FARRER&Co

# Implementation of the new Operational Resilience Regime for FS firms

February 2022

# Introduction

As the financial system begins to recover from Covid related shocks, the implementation date for the new operational resilience regime designed by the FCA in PS21/3 Building Operational Resilience and the PRA in its Statement of Policy on Operational resilience and PS6/21 Impact tolerances for important business services is fast approaching. In this briefing we examine what operational resilience is, summarise the new obligations on affected firms and what firms should be concentrating on as the implementation date of 31 March looms. We also examine the PRA's Supervisory Statement on Outsourcing.

## What is operational resilience?

According to the FCA and PRA (the regulators) operational resilience is "the ability of firms, financial market infrastructures and the financial sector as a whole to prevent, adapt and respond to, recover and learn from operational disruption." While firms already have obligations to protect their operational resilience, with the FCA's Principle 3 and the PRA's Fundamental Rule 6 requiring a firm to organise and control its affairs responsibly and effectively, recently the regulators have become more concerned with the operational resilience of the sector.

The financial industry has long had to deal with shocks and disruptions whether systemic such as the financial crisis of 2007/2008, or more localised with data hacking breaches targeting individual firms. Indeed, between the beginning of February 2020 and the end of April 2021, a survey by VMware found that cyber-attacks on the financial sector had increased 238 per cent globally. The pace of technological change and the growing reliance on third party providers for key services and functions mean that operational risk management is key to the smooth running of firms. Given these significant challenges for firms, the regulators' view is that operational disruption is inevitable and therefore firms should be planning and preparing for operational challenges.

The UK regulators are clear that ensuring the UK financial sector is operationally resilient is important for consumers, firms and financial markets. They regard operational resilience as vital to supporting a firm's financial resilience. Since the FCA, PRA and BoE published their original consultation papers regarding operational resilience in December 2019, the regulators have developed their rules which were published in final form in March 2021. Since then, firms have been working to ensure that they can meet their obligations from the implementation date of 31 March 2022.

F&
Co

## Who does it apply to?

| Firms subject to both PRA and FCA rules | Firms subject to FCA rules |
|---|---|
| UK banks, building societies and PRA designated investment firms | UK recognised investment exchanges |
| UK solvency II firms, the Society of Lloyd's and its managing agents. | Enhanced firms under the Senior Managers and Certification Regime (SMCR), including for example firms which hold in excess of £1 billion in client assets, firms with assets under management in excess of £50 billion etc. Estimated by the FCA at about 350 firms. |
| | Payment institutions, electronic money institutions and registered account information service providers authorised or registered under the Payment Services Regulations 2017 and the Electric Money Regulations 2011 |

In terms of territorial scope, this new regime does not apply to firms carrying out business in the UK under the temporary permissions regime or to UK branches of third country firms. While the FCA has confirmed that the new regime does not apply to third country branches of UK regulated firms, it has suggested that similar measures could be adopted by firms in respect of such third country branches in order to have a consistent approach across their business.

For firms that fall outside the current scope of the new rules, such as core firms under the SMCR, the FCA has reminded such firms of the requirement to meet current operational resilience obligations in the FCA Handbook. The FCA will be considering whether to extend the new regime to all firms it regulates in the future.

# The new framework

Given the UK's regulatory system which is split between FCA and the PRA both regulators have published their rules for firms within their respective remits. The rules are broadly consistent, but there are differences in emphasis in certain definitions which are set out below for each of the key components of the new regime. The FCA's new rules are set out in SYSC 15A and the PRA sets out its new rules in the Operational Resilience Parts of the PRA Rulebook and Group Supervision Part (for Group Operational resilience).

The incoming regime includes the following key elements:

- Identification of important business services
- Setting of impact tolerances
- Remaining within impact tolerances
- Strategies, processes and systems including:
  - Mapping
  - Scenario testing
- Self-assessment
- Governance and senior manager obligations

| Identification of important business services/ | FCA | PRA |
|---|---|---|
| Definition | A service which if disrupted could:<br>• cause intolerable levels of harm to any one or more of the firm's clients; or<br>• pose a risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets. | In summary, a service which if disrupted could pose a risk:<br>• to the stability of the UK financial system;<br>• the firm's safety and soundness;<br>• to an appropriate degree of protection for those who are or may become the firm's policyholders. |
| Type of services to be included | **Both** regulators state that external services only should be included.<br>While internal services (such as payroll and HR) and shared group services (such as IT or risk management) can be important to the running of a firm, they are not captured as important business services by the regulators. However, such internal services constitute processes which may be necessary to the provision of important business services and should be captured by firms as part of their mapping exercises as set out below.<br>The regulators have not set out a definitive list of important business services, as firms need to decide that for themselves, but they have provided some examples such as:<br>• an investment bank's provision of currency hedging services;<br>• a retail bank's provision of ATM cash withdrawals to customers;<br>• an online wealth management platform provider's administration of investments;<br>• a custodian's safekeeping of securities for its consumers. | |
| Factors to consider in deciding whether a service constitutes an important business service | Some of the factors the FCA expects firms to consider include:<br>• the nature of the client base, including vulnerabilities that would make the person more susceptible to harm from a disruption;<br>• the ability of clients to obtain the service from other providers;<br>• the time criticality for clients receiving the service;<br>• the number of clients that would be affected;<br>• the sensitivity of data held in the case of a breach;<br>• the firm's potential to inhibit the functioning of the UK financial system;<br>• the firm's potential to impact the soundness, stability or resilience of the UK financial system. | Some of the factors the PRA expects firms to consider include:<br>• financial stability: the impact on the wider financial sector and UK economy;<br>• the firm's safety and soundness: the impact on the firm itself, including the:<br>  • impact on the firm's profit and loss;<br>  • potential to cause reputational damage;<br>  • the potential to cause legal or regulatory censure. |
| Review | At least annually and when any "material" change such as the firm beginning to carry out a new business service or outsourcing a new or existing service. | Firms to undertake an annual check of their existing important business services and whether any new important business services need to be identified. |

| Setting of impact tolerances | FCA | PRA |
|---|---|---|
| Definition – at what point should firms set their tolerance level. | The maximum tolerable level of disruption to an important business service as measured by a length of time and any other relevant metrics, reflecting the point at which any further disruption to the important business service could pose intolerable harm to any one or more of the firm's clients or risk to the soundness, stability or resilience of the UK financial system or the orderly operation of the financial markets.<br><br>FCA guidance on what constitutes intolerable harm indicates that it is harm from which consumers cannot easily recover. It is greater than inconvenience and harm which can be easily financially remediated by the firm. | The maximum tolerable level of disruption to an important business service or an important group business service as measured by a length of time in addition to any other relevant metrics<br><br>Depending on the type of firm, a firm's impact tolerance must specify the first point at which a disruption to the important business service would pose a risk to:<br><br>• the stability of the UK financial system;<br><br>• the firm's safety and soundness;<br><br>• an appropriate degree of policyholder protection. |
| Number of impact tolerances | At least one impact tolerance for each important business service should be identified. For dual regulated firms, see below. | |
| Measuring impact tolerances | **Both** regulators require firms to set their impact tolerances using clear metrics.<br><br>Firms must use a time-based metric for all impact tolerances, specifying the length of time for which a disruption to an important business service can be accepted.<br><br>Firms should also consider:<br><br>• the fluctuations in demand for important business services;<br><br>• frequency of operational disruption;<br><br>• disruption to multiple important services. | |
| Dual regulated firms | Dual regulated firms can set their impact tolerances at the same point for a business process if they are sure that such a tolerance point is suitable for both regulators. Such dual regulated firms should be able to justify such a decision if required to do so by a regulator.<br><br>The FCA also notes that firms can concentrate their efforts to ensure that they remain within the most stringent tolerance point, provided they can show that they have considered each regulator's objectives, that any recovery and response arrangements are suitable for both longer and shorter time periods of disruption. | |
| Reviewing impact tolerances | Firms must keep their compliance with the obligation to set impact tolerances under review at least annually and consider whether they remain compliant if there is a relevant change to their business or the market in which they operate. | Firms must prepare and regularly update a written self-assessment of their compliance with the operational resilience regime including setting impact tolerances. |
| **Remaining within impact tolerances** | Firms are required to ensure they are able to remain within their impact tolerances should they be subject to a "severe but plausible" disruption. To identify such "severe but plausible" scenarios firms can consider previous near misses, but the regulators stress that the scenarios must be sufficiently severe, otherwise senior management can be challenged by the regulators as to the level of risk they are taking with the business.<br><br>This obligation applies whether or not they use third parties in the delivery of their important business services. Firms should effectively manage their use of third parties to ensure they can meet the required standard of operational resilience. For more on outsourcing and third-party services please see below. | |
| Transitional period for remaining within impact tolerances | Firms must comply with the requirement to remain within their impact tolerances within a reasonable time of the new rules coming into effect on 31 March 2022 and, in any event, by no later than 31 March 2025.<br><br>The regulators expect firms to agree with their supervisors what a reasonable compliance date would be for each firm. | |
| Failure to meet impact tolerances | Where a firm fails to remain within an impact tolerance it has set, it would be expected to notify the FCA under Principle 11 of the FCA's Principles for Businesses | Where a firm fails to remain within an impact tolerance it has set, it would be expected to notify the PRA under Fundamental Rule 7 of the PRA's Fundamental Rules. |

| | FCA | PRA |
|---|---|---|
| **Strategies Systems & Processes** | Firms must have sound, effective and comprehensive strategies, processes and systems to enable them to comply with their operational resilience obligations. These strategies and processes include mapping and scenario testing. | |
| **Mapping** | The purpose of mapping is to identify the resources that are critical to delivering an important business service. It should enable firms to:<br>• identify vulnerabilities in the delivery of important business services within an impact tolerance, such as high complexity, single points of failure, concentration risk and dependencies on third parties. This identification will enable firms to remedy such weaknesses.<br>• test their ability to stay within impact tolerances (see scenario testing below).<br>Firms should understand how any third-party providers support important business services. Firms should also ensure that such arrangements would not create a vulnerability in meeting the firm's impact tolerances. For more on outsourcing see below. | |
| Transitional period | The regulators recognise that firms' mapping processes will evolve over time. Firms should have carried out such mapping to identify important business services, set impact tolerances and identify any vulnerabilities in their operational resilience by 31 March 2022. By this date, firms should be able to set out a compelling gap analysis, identify any major shortcomings and begin work on such areas.<br>Firms will then have until 31 March 2025 to develop their mapping with a view to being able to remain within impact tolerances for each important business service. | |
| Review | Firms are required to update their mapping exercise at least annually or following significant change. | |
| **Scenario testing** | In order to identify vulnerabilities that could mean firms would be unable to stay within their impact tolerances, firms must regularly test their ability to deliver important business services within their impact tolerances in the event of a severe but plausible disruption of their operations. | |
| Types of scenario firms should test for | While firms need to set their own scenarios, they could consider the following:<br>• previous incidents or near misses within their organisation, across the financial sector etc;<br>• other risks such as the evolving cyber threat, technological developments and business model changes.<br>Firms should ensure that testing considers realistic timeframes, for example, the time needed for data analysis and decision making, and that it should develop as the firm learns from previous testing.<br>When developing testing plans, firms should consider numerous factors including for example:<br>• the type of scenario testing, eg, paper-based, simulations or live-systems testing;<br>• the frequency of the scenario testing;<br>• the number of important business services tested - firms that have identified more important business services should undertake more scenario testing to reflect this. | |

*Continued on next page*

| | FCA | PRA |
|---|---|---|
| Frequency of scenario testing | The FCA requires firms to carry out regular scenario testing and if there is a material change to a firm's business important business services or impact tolerances. | The PRA will also require firms to carry out scenario testing regularly. It expects firms that implement changes to their operations more frequently to undertake more frequent scenario testing. |
| Transitional period | The regulators recognise that firms' scenario testing processes will evolve over time.<br><br>Firms are expected to have carried out scenario testing to a level which allows firms to identify important business services, set impact tolerances and identify any vulnerabilities in their operational resilience. In practice, this means that firms will not need to have performed scenario testing of every important business service by that date.<br><br>Firms will then have until 31 March 2025 at the latest to continue performing scenario testing with a view to being able to remain within impact tolerances for each important business service. They should continue to test as effectively as possible during the transition period. | |
| **Lessons learned** | After any scenario testing, or any operational disruption, firms should carry out a lessons learned exercise, which they should document appropriately, and update the self-assessment documentation accordingly. | |
| **Communications** | The FCA requires firms to maintain an internal and external communication strategy to act quickly to reduce the anticipated harm caused by operational disruptions. | |

| Self-assessment | FCA | PRA |
|---|---|---|
| | Firms will be required to prepare and keep up to date a written self-assessment of their compliance with the operational resilience requirements.<br>The regulators have confirmed that they do not plan to issue a template for the self-assessment document. | |
| Contents | The FCA has set out content requirements in SYSC15A.6.1R including:<br>• the important business services identified and the justification for the determinations made;<br>• their impact tolerances and justification for the level at which they have set them;<br>• their approach to mapping;<br>• their testing plan and justification for the plan adopted;<br>• details of the scenario testing they have carried out;<br>• any lessons learned exercises they have conducted. | The PRA identifies content requirements in Chapter 9 of SS1/21 including requiring firms to:<br>• list their important business services and state why each of these have been identified;<br>• specify the impact tolerances set for these important business services and why each impact tolerance has been set;<br>• detail their approach to mapping important business services, identifying the resources that contribute to the delivery of important business services and how firms have captured the relationships between these. Firms should also document how they have used mapping to identify vulnerabilities and to support testing activity.<br>• describe their strategy for testing their ability to deliver important business services within impact tolerances through severe but plausible scenarios. |
| Format | The FCA expects a firm's self-assessment document to be in a format that is clear and well-structured, it could be a text document, slide-deck or spreadsheet. It must accurately reflect the firm's operational resilience. | Similarly, the PRA leaves it up to individual firms to decide how the self-assessment document should be structured and the approach to creating it. |
| Submission expectations | Firms will need to provide the self-assessment documentation to the FCA on request or make it available for inspection as part of firm engagement. | The PRA will require firms to maintain and be able to provide the current version of their self-assessment to it on request from the 31 March 2022. |
| Review | The FCA will require firms to review and update their self-assessment document regularly. Where changes occur that may have a clear impact on the firm's operational resilience, such as structural changes, rapid expansion, poor trading or entry into new markets, firms will need to carry out more frequent reviews of the document. | The PRA will require firms to regularly update the self-assessment. |

| | FCA | PRA |
|---|---|---|
| **Governance and Senior Manager obligations** | The regulators expect boards and senior management to have a clear focus on their firms' operational resilience and be sufficiently engaged in setting effective operational resilience standards. Firms should ensure that board members and senior management have the knowledge, skills and experience needed to discharge the responsibilities allocated to them and the board should be in a position to provide constructive challenge to senior management as part of their oversight responsibilities. The board should ensure that it receives appropriate management information to inform operational resilience-related decision-making.<br><br>In terms of allocating responsibility for operational resilience, the regulators believe that it falls within the SMF24 function (Chief Operations Function). The FCA notes that a firm does not have an individual performing the SMF24 function, the firm must determine the most appropriate individual within the firm who is accountable for operational resilience.<br><br>The PRA notes that final sign off on the operational resilience policy should remain at board level. | |
| Board obligations | The FCA will require firms to ensure that their governing body approves and regularly reviews the self-assessment and lessons learned exercise documentation. | The PRA will require boards and senior management to:<br>• approve the important business services identified by their firm;<br>• approve the impact tolerances set by the firm;<br>• approve and regularly review the written self-assessment of their firms' compliance with the requirements;<br>• make investment decisions to enhance their firms' resilience. |

## How does the new operational resilience framework interact with PRA outsourcing requirements?

As the regulators set out in policy statements on the new operational resilience regime, firms' outsourcing, and other third-party arrangements can have a significant impact on their operational resilience. Regardless of any outsourcing or other third-party arrangements firms have in place, the regulators expect them to be operationally resilient. Firms should not allow their ability to deliver their important business services within their impact tolerances to be undermined by the use of such arrangements.

The PRA has published a policy statement (PS7/21) on the introduction of a new Supervisory Statement on outsourcing and third-party risk management (SS2/21), which is intended to complement the new operational resilience regime. SS2/21 reflects the increased importance to firms of cloud computing and other new technologies and the PRA intends affected firms to apply the provisions set out in SS2/21 in a proportionate manner depending on the materiality of any given outsourcing arrangement.

The PRA states that firms should meet these obligations in an appropriate manner, which will depend on various characteristics of the firm (such as its size) and its activities (such as the nature, scope and complexity of its activities). Outsourcing requirements should be applied in a proportionate manner, which relates to the systemic importance of the firm itself. The PRA also notes that the materiality of the outsourcing arrangements should also be considered and explains that the materiality of an arrangement relates to the potential impact of the failure on an arrangement on the firm. An arrangement can be considered material if the failure of such an arrangement would affect a firm’s safety and soundness, including: its operational resilience; its ability to comply with legal and regulatory obligations; the risk that firms’ ability to meet these obligations could be compromised if the arrangement is not subject to appropriate controls and oversight.

We have set out key points from SS2/21 on the next page.

# PRA outsourcing requirements

| | |
|---|---|
| **Before entering into arrangement, firms should:** | • determine the materiality of every outsourcing and third-party arrangement;<br>• perform appropriate and proportionate due diligence on all potential service providers;<br>• assess the risks of every outsourcing arrangement irrespective of materiality;<br>• notify the PRA of the material outsourcing arrangement in line with Notifications 2.3(1)(e);<br>• consider notifying the PRA of material non-outsourcing third party arrangements under Fundamental Rule 7. |
| **Determining materiality**<br><br>Please note that the concept of materiality itself and the PRA criteria apply to all third-party arrangements. Firms should determine the materiality of all third-party arrangements using all relevant criteria in chapter 5 of SS2/21 | An outsourcing or third-party arrangement will be considered material if the failure of the arrangement could materially impair the:<br>• financial stability of the UK;<br>• firms' ability to meet the Threshold Conditions;<br>• compliance with the Fundamental Rules; requirements under 'relevant legislation' and the PRA Rulebook;<br>• safety and soundness;<br>• Operational Continuity In Resolution and if applicable, resolvability.<br><br>Further, an outsourcing arrangement will be regarded as 'material' if the service being outsourced involves an 'entire 'regulated activity'' (for example portfolio management) or an "internal control or key function". |
| **Timing and frequency of materiality assessments**<br><br>Firms are responsible for assessing the materiality of their outsourcing and third-party arrangements. | Materiality may vary throughout the duration of an arrangement and should therefore be (re)assessed:<br>• prior to signing the written agreement;<br>• at appropriate intervals thereafter, e.g., during scheduled review periods;<br>• where a firm plans to scale up its use or dependency on the service provider; and / or<br>• if a significant organisational change at the service provider or a material sub-outsourced service provider takes place that could materially change the risks inherent in the outsourcing arrangement. |
| **Sub outsourcing**<br><br>This is where the service provider under an outsourcing arrangement further transfers the function to another service provider. This can increase certain risks, such as making it harder for the firm to manage the risks of the original outsourcing arrangement. | Firms must assess the relevant risks of sub-outsourcing before they enter into an outsourcing agreement. Firms should have visibility of the supply chain, and service providers should facilitate this by maintaining up-to-date lists of their sub-outsourced service providers.<br><br>Firms should ensure that the service provider has the ability and capacity on an ongoing basis to appropriately oversee any material sub-outsourcing in line with the firm's relevant policies.<br><br>Any sub-outsourcing should only be permitted in accordance with the written agreement for the original outsourcing arrangement in order to allow the firm to manage its risks appropriately. |



*Continued on next page*

| | |
|---|---|
| **Negotiating with suppliers where there is an imbalance of power** | An imbalanced negotiating position between a firm and an outsourced service provider in a material outsourcing arrangement is not a sufficient reason for a firm to accept terms which do not allow the firm to meet its regulatory obligations. If a service provider is unable or unwilling to contractually facilitate a firm's compliance with its regulatory obligations firms should make the PRA aware of this. |
| **Exit plans**<br><br>for both stressed and non-stressed exits should be maintained by firms. | For each material outsourcing arrangement, the PRA expects firms to develop, maintain, and test a:<br><br>• business continuity plan; and<br><br>• documented exit strategy, which should cover and differentiate between situations where a firm exits an outsourcing agreement:<br><br>o in stressed circumstances, (eg, following the failure or insolvency of the service provider (stressed exit)); and<br><br>o through a planned and managed exit due to commercial, performance, or strategic reasons (non-stressed exit).<br><br>***Stressed exit***<br><br>Firms' exit plans should cover stressed exits and be appropriately documented and tested as far as possible. These plans should provide a last resort risk mitigation strategy in the event of disruption that cannot be managed through other business continuity measures, including for example the insolvency of a service provider.<br><br>The PRA does not prescribe or have a preferred form of exit in stressed scenarios. Its focus is on the outcome of the exit, (i.e., the continued provision by the firm of important business services provided or supported by third parties), rather than the method by which it is achieved, although the PRA does suggest that firms could consider bringing services back in-house in such cases. |
| **Transition arrangements** | SS2/21 applies as of 31 March 2022. The PRA expects that any outsourcing arrangements entered into after 31 March 2021 to be compliant with the SS2/21. However, the PRA has given firms additional time to update pre-existing arrangements. Such arrangements should be at the first appropriate contractual review point so that they can be consistent with SS2/21 as soon as possible on or after 31 March 2022. |

## What firms should be doing now?

As we come to end of the implementation period, firms should be finalising their change projects.

At the end of January 2022, a FCA webinar on Operational Resilience the FCA flagged the importance of firms documenting the operational resilience plans. In particular the FCA noted that each important business services should have a distinct justification as to what made the services an important business service. In addition, the FCA highlighted the value of using metrics as part of this justification, so if firms have data on customer numbers, transaction volumes etc these should be reviewed and included in the justification.

The FCA also stressed that at this point one of the main objectives of the mapping exercise that firms should have carried out is to highlight vulnerabilities in a firm's business processes. These gaps do not need to be remediated by 31 March 2022, but firms should have identified any vulnerabilities and have plans to address such vulnerabilities. The FCA has noted that it does not intend to carry out a mass review of the firms' operational resilience documentation, though it will start requesting copies of the self-assessment document from 1 April 2022. The FCA confirmed that it will automatically request such documentation in the aftermath of any disruption incident.

Firms should be ensuring that senior management and the board are thoroughly briefed and should have approved (or be in a position to approve before 31 March 2022) the self-assessment document.

## Next steps

Operational Resilience does not end on the 31 March 2022, as firms will be entering a three-year transition period during which firms will be further developing their operational resilience including developing more sophisticated mapping processes and scenario testing and carrying out appropriate lessons learned exercises.

In addition, the PRA is planning a further consultation on operational resilience incident reporting in the first half of this year.

# Authors

**Grania Baird**
Partner

Email Grania
+44(0)20 3375 7443

**Andy Peterkin**
Partner

Email Andy
+44 (0)20 3375 7435

**Fiona Lowrie**
Consultant

Email Fiona
+44(0)20 3375 7515

F&
Co

Farrer & Co LLP
66 Lincoln’s Inn Fields
London WC2A 3LH

+44(0)20 3375 7000
enquiries@farrer.co.uk
www.farrer.co.uk