ADDLESHAW GODDARD

OPERATIONAL RESILIENCE, OUTSOURCING AND THIRD PARTY RISK MANAGEMENT POLICIES FINALISED: CLARITY FOR FIRMS ON THE ROAD AHEAD

UK regulators have finalised their operational resilience policies, giving firms a clear picture of implementation timeframes for achieving compliance. Useful changes and clarifications have been made in the final policy, including changes to key concepts and better alignment with existing domestic requirements and with existing or forthcoming international standards and guidelines. However, some areas of difficulty remain. In this briefing we highlight some of the challenges ahead for firms.

FINALISED POLICY

On 29 March 2021 the FCA and PRA released their finalised policy statements[1], near final rules[2], and, in the case of the PRA, a supervisory statement[3] and statement of policy[4] on operational resilience. The PRA has also released its finalised policy[5] and supervisory statement[6] on outsourcing and third party risk management. The regulatory objective is that firms will strengthen their overall resilience by:

- identifying their important business services (**IBS**) by considering how disruption to them can have impacts beyond their own commercial interests;
- mapping their IBS with a view to identifying vulnerabilities and remedying these as appropriate, and enabling firms to conduct scenario testing;
- setting a tolerance for disruption for each IBS (an **impact tolerance**); and
- ensuring they can continue to deliver their IBS and are able to remain within their impact tolerances during '*severe but plausible*' scenarios.

1 FCA https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf
PRA https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2021/march/ps621.pdf

2 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2021/march/ps621app1.pdf

3 PRAhttps://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss121-march-21.pdf

4 PRA https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-sop

5 PRAhttps://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2021/march/ps721.pdf

6 PRAhttps://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf

The finalised regulatory framework has been a coordinated effort, with each regulator setting policy in line with their statutory objectives. The Bank of England has separately published a finalised operational resilience policy applicable to financial market infrastructures.

Firms should note two key dates:

- **31 March 2022** – firms should have mapped their IBS, set impact tolerances for those IBS and commenced a programme of scenario testing; and

- **31 March 2025** (and on an ongoing basis from that date) – a hard deadline, by which all firms should have sound, effective, and comprehensive strategies, processes, and systems that enable them to address risks to their ability to remain within their impact tolerance for each IBS in the event of a severe but plausible disruption.

WELCOME CHANGES AND CLARIFICATIONS

Following consultation responses, both regulators have made a number of changes and clarifications in their finalised policy. Notably, they have taken note of the persistent feedback that there should not be divergence or duplication in the FCA's and PRA's regulatory and supervisory approaches, and confirm in the final policy that work done to meet the requirements of one regulator can and should be leveraged to meet those of the others. The regulators have also committed to carry this approach through with collaborative supervision.

Other welcome clarifications include:

1 **Alignment of definitions** – there was feedback that the inconsistencies in terminology used by the FCA and PRA at consultation stage caused unnecessary confusion. The regulators have clarified and amended some definitions including those of important business services and impact tolerance to ensure alignment of terminology where this is possible (subject to the constraints of the regulators' individual objectives).

2 **Important Business Services** – clarifications have been made including the extent to which internal services and central shared services – which can largely be viewed as only enablers of IBS – may need to be categorised as an IBS in their own right, and the frequency with which a firm's IBS should be reviewed. More guidance has also been provided on what constitutes a *'significant/material*' change that would trigger a review of IBS. Consultation feedback highlighted the need for greater clarity on the level of granularity firms should use to identify and map their IBS. The regulators have resisted creating lists of IBS but have provided some further guidance and examples including, in relation to treatment of vulnerable customers, the approach to IBS where only a small number of customers would be adversely affected by disruption, and how firms should take into account disruptions that impact multiple IBS. The PRA has also clarified and provided an example of important group business services.

3 **Impact Tolerance** – Following comments from consultation respondents, the PRA and FCA have reviewed their respective definitions of impact tolerance to improve consistency and clarity for firms. In response to feedback on how small firms may find it challenging to set impact tolerances for financial stability, the PRA, in the interests of proportionality, is narrowing the scope of its rules to exclude smaller firms from the requirement.

One of the most difficult aspects of the regime is the position of dual-regulated firms, who under the proposals will be required to set up to two impact tolerances to meet the requirements of the FCA and the PRA. The regulators have retained this requirement, but make clear that a firm may in fact choose to set the impact tolerance at the same point for both the FCA and PRA if

this can be justified. Moreover, if a disruption to an IBS was, for example, only to result in consumer harm, then a PRA impact tolerance may not need to be set for that IBS. The PRA has provided examples to illustrate where the impact tolerances between the PRA and FCA would differ, and how firms can demonstrate that they have the recovery and response arrangements that would allow them to remain within both their shorter and longer impact tolerances. The FCA has provided guidance on factors to consider when setting impact tolerances in relation to vulnerable customers.

Despite consultation feedback questioning its appropriateness, the regulators have decided to maintain as mandatory the use of a time-based metric for the setting of impact tolerances, but explain that this could be a number of hours/days or a point in time, such as the end of the day, in conjunction with other appropriate metrics, for example, a certain volume of interrupted transactions. Other metrics that might be used in conjunction with the time-based metric could include: cost, scale, key business process, potential value of market impact, materiality (i.e. business/customer impact), volumes (e.g. data volume, transaction/account volume), type of transaction, number of customers affected, and the nature of the consumer base.

4 **Mapping and scenario testing** – In response to consultation feedback on the difficulty and resource-intensiveness of mapping and testing, the regulators have reduced the scope of mapping and testing that needs to be done by the first deadline of 31 March 2022 to give firms the flexibility to implement scenario testing proportionately through the initial phase. Both regulators emphasise that mapping and testing need not be done to the "full level of sophistication" by that date. Firms need only to have performed mapping and testing to the level of sophistication necessary to accurately identify their IBS, set impact tolerances and identify any vulnerabilities in their operational resilience. Firms will not be expected to have performed scenario testing of every IBS by this date. The regulators do however expect firms to endeavour to carry out full mapping as soon as reasonably practicable. Both regulators have clarified that the requirement for 'regular' scenario testing does not automatically mean that all scenario testing must be repeated annually. Instead, firms are required to scenario test when there is a material change to the firm's business, to an IBS or to impact tolerances, or following improvements made by the firm in response to a previous test.

5 **Scope** – The FCA has made some changes to its policy wording to clarify: (i) that third country branches are not within the scope of the FCA rules; and (ii) its expectations with respect to firms who would be outside the scope of the policy but for their permissions under the Payment Services Regulations 2017 or the Electronic Money Regulations 2011.

6 **Interaction with domestic and international frameworks** – A key issue raised by consultation respondents was that the finalised UK operational resilience policy must align domestically and internationally. The regulators have provided very useful clarification on alignment, interaction and interplay of operational resilience requirements with:

- ***domestic frameworks***: Business Continuity Planning (BCP), Recovery and Resolution Planning (RRP), Operational Continuity in Resolution requirements (OCIR), the Bank of England's Resolution Assessment Framework, Operational Risk Management, Cyber Risk Management;

- ***EU frameworks***: EBA Guidelines on (i) ICT and Security Risk Management (ii) Outsourcing Arrangements; ESMA and EIOPA Guidelines on Outsourcing to Cloud Service Providers; European Commission's proposed Digital Operational Resilience Act (DORA);

- ***International frameworks***: BCBS' recently finalised Principles for Operational Resilience, International Organization of Securities Commission's (IOSCO's) Principles on Outsourcing.

The guidance emphasises that operational resilience requires firms to take a holistic approach to overall resilience and that the requirements are intended to complement rather than supplant other requirements in the regulatory ecosystem. Firms can therefore leverage work done to meet other UK regulatory requirements towards achieving their operational resilience compliance. So for example, the PRA encourages firms to integrate impact tolerances into their existing approaches where they are suitable for meeting the requirements and expectations of the policy. This means that firms may look to existing tools such as Business Impact Analysis (BIA) to identify their impact tolerances. Firms may also wish to link their operational resilience scenario testing with existing approaches to testing, including reference to the Guidelines on ICT and Security Risk Management, BCP, operational risk testing, capital provisioning and stress testing for OCIR.

AREAS WHERE FURTHER GUIDANCE AND CLARIFICATION WILL NOT BE FORTHCOMING IN THE NEAR TERM

1 **Severe but plausible 'scenarios'** – The regulators have not provided a definition or further guidance on what constitutes a severe but plausible scenario, on the footing that the nature and severity of scenarios appropriate for firms to use may vary according to their size and complexity. Nor does the PRA intend at this stage to introduce an 'incident library' to record scenarios experienced by firms, although it may consider doing so in the future. The regulators envisage that best practice will emerge over time. This is an area where we consider that trade associations may play a useful role.

2 **Self-assessment templates** – Firms must document a self-assessment which must set out a summary of the vulnerabilities they have identified to the delivery of their important business services and an outline of the scenario testing performed and the findings from the tests, including any lessons learned. This document need not be submitted to the regulators but must be provided on request. The regulators have resisted calls to set out templates for the self-assessment document. The expectation is that this will be a bespoke document, and there is no prescription in the finalised policy as to its content or format. In light of this firms should structure the self-assessment document to suite their own internal purposes, to promote the need for effective project management, and to ensure that the firm's decisions and approaches can be understood by senior management.

3 **Governance** – The regulators have confirmed that they do not consider it appropriate for the approval of the mapping exercise to be delegated to individuals below Board level. The regulators also do not consider that responsibility for a firm's operational resilience oversight should be allocated to SMFs other than the SMF24, and have confirmed their initial view that sign-off of the firm's operational resilience strategy is a responsibility of sufficient materiality that it must be allocated to the Board.

4 **Application of PRA operational resilience to holding companies** – The PRA is currently monitoring the progress of the Financial Services Bill through Parliament. Once the Bill has received Royal Assent, the PRA will consider whether PRA operational resilience rules should be applied to holding companies.

OUTSOURCING AND THE USE OF THIRD PARTIES

The finalised policy requires firms to map their IBS and test their ability to remain within impact tolerances to build operational resilience, and this requirement applies irrespective of whether the IBS

is outsourced or not or the services are provided wholly or partly by a third party. Firms that enter into outsourcing or third party arrangements remain fully accountable for complying with all their regulatory obligations.

The key issue for firms is that they will need to gain assurance that outsourcing or other third party arrangements would not create a vulnerability in meeting the firm's impact tolerances. Mapping and testing on third parties is necessary for the firm and its supervisor to obtain an accurate understanding of the firm's operational resilience. The regulators clarify in their finalised policy that, as part of their assurance work, firms may ask third parties to provide mapping or scenario testing data but this is not required in all cases, particularly if other assurance mechanisms are effective and more proportionate. However, there may be scenarios where a third party refuses to provide mapping or scenario testing data and there are no other assurance mechanisms that the firm could fall back on. Similarly, as raised by some respondents, third party suppliers may be reluctant or slow to take the necessary actions for firms to comply with the policy, particularly where firms have low negotiating power with large suppliers. The regulators will supervise these requirements proportionately. They also consider that clarification of firms' expectations of suppliers will enable suppliers to understand the constraints firms are operating under when agreeing contract terms, and thus improve the negotiating position for firms over time.

The PRA's Supervisory Statement (SS1/21) on Operational Resilience cross refers to its related Supervisory Statement (SS2/21) on Outsourcing and Third Party Risk Management, which integrates the existing EBA Guidelines on outsourcing arrangements (**EBA Outsourcing Guidelines**) into the UK regime. This is relevant for firms that have been undertaking remediation of contracts in line with the EBA Outsourcing Guidelines. We have noted below some key points of interest from a contractual perspective arising from the PRA's Policy Statement (PS7/21) and Supervisory Statement (SS2/21) on Outsourcing and Third Party Risk Management.

1 Remediation timescales

The PRA has helpfully clarified that it no longer thinks it is proportionate for firms to make every effort to comply with the remediation timeline in the EBA Outsourcing Guidelines (i.e. by 31 December 2021) and that firms are not expected to inform the PRA if they have not met that timeline. Instead, firms are expected to comply with the expectations in SS2/21 by 31 March 2022 – in particular:

- outsourcing arrangements entered into on or after 31 March 2021 should meet the expectations in SS 2/21 **by 31 March 2022**;
- firms should seek to review and update legacy outsourcing agreements entered into before 31 March 2021 at the first appropriate contractual renewal or revision point to meet expectations **as soon as possible on or after 31 March 2022**.

2 Negotiation challenges

Overall, the PRA has indicated that it decided not to reduce expectations in response to comments on the challenges of negotiating outsourcing agreements. The PRA considers that the imbalance in contractual power between a small firm and a dominant provider should not be considered justification for a firm to accept clauses that do not meet legal or regulatory expectations. That said, the PRA has made a number of helpful comments and differentiations from the EBA Outsourcing Guidelines in some of the most challenging areas – for example:

(a) **Termination rights**

The PRA has clarified, in the interests of proportionality and pragmatism, that firms may elect to limit contractual termination rights to situations where the breaches of law, regulation or contractual provisions are material, not expediently remediated, or create risks beyond a firm's tolerance. This is a helpful clarification in the context of the challenging termination rights in paragraph 98 of the EBA Outsourcing Guidelines and will give firms more flexibility to agree termination rights which are closer to current market standard.

(b) **Audit**

The PRA has acknowledged that certain types of onsite audit may create an unmanageable risk for the environment of the provider or its other clients. In such cases, the firm and service provider may agree alternative ways to provide an equivalent level of assurance (e.g. specific controls to be tested in a report or certification). For material outsourcing arrangements, the firm should inform their supervisor if alternative means of assurance have been agreed. However, the PRA expects that the firm should still retain their underlying contractual right to conduct an onsite audit, which will be a challenge, though providers might be comforted that this is a back-up right to be used only when alternatives do not provide adequate assurance.

(c) **Penetrating testing**

In light of the challenges of expecting firms to conduct their own penetration testing, the PRA has amended SS2/21 to clarify that access, audit and information rights in material outsourcing agreements should include, where relevant, the results of security penetration testing undertaken by the supplier. This is more in line with what suppliers are willing to provide.

(d) **Sub-outsourcing**

The PRA has amended SS2/21 to clarify that the detailed expectations on sub-outsourcing only apply to material sub-outsourcing, meaning that challenging flow-down requirements are not applicable to non-material sub-outsourcings. Further, the PRA has clarified that it does not expect firms to monitor the provider's downstream sub-contractors directly, although firms should consider the potential impact of large, complex sub-outsourcing chains on their operational resilience and their ability to oversee and monitor the effectiveness of those chains.

(e) **Notification**

The PRA has recognised that firms may need to secure specific contractual arrangements with third parties to meet the PRA's expectations and so has introduced a new expectation that the firm should make the PRA aware if a third party service provider to a proposed material outsourcing arrangement is unable or unwilling to include certain contractual terms which reflect the firm's obligations. This emphasises the importance of re-assessing what gaps there are following the negotiation process and allowing sufficient time to inform and engage with the PRA as needed.

3 Scope

SS2/21 has removed the expectation that arrangements performed or provided in a prudential context fall within the definition of outsourcing (which had blurred the distinction between

outsourcing and other third party arrangements). Instead, firms should assess the materiality and risks of all third party arrangements, irrespective of whether they fall within the definition of outsourcing. This emphasises that the PRA is taking a more holistic approach, expecting firms to attach greater importance to the risks that outsourcing and third party arrangements create, rather than following a narrow definitional approach.

Where a non-outsourcing third party arrangement is "material" or "high risk", the firm should implement proportionate, risk-based, suitable controls. This is in line with the approach many firms have been taking in any event (on the basis that many of the outsourcing requirements are general good practice) and SS2/21 is clear that the controls do not necessarily have to be the same as those that apply to outsourcing arrangements, which does provide some flexibility. However, the controls should be appropriate to the materiality and risks of the third party arrangement and as robust as the controls that would apply to outsourcing arrangements with an equivalent level of materiality or risk i.e. firms should apply stricter controls to material, non-outsourcing third party arrangements than to non-material outsourcing arrangements.

As part of their contracting process, firms might find it helpful to use checklists for non-outsourcing third party arrangements (in a similar way to outsourcing arrangements) to ensure that appropriate contractual protections are included in the context of the materiality categorisation and risk assessment.

CONCLUSION

UK regulators should be applauded for the extra guidance they have given, and for listening to many of the concerns of industry. Firms' thoughts will now turn to implementation. For some – large firms with numerous business and service lines and cross-jurisdictional operations – it will be essential to control complexity. All should have in mind the injunction from the regulators that this is an issue for the Board – this, it is to be hoped, should ensure that firms do not lose sight of proportionality and will continue to generate management information which is accurate and meaningful through the life of what may be an enormous programme of work.

We see also a crucial role for trade associations, and believe that, through them, regulators might be persuaded to provide extra guidance and positioning on regulatory expectations in areas where, to date, they have been reluctant to accommodate.

CONTACTS

STEVEN FRANCIS
Partner
+44(0)207 160 3949
steven.francis
@addleshawgoddard.com

SARA EVANS
Principal Knowledge Lawyer
+44(0)207 160 3045
sara.evans
@addleshawgoddard.com

FIONA GHOSH
Partner
+44(0)207 788 5120
fiona.ghosh
@addleshawgoddard.com

PRISCILLA HETHERTON
Managing Associate
+44(0)113 209 2215
priscilla.hetherton
@addleshawgoddard.com

LORNA FINLAYSON
Partner
+44(0)131 222 9579
lorna.finlayson
@addleshawgoddard.com

SIMON LOFTHOUSE
Partner
+44(0)113 209 7732
simon.lofthouse
@addleshawgoddard.com

SARAH HERBERT
Compliance Director
(Non-Lawyer)
+44(0)207 160 3429
sarah.herbert
@addleshawgoddard.com

MICHAEL LOWRY
Partner
+44(0)207 880 5712
michael.lowry
@addleshawgoddard.com

NIKESH SHAH
Senior Compliance Manager
+44(0)207 160 3372
nikesh.shah
@addleshawgoddard.com

EMMA PITCHER
Assistant Team Leader
+44(0)161 934 6834
emma.pitcher
@addleshawgoddard.com

MICHAEL KENNEDY
Associate
+44(0)161 934 6269
michael.kennedy
@addleshawgoddard.com