BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Publication

Statement of Policy

Operational resilience

March 2021

BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Statement of Policy

Operational resilience

March 2021

Prudential Regulation Authority | 20 Moorgate | London EC2R 6DA

Contents

1 Introduction

1.1 This Statement of Policy (SoP) is relevant to all:

- UK banks, building societies, and PRA-designated investment firms (hereafter banks); and
- UK Solvency II firms, the Society of Lloyd's, and its managing agents (hereafter insurers).

1.2 Banks and insurers are collectively referred to as 'firms'.

1.3 The Prudential Regulation Authority (PRA) considers that for firms to be operationally resilient, they should be able to prevent disruption occurring to the extent practicable; adapt systems and processes to continue to provide services and functions in the event of an incident; return to normal running promptly when a disruption is over; and learn and evolve from both incidents and near misses. Therefore, operational resilience is an outcome that is supported by several parts of the PRA's regulatory framework.[1]

1.4 The Operational Resilience Parts of the PRA Rulebook[2] and SS1/21 'Operational resilience: Impact tolerances for important business services'[3] respectively require and expect firms to identify important business services and set impact tolerances for these services. Firms must take action to ensure they are able to deliver their important business services[4] within their impact tolerances.[5] Testing against severe but plausible operational disruption scenarios enables firms to identify vulnerabilities and take mitigating action. The PRA's operational resilience policy requires boards and senior management to drive improvement where deficiencies are found.

1.5 The context of important business services and impact tolerances influences the PRA's approach to other parts of the PRA's regulatory framework as well. This SoP sets out how the PRA implements a consistent and targeted approach across its regulatory framework.

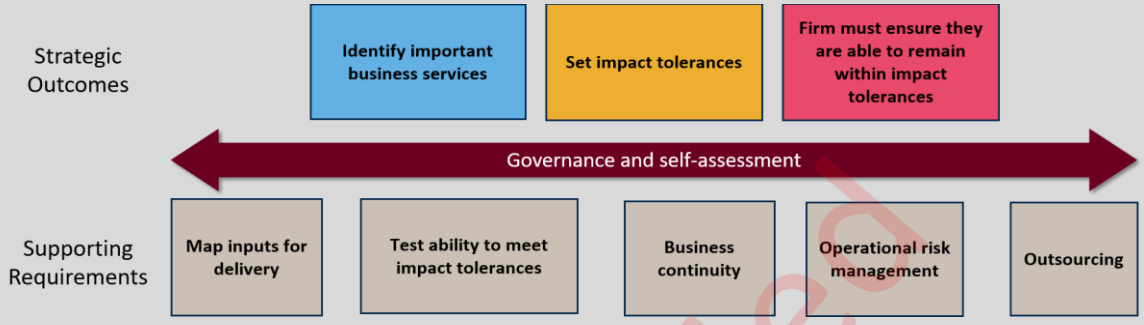
1.6 The SoP clarifies how the PRA's operational resilience policy affects its approach to four key areas of the regulatory framework in particular (the relationship between these policies is depicted in Figure 1 below):

- governance;
- operational risk management;
- business continuity planning (BCP); and
- the management of outsourced relationships.

1 As explained in PRA DP1/18 'Building the UK financial sector's operational resilience', p.8: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.
2 Operational Resilience – CRR Firms; Operational Resilience – Solvency II Firms; and Chapter 22 in the Group Supervision Part of the PRA Rulebook.
3 March 2021: https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-impact-tolerances-for-important-business-services-ss.
4 'Important business service' as described in Chapter 2 of SS1/21.
5 'Impact tolerance' as described in Chapter 3 of SS1/21.

1.7 There is a valuable set of other relevant existing policies and guidelines (eg the European Banking Authority's (EBA's) guidelines on information and communication technology (ICT) risks, and the EBA's guidelines on ICT and security risk management).[6] The PRA considers all of its policies and relevant international guidelines in the context of its operational resilience policy, not just those outlined here. The PRA's operational resilience policy will complement existing policies and is not intended to conflict with or amend them.

Figure 1: The relationship between the PRA's operational resilience policy with other key areas of the PRA's regulatory framework



The framework of: identifying important business services; setting impact tolerances; and taking actions to be able to remain within impact tolerances set the strategic direction that the PRA expect firms to take. To achieve the strategy, firms must:

- map resources;
- test their ability to remain within impact tolerances;
- implement BCP requirements;
- implement operational risk management requirements; and
- implement outsourcing requirements.

Governance is an inherent part of each of the above elements, and self-assessment looks at how all of these elements combine to build the resilience of a firm.

6 Unless otherwise stated, any references to EU or EU derived legislation refer to the version of that legislation which forms part of retained EU law. See Appendix 2 of the SoP 'Interpretation of EU Guidelines and Recommendations: Bank of England and PRA approach after the UK's withdrawal from the EU': https://www.bankofengland.co.uk/-/media/boe/files/paper/2019/interpretation-of-eu-guidelines-and-recommendations-boe-and-pra-approach-sop-december-2020.pdf.

2 The relationship between operational resilience and governance

2.1 The role of firms' boards and senior management is central to the PRA's operational resilience policy. Boards are accountable for, and should approve, the identification of their firm's important business services, impact tolerances, and self-assessment.

2.2 The ability of firms to deliver their important business services within their impact tolerances depends upon appropriate reporting and accountability to be in place throughout the firm. Where limitations are identified, leadership from the firms' board and senior management is essential to prioritise the investment and cultural change required to improve operational resilience.

Interaction with other board responsibilities

2.3 The PRA considers whether firms are delivering the outcome of operational resilience when assessing the adequacy of a firm's arrangements to deliver other expectations of boards. When the PRA considers its expectations for boards in its operational resilience policy and elsewhere in its regulatory framework, it considers, for example, if boards:

- have appropriate management information available to inform decisions which have consequences for operational resilience;
- have adequate knowledge, skills, and experience in order to provide constructive challenge to senior management and meet their oversight responsibilities in relation to operational resilience; and
- articulate and maintain a culture of risk awareness and ethical behaviour for the entire organisation, which influences the firm's operational resilience.

Interaction with other management responsibilities

2.4 The Chief Operations Senior Management Function (SMF) 24, where it applies, includes responsibility for the firm's operational resilience. The PRA's operational resilience policy provides further detail to firms on this responsibility.

3 The relationship between operational resilience and operational risk policy

3.1 Operational risk management supports both operational resilience and financial resilience. Firms should have effective risk management systems in place to manage operational risks that are integrated into their organisational structures and decision-making processes.[7]

3.2 When assessing a firm's operational risk management, the PRA considers the extent to which firms: have reduced the likelihood of operational incidents occurring; can limit losses in the event of severe business disruption; and whether they hold sufficient capital to mitigate the impact when operational risks crystallise.

3.3 The additional requirements the PRA's operational resilience policy places on firms to limit the impact of disruptions when they occur, whatever their cause, develops the PRA's approach to operational risk in two key ways:

7 Directive 2013/36/EU (Article 85(1)). Solvency II Directive (Article 44).

- it increases firms' focus on their ability to respond to and recover from disruptions, assuming failures will occur; and

- it addresses the risk that firms may not necessarily consider the public interest when making investment decisions to build their operational resilience. The PRA's operational resilience policy requires firms to take action so they are able to provide their important business services within their impact tolerances through severe but plausible disruptions.

Risk appetite and impact tolerances

3.4 Impact tolerances differ from risk appetites in that they assume a particular risk has crystallised instead of focusing on the likelihood and impact of operational risks occurring. Firms that are able to remain within their impact tolerances increase their capability to survive severe but plausible disruptions, but risk appetites are likely to be exceeded in these scenarios (see Figure 2 below). Impact tolerances are set only in relation to impact on financial stability, the firm's safety and soundness and, in the case of insurers, the appropriate degree of policyholder protection.

Figure 2: The relationship between risk appetite and impact tolerance

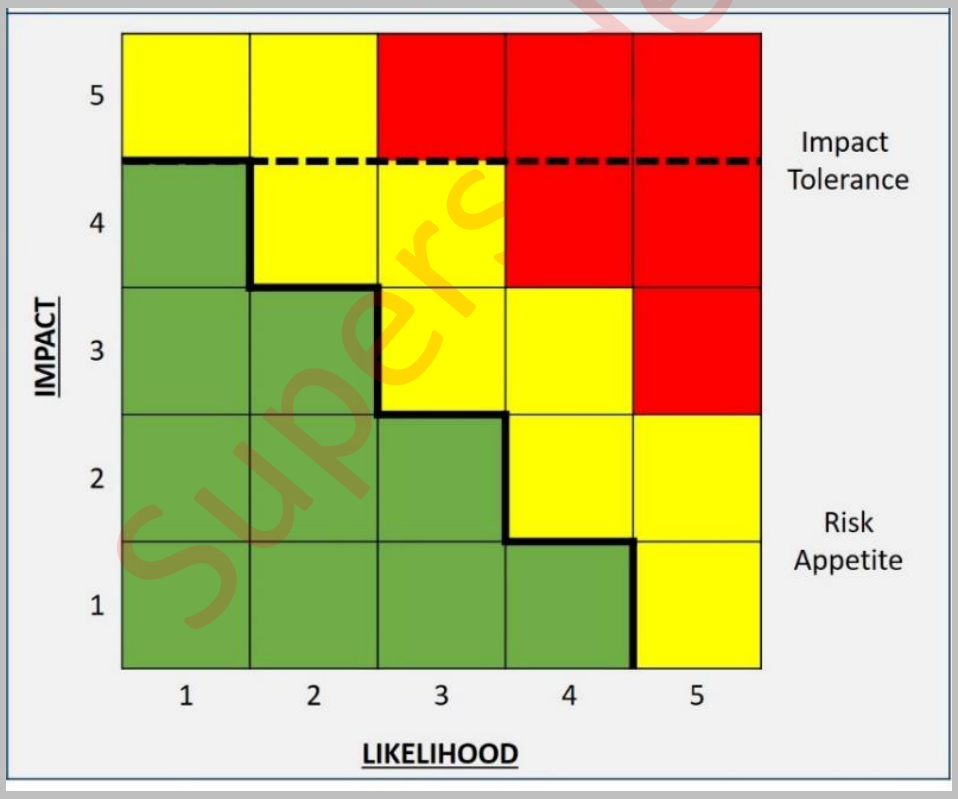


Figure 2 shows the relationship between impact and likelihood for a firm's risk appetite and impact tolerance. Both risk appetite and impact tolerances help ensure a firm's operational resilience.

- The thick solid line represents the risk appetite, which changes with impact and likelihood. Green, yellow, and red illustrate the firm's appetite towards disruption at different levels of impact and likelihood (green is within the firm's risk appetite, yellow is outside of the firm's risk appetite, and red is significantly outside of the firm's risk appetite).
- The dashed dark line represents the impact tolerance, which is set at a high level of impact and assumes disruption has occurred, so is indifferent to likelihood. The green, yellow, and red are not related to the impact tolerance.

Financial resilience

3.5 Firms are required to hold capital to ensure they can absorb losses resulting from operational risks such as fraud, damage to physical resources, or business disruption and system failures.[8] However, the PRA's operational resilience policy does not have an associated capital requirement. As such, it does not affect the PRA's approach to operational risk capital policy or add additional considerations for firms when they make capital calculations.

Incident management

3.6 In the PRA's general notification rules[9] firms are required to notify the PRA where an incident: could lead to the firm failing to satisfy one or more of the threshold conditions; could have a significant adverse impact on the firm's reputation; could impact the firm's ability to continue to provide adequate services to its customers; or could result in serious financial consequences to the UK's wider financial sector or to other firms.

3.7 The PRA considers whether a firm has met the PRA's notification requirements alongside the PRA's expectations in its operational resilience policy. For example the PRA expects incidents to meet the test for notification if the incident would disrupt the firm's ability to deliver its important business services within its impact tolerances. This includes incidents which have occurred, may have occurred or may occur in the foreseeable future.

4 The relationship between operational resilience and Business Continuity Planning (BCP)

4.1 The PRA requires a bank to 'have in place adequate contingency and business continuity plans aimed at ensuring that in the case of a severe business disruption the firm is able to operate on an ongoing basis and that any losses are limited'.[10] Similarly, an insurer is required to 'take reasonable steps to ensure continuity and regularity in the performance of its activities, including the development of contingency plans'.[11] These requirements and the PRA's operational resilience policy contribute to firms' response and recovery capabilities.

4.2 BCP policies and the PRA's operational resilience policy are closely linked. However, the PRA's operational resilience policy focuses on a firm's ability to deliver its important business services rather than single points of failure. The PRA considers both policies together when supervising firms. For example, when assessing whether banks are meeting the PRA's expectations in SS21/15 'Internal governance',[12] the PRA considers if banks':

- recovery priorities for their operations[13] prioritise the delivery of important business services within impact tolerances;

- allocation of resources and communications planning for business continuity planning focuses on the delivery of important business services; and

8 CRR Firms – Internal Capital Adequacy Assessment 10.1 (for banks), for insurers Solvency Capital Requirement – General Provisions 3.3 (for insurers).
9 Rule 2.1 in the Notifications Part of the PRA Rulebook.
10 CRR Firms – Internal Capital Adequacy Assessment 10.2.
11 Rule 2.6 in the Solvency II Firms – Conditions Governing Business Part of the PRA Rulebook.
12 April 2017: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/internal-governance-ss.
13 Paragraph 2.1(b), SS21/15.

- tests of business continuity plans complement the testing of disruption scenarios and relate to impact tolerances.

5 The relationship between operational resilience and outsourcing

5.1 As set out in the PRA's outsourcing rules,[14] firms remain responsible for their obligations when functions are outsourced to a third party. In the PRA's operational resilience policy, the PRA expects firms to be operationally resilient regardless of any outsourcing arrangements or use of third parties. Firms should not allow their ability to deliver their important business services within their impact tolerances to be undermined when they are delivered wholly or in part by third parties, whether these third parties are other entities within their group or external providers.

5.2 The PRA's policy for modernising the regulatory framework on outsourcing and third party risk management (SS2/21 'Outsourcing and third party risk management')[15] complements the PRA's operational resilience policy. SS2/21 reflects the increased importance to firms of cloud computing and other new technologies. The PRA's approach is to consider SS2/21 and the PRA's operational resilience policy in combination.

14 CRR Firms – Outsourcing, Solvency II Firms – Conditions Governing Business 7.
15 March 2021: https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss.