processes, governance arrangements, reporting, policies and procedures. We can support you to implement this framework or enhance your existing framework based on our industry insights and the best practices we observe across the market.

- **Framework Integration**: Support you to integrate your operational resilience framework with other existing frameworks including your Risk Management Framework, Business Continuity Planning, and Recovery and Resolution Planning.

Contacts

Vishwas Khanna, Partner

Vishwas specialises in prudential regulation, risk transformations, programme leadership and new bank authorisations.
vi.khanna@reply.com

Rohan Wilson, Senior Manager

Rohan has significant experience leading regulatory change and risk management projects at key financial services clients across investment and challenger banks, including for climate and environmental risk. He has also supported European regulators.
r.wilson@reply.com

Sam Russell, Senior Consultant

Sam formerly worked at the Prudential Regulation Authority supervising the UK operations of international investment Firms prior to joining Avantage Reply.
s.russell@reply.com

Federico Dalbon, Consultant

Federico has developed a solid background in data analysis and statistical modelling, with skills gained on delivering projects covering risk modelling, internal process reviewing and data governance at a range of private and retail banks.
f.dalbon@reply.com