BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Publication

Supervisory Statement | SS1/21

Operational resilience: Impact tolerances for important business services

March 2022

(Updating March 2021)

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Supervisory Statement | SS1/21

Operational resilience: Impact tolerances for important business services

March 2022

Prudential Regulation Authority | 20 Moorgate | London EC2R 6DA

Contents

1 Introduction

1.1 This Supervisory Statement (SS) sets out the Prudential Regulation Authority's (PRA) expectations for the operational resilience of firms' important business services, for which they are required to set impact tolerances. The policy objective is to improve the resilience to operational disruptions of both firms and the wider financial sector.

1.2 The policy addresses risks to operational resilience from the interconnectedness of the financial system and the complex and dynamic environment in which firms operate. The PRA considers that there is a need for a proportionate minimum standard of operational resilience that incentivises firms and, where relevant, their groups to prepare for disruptions and to invest where needed. Disruptions can affect firms' safety and soundness, undermine policyholder protection, and, in some cases, affect financial stability.

1.3 This SS is relevant to all:

- UK banks, building societies, PRA-designated investment firms (hereafter banks), and CRR consolidation entities; and

- UK Solvency II firms, the Society of Lloyd's, and its managing agents (hereafter insurers).

1.4 Banks and insurers are collectively referred to as 'firms' in this SS. In chapter 9, where those expectations relate to a banking group, the term 'CRR consolidation entity' is used; where those expectations refer to an insurance group, the term 'insurer' is used.

1.5 Operational resilience in this SS refers to the ability of firms, their groups, and the financial sector as a whole to prevent, adapt to, respond to, recover from, and learn from operational disruptions. The PRA's approach to operational resilience is based on the assumption that, from time to time, disruptions will occur which will prevent firms from operating as usual and see them unable to provide their services for a period.

1.6 A clear focus by boards and senior management on their firm's operational resilience will become increasingly important as the wider financial sector becomes more dynamic, complex, and reliant on technology and third parties. Moreover, international interconnectedness is increasing, for example as UK firms may outsource to cloud computing providers operating in a number of different countries. While this can improve firms' resilience, it also gives rise to new risks to operations which the PRA expects firms to manage effectively.

1.7 To address the growing risk a lack of operational resilience poses, the Operational Resilience Parts of the PRA Rulebook[1] require firms to set and meet clear standards for the services they provide and test their ability to meet those standards. Firms are required to review their existing approaches and make improvements where necessary.

1.8 The policy supports the PRA in embedding operational resilience into its prudential framework. The policy provides an objective basis for the PRA to assess firms' operational resilience and for the PRA's supervisors to have an informed dialogue with the firms they supervise and drive them to implement change where necessary.

1.9 This SS complements, and should be read in conjunction with:

1 Operational Resilience; Insurance - Operational Resilience; and Chapter 22 in the Group Supervision Part of the PRA Rulebook.

- 'The PRA's approach to banking supervision' or 'The PRA's approach to insurance supervision';[2]
- the Fundamental Rules Part of the PRA Rulebook;[3]
- the Operational Resilience Parts;
- the PRA Statement of Policy 'Operational resilience';[4] and
- SS2/21 'Outsourcing and third-party risk management'.[5]

2 Important business services

2.1 A business service is a service that a firm provides. Business services deliver a specific outcome or service to an identifiable user external to the firm and should be distinguished from business lines, which are a collection of services and activities.

2.2 As set out in the Operational Resilience Parts,[6] firms must identify their important business services. The Operational Resilience Parts define important business services as the services a firm provides which, if disrupted, could pose a risk to a firm's safety and soundness or, if a firm meets the criteria set out in the Operational Resilience Parts,[7] the financial stability of the UK. The Operational Resilience Parts[8] set out that insurers must also identify important business services that may pose a risk to policyholder protection.

2.3 The PRA expects firms to identify important business services considering the risk their disruption poses to financial stability (where applicable), the firm's safety and soundness and, in the case of insurers, policyholder protection. A firm's important business services will be a relatively short list of external-facing services for which the firm has chosen to build high levels of operational resilience in anticipation of operational disruption.

2.4 Firms should also consider the practicalities of how they identify their important business services. For example, they should identify important business services so that:

- an impact tolerance can be applied and tested; and
- boards and senior management can make prioritisation and investment decisions.

2.5 When assessing the risk a business service poses to financial stability (where applicable), the firm's safety and soundness, or policyholder protection, the PRA expects firms to consider the following factors:

(a) Financial stability – the impact on the wider financial sector and UK economy, including:

2 Available at: https://www.bankofengland.co.uk/prudential-regulation/publication/pras-approach-to-supervision-of-the-banking-and-insurance-sectors.
3 Fundamental Rules 2, 3, 5, and 6 are particularly relevant.
4 March 2021: https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-sop.
5 March 2021: https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss.
6 Operational Resilience 2.1, Insurance – Operational Resilience 2.1.
7 Operational Resilience 2.3, Insurance – Operational Resilience 2.3.
8 The definition of 'important business service' is in the Insurance – Operational Resilience Part.

- the potential to inhibit the functioning of the wider economy, in particular the economic functions listed in SS19/13 'Resolution planning';[9]

- the potential to cause knock-on effects for counterparties, particularly those that provide financial market infrastructure or critical national infrastructure; and

- whether the service is covered by an impact tolerance set by the Bank's Financial Policy Committee.

(b) The firm's safety and soundness – the impact on the firm itself, including the:

- impact on the firm's profit and loss;

- potential to cause reputational damage; and

- the potential to cause legal or regulatory censure.

(c) In the case of insurers, an appropriate degree of policyholder protection – the impact on policyholders affected by a disruption to the service, including consideration of:

- the type of product, type of policyholder, and their current or future interests;

- the significance to the policyholder of the risk insured;

- the availability of substitute products that would offer a policyholder a similar level of protection; and

- the potential for significant adverse effects on policyholders if cover were to be withdrawn or policies not honoured.

2.6 When assessing if an impact tolerance can be applied to an important business service, firms are expected to consider if the users of the service are identifiable. This means that the impacts of disruption should be clear. The users of the service may include retail customers, business customers, other legal entities, trustees, market participants, the supervisory authorities, or other members of a regulated entity's group.

2.7 The focus on the implications of operational disruption for firms' safety and soundness, financial stability, and policyholder protection means that firms should not identify internal services alone (for example those provided by human resources or payroll) as important business services. Such internal services, if necessary for the delivery of important business services, would be included in the mapping, scenario testing, and any remediation work the PRA requires firms to perform.

2.8 Important business services deliver a specific outcome or service to an identifiable user and should be distinguished from business lines, such as mortgages, which are a collection of services and activities. They will vary from firm to firm. Firms should consider the chain of activities which make up the important business service, from taking on an obligation to delivery of the service, and determine those parts of the chain that are critical to delivery of the important business service. The PRA expects that the critical parts of the chain should be operationally resilient, and that firms should focus their work on the resources necessary to deliver them. Below is an example of where

9 June 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/2013/resolution-planning-ss.

activities performed by internal services within a firm would need to be included in the chain of activities (note, in the example below, the risk management function itself is not required to be operationally resilient in the terms of this policy):

- Trade execution: Where trade execution requires clearance from the risk management function, the clearance process would be included in the chain of activities that form part of the important business service, and the operational resources needed to provide that clearance would need to be operationally resilient. In this example, the important business service (trade execution) could not be delivered if the clearance process was operationally disrupted.

2.9 When assessing if boards and senior management can make prioritisation and investment decisions for an important business service, firms are expected to consider whether the number of important business services is proportionate to their business. It is likely that larger firms will identify a larger number of important business services than smaller firms.

2.10 The PRA expects firms to review their important business services annually at a minimum, or sooner if a significant change occurs, and to determine whether any changes are required to their list of important business services.

3 Impact tolerances

Setting an impact tolerance

3.1 The Operational Resilience Parts[10] require firms to set an impact tolerance for each of their important business services. The Operational Resilience Parts define an impact tolerance as the maximum tolerable level of disruption to an important business service as measured by a length of time in addition to any other relevant metrics.

3.2 The Operational Resilience Parts[11] require firms to set their impact tolerances at the point at which any further disruption to the important business service would pose a risk to the firm's safety and soundness, and in the case of insurers, policyholder protection, and, if a firm meets the criteria as set out in the Operational Resilience Parts,[12] the financial stability of the UK.

3.3 When setting an impact tolerance for an individual important business service, the PRA expects firms to take into account the impact of failure of other related important business services. These may be related because, for example, they share common resources which support the delivery of the important business services or where simultaneous disruption could have compounding impacts on similar external end users. The PRA expects firms to take a proportionate approach in making this assessment, and only to consider extra layers of complexity where there are significant benefits in terms of building operational resilience.

3.4 Impact tolerances provide a standard which boards and senior management should use for prioritising investment and making recovery and response arrangements (see Chapters 4 to 6 of this SS). They may be helpful in informing decision-making during operational disruptions, when they would be considered alongside other information relevant to managing an incident effectively.

10 Operational Resilience 2.2, Insurance – Operational Resilience 2.2.
11 Operational Resilience 2.3, Insurance – Operational Resilience 2.3.
12 Operational Resilience 2.3, Insurance – Operational Resilience 2.3.

3.5 The PRA expects impact tolerances to be set on the assumption that a disruption will occur. Firms should not consider the cause or probability of disruption when setting their impact tolerances.

3.6 An impact tolerance must,[13] in all cases, include a time-based metric to measure the tolerable level of disruption to an important business service. Firms are also required to consider[14] whether time-based impact tolerances should be used in conjunction with additional metrics, such as the volume or value of transactions that the firm can tolerate being interrupted for that period of disruption. See paragraphs 3.10 to 3.16 for more on impact tolerance metrics.

3.7 Firms may choose to set their impact tolerances by assuming an important business service is unavailable for a specified period of time and judging the potential impact this would have. If this disruption would not pose a risk to the firm's safety and soundness, (in the case of insurers) policyholder protection, and (if applicable) the financial stability of the UK, the firm could consider the impact of a longer disruption. If, for example, the firm judges that after an important business service has been unavailable for five days, there would be a risk to the financial stability of the UK, this would be the point within which the firm would set its impact tolerance.

3.8 When judging the point at which safety and soundness, (in the case of insurers) policyholder protection, or (if applicable) the financial stability of the UK is at risk, firms should consider identifying quantitative and qualitative indicators. In identifying indicators, firms should consider the factors identified in paragraph 2.5 of this SS.

3.9 Impact tolerances are defined as the maximum tolerable amount of disruption and should apply at peak times as well as in normal circumstances. As such, when setting impact tolerances, firms may wish to consider different times of the day, different points in the year, or broader factors which may lead to activity within the important business service significantly increasing.

Impact tolerance metrics

3.10 Firms should state their impact tolerances using clear metrics. Firms should set at least one impact tolerance for each important business service they have identified.

3.11 The PRA requires[15] firms to use a time-based metric for all impact tolerances, but, where appropriate, firms should use a time-based metric in conjunction with other metrics. For example, a firm could set its impact tolerance at a certain volume of interrupted transactions due to the disruption of the firm's important business service, in conjunction with the disruption continuing after a certain number of hours.

3.12 A time-based metric for an impact tolerance should specify that a particular important business service should not be disrupted beyond a certain period of or point in time, for example after 24 hours or at the end of the day. An impact tolerance that combines time with a volume and/or value metric might state that the firm will not tolerate the business service delivering less than a certain percentage of normal operating capacity for a specified period of time.

3.13 Impact tolerances should not consider the frequency at which operational disruptions are likely to occur. Rather, they should be focused on setting the limit of the impact the firm can tolerate from a single disruption.

13 Operational Resilience 2.4, Insurance – Operational Resilience 2.4.
14 Operational Resilience 2.4, Insurance – Operational Resilience 2.4.
15 Operational Resilience 2.4, Insurance – Operational Resilience 2.4.

3.14 Setting an impact tolerance enables firms to assess the status of, and set resilience requirements for, the necessary people, processes, technology, facilities, and information (the 'resources') that contribute to the delivery of important business service. These requirements might include capacity specifications, recovery time objectives, and recovery point objectives. These requirements should be set to enable the firm to deliver the important business service within its impact tolerance.

3.15 There may be circumstances when a firm continuing to deliver a service through disruption may have a more adverse impact than suspending it. An example of this is where the firm cannot sufficiently assure the integrity of data underpinning an important business service.

3.16 The PRA's Fundamental Rules[16] will remain relevant to decision making during operational disruptions, including decisions about when an important business service is suspended or restored. When setting impact tolerances, the PRA expects firms to consider the circumstances that might be prevailing at the time of the disruption to help them make informed recovery and response decisions and when they may decide not to resume the functioning of their important business services within the specified time. The PRA expects firms should not be forced into inappropriate actions because of their impact tolerances in the event of a disruption.

4 Actions to remain within impact tolerance

4.1 The Operational Resilience Parts[17] require firms to ensure they are able to deliver their important business services within impact tolerances in severe but plausible scenarios. Mapping and testing the delivery of important business services will equip firms to establish whether and how they can remain within impact tolerances.

4.2 The PRA expects firms to take action where they identify a limitation in their ability to deliver important business services within impact tolerances. The PRA is unlikely to consider complicated business models or the provision of services across borders as good reasons for a firm not to be able to act to ensure they can remain within an impact tolerance – these factors are themselves vulnerabilities that the PRA expects firms to address. However, incidents such as rapid technological change may be a reason for a firm to not be able to remain within an impact tolerance, as it may take time to improve resilience under those conditions.

4.3 The PRA expects firms to develop and implement effective remediation plans for the important business services that would not be able to remain within their impact tolerance. Firms should take prompt action where they cannot remain within the impact tolerance, so these plans should include appropriate timing for the necessary improvements.

4.4 In developing these plans to improve resilience and prioritising their work, firms should also consider the:

16 Fundamental Rules 2, 3, 5, and 6 are particularly relevant for this example.
17 Operational Resilience 2.5, Insurance – Operational Resilience 2.5.

- nature and scale of the risk that disruption to the important business service could have on financial stability (if applicable), safety and soundness, and (in the case of insurers) the appropriate degree of policyholder protection. Firms should prioritise those that pose the greatest risk.

- time-criticality of the important business service, which is high when the impact tolerance is set for a short amount of time. The PRA expects firms to have undertaken planning and set up recovery and response arrangements in advance to be able to respond quickly to disruptions when they occur.

- scale of improvement necessary to remain within the impact tolerance. An important business service that is far from remaining within the impact tolerance may need to be prioritised over a business service that could nearly remain within its impact tolerance in a severe but plausible disruption.

4.5 The PRA expects firms to be able to remain within impact tolerances for important business services, irrespective of whether or not they use third parties in the delivery of these services. This means that firms should effectively manage their use of third parties to ensure they can meet the required standard of operational resilience.

4.6 Although firms may assume that an arrangement is inherently less risky where the service provider is part of its own group, this is often not the case. The PRA expects firms to manage risk and make appropriate arrangements to be able to remain within impact tolerance, whether using third parties that are other entities within their group or external providers.

4.7 The PRA expects firms to develop communication strategies for both internal and external stakeholders as part of their planning for responding to operational disruptions. These communication plans should be developed with a view to reducing harm to counterparties and other market participants and supporting confidence in both the firm and financial sector. The PRA expects firms' plans to include the escalation paths they would use to manage communications during an incident and to identify the appropriate decision makers. For example, the plan should address how to contact key individuals, operational staff suppliers, and the appropriate regulators.

4.8 The PRA requires[18] firms to consider PRA objectives when setting impact tolerances. It is also aware that dual-regulated firms must identify a separate impact tolerance for their important business services, where the delivery of the important business service is also relevant to the FCA's objectives. Where appropriate, a firm may set its PRA impact tolerance for a given important business service at the same point as its FCA impact tolerance. The PRA expects that work done to meet the requirements of one regulator should be leveraged to meet those of the other, and would encourage firms to avoid duplicative work.

4.9 The PRA expects dual-regulated firms to understand whether the scenarios that may cause firms to exceed their respective PRA and FCA impact tolerances would differ (whether or not those impact tolerances are aligned), and to take action to remain within their PRA impact tolerances as appropriate.

4.10 The PRA understands that in practice firms may concentrate their efforts on ensuring they can remain within the more stringent tolerance. Where the PRA and FCA impact tolerances differ for a

18 Operational Resilience 2.3, Insurance – Operational Resilience 2.3.

dual-regulated firm, taking action to ensure firms can remain within the more stringent tolerance will be acceptable if a firm can demonstrate:

- how they have considered the PRA's objectives when setting their impact tolerances;
- how their response and recovery arrangements ensure firms are able to remain within the PRA impact tolerance; and
- that scenario testing has been performed with the PRA impact tolerance in mind.

4.11 Below is an example illustrating how firms could effectively concentrate their efforts on ensuring they can remain within the more stringent impact tolerance for a given important business service:

- Where a firm providing custodian services to small and medium-sized asset managers and investment firms identifies the safekeeping of securities for customers as an important business service, it may judge that: (a) after six hours of disruption, this impacts customers' abilities to settle transactions and thus poses a risk of consumer harm; and (b) after eight hours of disruption, this creates a reputational risk which threatens their safety and soundness. The firm identifies vulnerabilities in its safeguarding systems and thus increases its investment to improve the robustness of its systems to allow it to remain within the shorter impact tolerance, which also serves to meet the longer impact tolerance.

Policy implementation

4.12 The Operational Resilience Parts are effective from Thursday 31 March 2022. By this point, firms must have identified their important business services and set impact tolerances. In order to achieve this, and to identify any vulnerabilities in their operational resilience, firms should have mapped their important business services and commenced a programme of scenario testing.

4.13 Firms are not expected to have performed mapping and scenario testing to the full extent of sophistication by Thursday 31 March 2022. Both mapping and scenario testing are ongoing processes, and firms are expected to perform them at varying levels of sophistication over time. The PRA expects that firms' approaches to both mapping and scenario testing should evolve over time.

4.14 Senior management are expected to take responsibility for delivering the policy outcomes. Firms are expected to have a prioritised plan which sets out how they will comply with the requirement to be able to remain within their impact tolerances within a reasonable time, and no later than Monday 31 March 2025.[19] For a firm's plan to be effective, firms must have started putting the plan into effect by Thursday 31 March 2022. As part of this planning, firms should prioritise their regular mapping and scenario testing so that they will be able to identify vulnerabilities in sufficient time so that measures can be taken to remediate them. Firms, particularly larger, more complex ones, will need to make choices and prioritise with the ultimate goal of delivering the outcomes of the policy.

4.15 The speed at which vulnerabilities are remediated should be commensurate with the potential impact that a disruption would cause, and will be an area of supervisory focus.

19 Operational Resilience 2.5, 2.6, Insurance – Operational Resilience 2.5, 2.6.

4.16 After Monday 31 March 2025, maintaining operational resilience will be a dynamic activity. By this point, 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 important business service in the event of a severe but plausible disruption.

5 Mapping

5.1 The Operational Resilience Parts[20] require firms to identify and document the necessary people, processes, technology, facilities, and information (the 'resources') required to deliver each of their important business services. This identification process is referred to as 'mapping'.

5.2 Adequate mapping should enable firms to meet the following outcomes:

(a) **The identification of vulnerabilities.** Mapping an important business service should allow a firm to identify the resources that are critical to delivering an important business service, ascertain whether they are fit for purpose, and consider what would happen if resources were to become unavailable.

(b) **Test ability to remain within impact tolerances.** Mapping should facilitate the testing of a firm's ability to deliver important business services within impact tolerances. To design and understand the full implications of scenarios, a map of the relevant business service is necessary. Further information on the approach to testing is outlined in Chapter 6.

5.3 To meet the requirements in the Operational Resilience Parts[21], the PRA expects firms to take action where a vulnerability is identified, or testing highlights a limitation to remaining within impact tolerances.

5.4 The PRA expects firms to map their important business services to the level of detail necessary to use the mapping to identify vulnerabilities and test ability to remain within impact tolerances.

5.5 The PRA expects firms to map the resources necessary to deliver important business services irrespective of whether the resources are being provided wholly or in part by a third party, which may be an intragroup or external service provider. Firms should understand how their outsourcing and third party dependencies support important business services.

5.6 Firms should understand the reliance placed on sub-outsourcing arrangements and if these arrangements pose a threat to their operational resilience. Paragraph 9.5 of SS2/21 sets out that firms should assess whether sub-outsourcing meets materiality criteria set out in Chapter 5 of SS2/21, which includes the potential impact on the firm's operational resilience and the provision of important business services. Paragraph 9.6 of SS2/21 sets out that 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 policy or policies.

5.7 As set out in SS2/21, 'firms that enter into outsourcing arrangements remain fully accountable for complying with all their regulatory obligations'. This is a key principle underlying all requirements and expectations regarding outsourcing and other third party arrangements. Therefore, a firm will remain responsible if a third party provider on whom it relies, whether wholly or in part, to provide an important business service, fails to remain within impact tolerances or causes the firm to do so.

20 Operational Resilience 4.1, Insurance – Operational Resilience 4.1.
21 Operational Resilience 2.5, Insurance – Operational Resilience 2.5.

SS2/21 sets out detailed expectations on how firms should obtain assurance from third parties throughout the lifecycle of an outsourcing or, where relevant, other third party arrangement. The level of assurance that the PRA expects should be proportionate to the size and complexity of the firm and reflect the materiality and risk of the outsourcing and third party arrangement. As part of this assurance, firms may ask third parties to provide mapping, but this is not required in all cases, particularly if other assurance mechanisms are effective and more proportionate.

5.8 Mapping information should be accessible and usable for the firm. Firms should document their mapping in a way that is proportionate to their size, scale, and complexity. Firms are expected to develop their own methodology and assumptions for mapping to best fit their business.

5.9 The PRA expects firms to update their mapping annually at a minimum, or following significant change if sooner.

6 Scenario testing

6.1 The Operational Resilience Parts[22] require firms to test regularly their ability to remain within impact tolerances in severe but plausible disruption scenarios. Impact tolerances assume a disruption has occurred, and so testing the ability to remain within impact tolerances should not focus on preventing incidents from occurring. The PRA expects firms to focus on recovery and response arrangements.

6.2 Firms should identify the severe but plausible scenarios they use for testing. When setting scenarios, firms could consider previous incidents or near misses within the organisation, across the financial sector, and in other sectors and jurisdictions. A testing plan should include realistic assumptions and evolve as the firm learns from previous testing.

6.3 The Operational Resilience Parts[23] require firms to prepare a written self-assessment of compliance with the Operational Resilience Parts. The PRA expects firms to document details of their scenario testing, including assumptions made in relation to scenario design and any identified risks to the firm's ability to remain within impact tolerances.

6.4 Over time, the PRA expects a firm's scenario testing to become more sophisticated as firms develop operational resilience for each important business service. Firms would be expected to test against more severe but plausible scenarios, proportionate to the firm and the degree of operational resilience each important business service has.

6.5 When considering the important business services to prioritise for testing, firms should consider the relative risk they pose to financial stability (if applicable), safety and soundness, and (in the case of insurers) the appropriate degree of policyholder protection.

6.6 The PRA expects firms to develop a testing plan that details how they will gain assurance that they can remain within impact tolerances for important business services. The nature and frequency of a firm's testing should be proportionate to the potential impact that disruption could cause and whether the operational resources supporting an important business service have materially changed. When developing a testing plan, firms should consider the following:

22 Operational Resilience 5.1, Insurance – Operational Resilience 5.1.
23 Operational Resilience 6.1, Insurance – Operational Resilience 6.1.

- the type of scenario testing, which may include paper-based assessments, simulations, or live-systems testing;

- the frequency of the scenario testing – firms that implement changes to their operations more frequently should undertake more frequent scenario testing;

- the number of important business services tested – firms that have identified more important business services should undertake more scenario testing to reflect this; and

- testing the availability and integrity of resources – impact tolerances are concerned with the continued provision of important business services. An important business service that can continue to be provided but has insufficient integrity is not within the impact tolerance. Firms should test their recovery plans for both availability and integrity scenarios, proportionate to their size and complexity; and

- how their environment is changing and whether this will give rise to different vulnerabilities.

6.7 Scenario testing should not pose a material risk of creating a disruption. Where firms consider that live-systems testing is most appropriate for scenario testing their ability to remain within impact tolerances, firms should assess the risk that the scenario testing may create a disruption to the delivery of important business services. The PRA's Fundamental Rules[24] will remain relevant to decision making for how firms approach their scenario testing. Firms should conduct scenario testing with due skill, care, and diligence, act prudently, have effective risk strategies and risk management, and control their affairs responsibly and effectively.

6.8 The entire chain of activities that have been identified as the important business service should be considered when developing testing plans.

6.9 The severity of scenarios used by firms for their testing could be varied by increasing the number or type of resources unavailable for delivering the important business service, or extending the period for which a particular resource is unavailable. The mapping work that firms will undertake is likely to be useful in informing them how their scenarios could be made more difficult.

6.10 The PRA recognises that it would not be proportionate to require firms to be able to remain within impact tolerances in circumstances which are beyond severe or implausible. There will be scenarios where firms find they could not deliver a particular important business service within their impact tolerance. For example, if essential infrastructure (such as power, transport, or telecommunications) were unavailable, some firms may not be able to deliver their important business services within their impact tolerance.

6.11 As impact tolerances are set on the assumption that disruptions will occur, the PRA does not expect firms to devote too much time to considering the relative probability of incidents occurring.

6.12 Firms should test a range of scenarios, including those in which they anticipate exceeding their impact tolerance. Understanding the circumstances where it is impossible to stay within an impact tolerance will provide useful information to firms' management and to their supervisors. Boards and senior management will need to judge whether failing to remain within the impact tolerance in specific scenarios is acceptable and be able to explain their reasoning to supervisors.

[24] Fundamental Rules 2, 3, 5, and 6 are particularly relevant for this example.

6.13 Chapters 5 to 10 of SS2/21 set out detailed expectations on how firms should perform due diligence and obtain effective and proportionate assurance from third parties, including through scenario testing. In particular, the PRA expects contractual agreements for material outsourcing arrangements to include 'requirements for both parties to implement and test business contingency plans. For the firm, these should take account of firms' impact tolerances for important business services. Where appropriate, both parties should commit to take reasonable steps to support the testing of such plans'. SS2/21 further notes that firms' business continuity and exit plans for material outsourcing arrangements should 'where possible and relevant … align to, support, or even be a component of firms' scenario testing for operational resilience. For instance, one of the severe but plausible scenarios that firms may select for this testing could involve a failure or disruption at a third party, or their supply chain, based on previous incidents or near misses within the organisation, across the financial sector, and in other sectors and jurisdictions'.

7 Governance

Board responsibilities

7.1 Boards are specifically required to approve the important business services identified for their firm and the impact tolerances that have been set for each of these. The Operational Resilience Parts[25] require that a firm's board must approve and regularly review the firm's important business services, impact tolerances, and written self-assessment (see Chapter 8 of this SS). In delivering this responsibility, boards must regularly review assessments of the firm's important business services, impact tolerances, and the scenario analyses of its ability to remain within the impact tolerance for these important business services.

7.2 While individual board members are not required to be technical experts on operational resilience, the PRA expects boards to ensure that they have the appropriate management information. Boards should also collectively possess adequate knowledge, skills, and experience to provide constructive challenge to senior management and inform decisions that have consequences for operational resilience.[26]

Management responsibilities

7.3 Firms should establish clear accountability and responsibility for the management of operational resilience, including implementation of the policy set out here. The PRA expects firms to structure their oversight of operational resilience in the most effective way for their business, using existing committees and roles or establishing new ones if necessary.

7.4 Where it exists,[27] the Chief Operations Senior Management Function (SMF) 24 should hold overall responsibility for implementing operational resilience policies and reporting to the board. Consistent with paragraph 2.11G of SS28/15 'Strengthening individual accountability in banking'[28] and paragraph 2.22L of SS35/15 'Strengthening individual accountability in insurance',[29] the SMF24 function may be shared or split among two or more individuals. This is on the basis that the split accurately reflects the firm's organisational structure and that comprehensive responsibility for

25 Operational Resilience 7, Insurance – Operational Resilience 7.
26 Rule 5.2 in the General Organisational Requirements Part of the PRA Rulebook (CRR firms), Rule 2.7 in the Conditions Governing Business Part of the PRA Rulebook (Solvency II firms).
27 Rule 3.8 in the Senior Management Functions Part of the PRA Rulebook (CRR firms), Rule 3.7 in the Insurance – Senior Management Functions Part of the PRA Rulebook (Solvency II firms).
28 December 2020: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-banking-ss.
29 February 2020: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-insurance-ss.

operations and technology is not undermined. However, firms that have a single senior individual with overall responsibility for internal operations and technology should only have that individual approved as the SMF24. Where the SMF24 function is split, the PRA does not expect it to be split among more than three individuals. Further information on the SMF24 function is contained in the aforementioned Supervisory Statements.

7.5 Where a firm does not have a board, senior management should take responsibility for the Operational Resilience Parts.[30]

8 Self-assessment

8.1 The Operational Resilience Parts[31] require firms to document a self-assessment of their compliance with the Operational Resilience Part. Firms are also expected to document the methodologies they have used to undertake these activities. Firms' boards are accountable for and should approve the information provided in these documents. The PRA expects boards and senior management to seek to build resilience so that they gain a high level of assurance that their firm is able to deliver its important business services within impact tolerances. Firms should document this information in the form of a self-assessment.

8.2 A self-assessment should directly address the requirements set out in the Operational Resilience Parts.[32] Broader elements of firms' operational resilience, for example, operational risk management and business continuity planning, should only be referenced where they directly pertain to the Operational Resilience Parts.[33] Broader elements of firms' resilience should be captured in existing firm practices.

8.3 When documenting a self-assessment to meet the Operational Resilience Parts,[34] firms should:

- list their important business services and state why each of these have been identified, with reference to the PRA's expectations in Chapter 2 of this SS;
- specify the impact tolerances set for these important business services and why each impact tolerance has been set, with reference to the expectations in Chapter 3 of this SS;
- detail their approach to mapping important business services. The PRA expects this to include how the firm has identified the resources that contribute to the delivery of important business services and how they have captured the relationships between these. Firms should also document how they have used mapping to identify vulnerabilities and to support testing activity;
- describe their strategy for testing their ability to deliver important business services within impact tolerances through severe but plausible scenarios. Firms should also describe the scenarios used, the types of testing undertaken, and specify the scenarios under which firms could not remain within their impact tolerances;
- identify any lessons learned when undertaking scenario testing or via practical experience, including the actions taken to address the issues encountered or risks highlighted; ~~and~~

30 Operational Resilience 7, Insurance – Operational Resilience 7.
31 Operational Resilience 6, Insurance – Operational Resilience 6.
32 Operational Resilience 6, Insurance – Operational Resilience 6.
33 Operational Resilience 6, Insurance – Operational Resilience 6.
34 Operational Resilience 6, Insurance – Operational Resilience 6.

- identify the vulnerabilities that threaten their ability to deliver important business services within impact tolerances. Firms should make every effort to remediate these vulnerabilities, detailing the actions taken or planned and justifications for their completion time. The completion time should be appropriate to the size and complexity of the firm, and the PRA will expect large and complex firms to take prompt action; and

- identify any additional risks to their ability to deliver important business services within impact tolerances arising from elsewhere in their group. In the case of a CRR firm, the self-assessment should also be informed by any work the CRR consolidation entity has undertaken to comply with the requirements under Rules 8.6, 8.7 and 8.8, regarding important group business services and whether each member of the CRR consolidation entity's consolidation group could remain within impact tolerance.

9 Groups

9.1 The PRA expects CRR consolidation entities (in the case of UK banking groups) or an insurer (in the case of UK insurance groups) to identify a proportionate number of important group business services and respective impact tolerances at the level of the group.[35] Taking a group level view of operational resilience ensures the risks arising in parts of the group that are not subject to the individual requirements, are taken into account.

9.2 When identifying important group business services, the PRA expects CRR consolidation entities and insurers to consider disruption to services in other entities within the group which could transmit risk directly to the safety and soundness of the CRR firm (or CRR firms) or insurer, or alternatively could transmit risk to the safety and soundness of the CRR firm (or CRR firms) or the insurer via the group. This includes, for example, where the relevant group has a subsidiary outside the UK providing a service to customers, which could, if disrupted, pose a risk to:

- for CRR consolidation entities, the safety and soundness of any CRR firm in the CRR consolidation entity's consolidation group or, where relevant, UK financial stability;

- for insurers, the firm's safety and soundness, policyholder protection or, where relevant, UK financial stability.

9.3 Impact tolerances should be set in the same way as they are for an individual firm[36]. Boards and senior management should consider the level of disruption that would represent a threat to the CRR firm or insurer, for example, via a threat to the viability of the group and therefore pose a risk to financial stability of the UK, a firm's safety and soundness, or (in the case of PRA-regulated insurers) there being an appropriate degree of protection for those who are or may become the firm's policyholders.

9.4 The PRA expects that, in complying with the Operational Resilience Part[37], the CRR consolidation entity would have regular dialogue with other members of its group so the CRR firm (or CRR firms) can take account of any additional risks to their safety and soundness when assessing their ability to remain within impact tolerance for their own important business services.

35 CRR consolidation must comply with Operational Resilience Part Rules 8.6 to 8.13 by no later than Thursday 30 June 2022.
36 The PRA expectations regarding the setting of impact tolerances are detailed in Chapter 3 of this SS.
37 Operational Resilience 8.8

9.5 The PRA expects firms to work with other members of their group to take action, should it be likely that a relevant important group business service could not be delivered within its impact tolerance. Firms are required to cover analysis of risks arising from elsewhere in the group in their self-assessments.

Annex – SS1/21 updates

This annex details the changes that have been made to this SS following its initial publication in March 2021:

2022

March 2022

Following publication of PS2/22 'Operational Resilience and Operational Continuity in Resolution: CRR firms, Solvency II firms, and Financial Holding Companies (for Operational Resilience)', this SS was updated to reflect the PRA's expectations in relation to applying the group provisions relevant to CRR firms to financial and mixed activity holding companies. This is detailed in paragraphs 1.3, 1.4 and paragraphs 9.1-9.7. This SS was also updated by amending paragraph 8.3 to clarify the PRA's expectations in relation to the CRR firm's self-assessment.

This policy is effective from Thursday 31 March 2022. CRR consolidation entities must implement the policy within a reasonable time, but no later than the 30th June 2022.