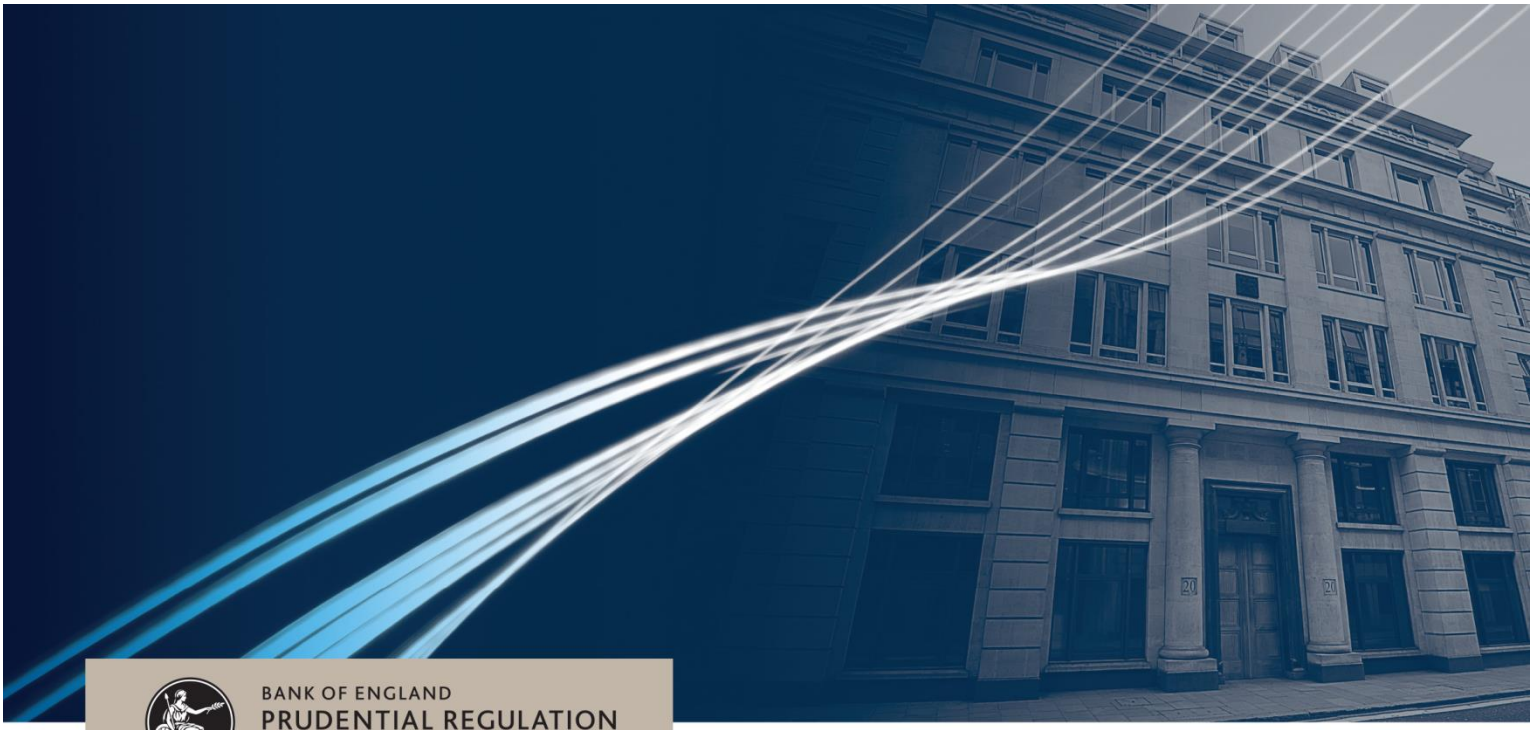


BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Consultation Paper | CP29/19

Operational resilience: Impact tolerances for important business services

December 2019

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

Consultation Paper | CP29/19

Operational resilience: Impact tolerances for important business services

December 2019

By responding to this consultation, you provide personal data to the Bank of England. This may include your name, contact details (including, if provided, details of the organisation you work for), and opinions or details offered in the response itself.

The response will be assessed to inform our work as a regulator and central bank, both in the public interest and in the exercise of our official authority. We may use your details to contact you to clarify any aspects of your response.

The consultation paper will explain if responses will be shared with other organisations (for example, the Financial Conduct Authority). If this is the case, the other organisation will also review the responses and may also contact you to clarify aspects of your response. We will retain all responses for the period that is relevant to supporting ongoing regulatory policy developments and reviews. However, all personal data will be redacted from the responses within five years of receipt. To find out more about how we deal with your personal data, your rights or to get in touch please visit bankofengland.co.uk/legal/privacy.

Information provided in response to this consultation, including personal information, may be subject to publication or disclosure to other parties in accordance with access to information regimes including under the Freedom of Information Act 2000 or data protection legislation, or as otherwise required by law or in discharge of the Bank's functions.

Please indicate if you regard all, or some of, the information you provide as confidential. If the Bank of England receives a request for disclosure of this information, we will take your indication(s) into account, but cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system on emails will not, of itself, be regarded as binding on the Bank of England.

Responses are requested by Friday 3rd April 2020.

Please address any comments or enquiries to:
Daniel Norris and Claire Ward
Prudential Regulation Authority
20 Moorgate
London
EC2R 6DA

Email: CP29_19@bankofengland.co.uk

Contents

1 Overview

1.1 In this consultation paper (CP), the Prudential Regulation Authority (PRA) sets out its proposals for PRA rules (Appendix 1 and 2), a Supervisory Statement (SS) (Appendix 3) and a Statement of Policy (SoP) (Appendix 4) designed to improve the operational resilience of firms and protect the wider financial sector and UK economy from the impact of operational disruptions. The draft rules and expectations seek to embed the concepts of the July 2018 Discussion Paper (DP) 1/18 'Building the UK financial sector's operational resilience' (the DP) into the PRA's prudential framework. The accompanying joint Bank of England (Bank), Financial Conduct Authority (FCA) and PRA covering paper, 'Building operational resilience: Impact tolerances for important business services'[1] sets out how the concepts in the DP have been updated in the proposed policy. The draft SoP sets out how the PRA proposes to supervise existing policies in the light of the proposed new operational resilience rules and expectations.

1.2 This CP is relevant to all:

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

1.3 Banks and insurers are collectively referred to as 'firms' in this CP.

1.4 The proposals aim to address risks to operational resilience including those arising 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 to prepare for disruptions and to invest where it is needed.

1.5 The proposed policy would support the PRA in embedding operational resilience into its prudential framework. It would establish an objective basis for the PRA to assess firms' operational resilience and help the PRA's supervisors to have a more informed dialogue with the firms they supervise. The PRA plans to continue to use a wide range of existing tools and powers to support its supervision of operational resilience, including for example the senior managers' regime, and its powers under section 166 of the Financial Services and Markets Act (FSMA) to require skilled persons' reports.

1.6 The proposals are consistent with the approach developed jointly with the FCA and the Bank's Financial Market Infrastructure Directorate (FMID). An explanation of the joint policy position can be found in the covering paper 'Building operational resilience: Impact tolerances for important business services'. The PRA has developed draft rules for firms which seek to implement the joint policy approach to operational resilience. The proposed new operational resilience rules are set out in 'The Operational Resilience Parts' which includes operational resilience rules in the Group Supervision Part.

1.7 Firms are also encouraged to read CP30/19, 'Outsourcing and third party risk management', which has been published by the PRA at the same time as this CP. It includes proposals which are relevant to firms' operational resilience.

---

1 https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.

Background

1.8 'Operational resilience' in this CP refers to the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover, and learn from operational disruptions. The PRA's proposed 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. The PRA considers that many firms currently may not sufficiently plan on the basis that disruptions will occur, and are therefore not ready to manage effectively when they do.

1.9 Consistent with the approach set out in the DP, the proposals aim to ensure that firms deliver improvements to their operational resilience in three main areas:

(i) prioritising the things that matter: boards and senior management should prioritise those activities that, if disrupted, would pose a risk to the stability of the UK financial sector (financial stability), a firm's safety and soundness, or the appropriate degree of policyholder protection (in the case of insurers).[2] For many firms, this will mean a shift away from thinking about the resilience of individual systems and resources and a shift towards considering the services that are provided to users (identifying important business services);

(ii) setting clear standards for operational resilience: firms should articulate specific maximum levels of disruption, including time limits within which they will be able to resume the delivery of important business services following severe but plausible disruptions (setting impact tolerances); and

(iii) investing to build resilience: firms should have contingency arrangements in place to enable them to resume the delivery of important business services, taking action in advance to ensure that firms' important business services are able to remain within impact tolerances in severe but plausible scenarios.

1.10 The PRA would monitor the work firms undertake to achieve these standards. Where firms fall short, the proposals would mean that the PRA would be able to hold firms to account if they fail to make the necessary improvements.

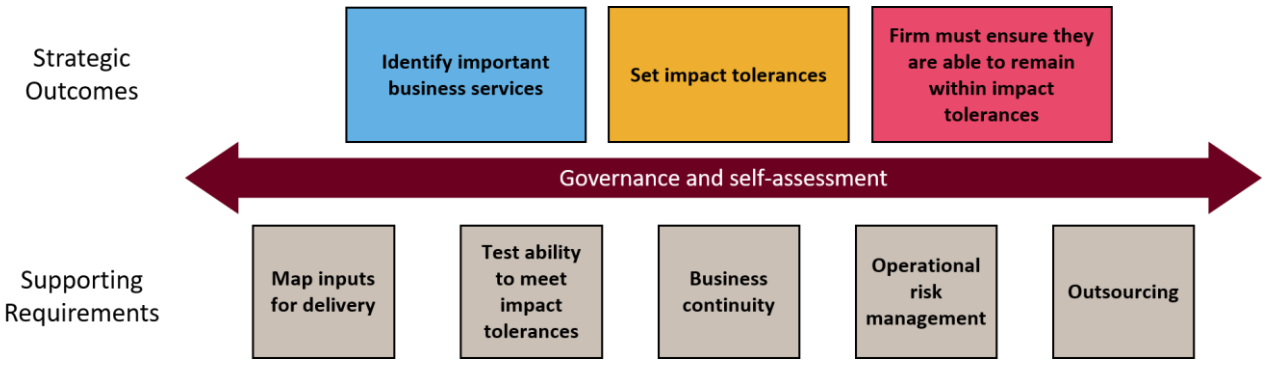
1.11 Figure 1 on page 3 illustrates the key elements in the PRA's proposed approach and how they are supported by existing PRA policy. The new elements of the proposed policy are introduced in the CP chapters that follow. The CP also introduces a proposed SoP which sets out how the PRA views the interaction between the proposed Operational Resilience Parts, SS, and other parts of the PRA's regulatory framework.

1.12 The PRA proposes that boards and senior management be actively involved in the oversight of their firms' operational resilience work, in particular focusing on the strategic outcomes illustrated in the top row of Figure 1. Board leadership is necessary, in part because strategic decisions about budgets and spending has implications for a firm's operational resilience.

---

2 Policyholder protection in this CP means contributing to the securing of an appropriate degree of protection for those who are or may become insurance policyholders.

Figure 1: Strategic outcomes and supporting requirements for operational resilience policy



Structure of the CP

1.13 The CP is structured as follows:

- Chapter 2 sets out proposals relating to the identification of important business services, including examples of important business services firms might identify;
- Chapter 3 sets out proposals relating to impact tolerances for important business services;
- Chapter 4 sets out proposals relating to the actions the PRA considers firms should take to ensure that firms' important business services are able to remain within impact tolerances in severe but plausible scenarios. The chapter also includes proposals for firms to map, test and prepare self-assessments to support their operational resilience;
- Chapter 5 sets out proposals relating to groups; and
- Chapter 6 sets out how the PRA is meeting its statutory obligations in respect of policy-making.

Implementation

1.14 The proposed implementation date for the proposals in the CP is the second half of 2021.

Responses and next steps

1.15 This consultation closes on Friday 3rd April 2020. The PRA invites feedback on the proposals set out in this consultation. Please address any comments or enquiries to CP29_19@bankofengland.co.uk.

1.16 Subject to the feedback received, the PRA will work to develop final Operational Resilience Parts for publication in the second half of 2020. This aligns with the proposed publication date for the proposals in CP30/19, 'Outsourcing and third party risk management'. The PRA will continue to collaborate with the FCA and the Bank to develop an approach for regulated firms and Financial Market Infrastructures (FMIs) that is aligned as far as practicable.

1.17 During 2020, the PRA plans to consider the regulatory reporting requirements for operational resilience, including whether new quantitative information should be submitted by firms and what information should be submitted when operational incidents occur.

1.18 The proposals set out in this CP have been designed in the context of the current UK and EU regulatory framework. The PRA will keep the policy under review to assess whether any changes

would be required due to changes in the UK regulatory framework, including those arising once any new arrangements with the European Union take effect.

1.19 In the event that the UK leaves the EU with no implementation period in place, the PRA has assessed that the proposals would need to be amended.

- A second version of the proposed rules which includes the relevant amendments is attached to this CP. Depending on the timing of the UK's withdrawal from the EU, the amendments may be made under the EU (Withdrawal) Act 2018 (EUWA). Please see PS5/19 'The Bank of England's amendments to financial services legislation under the European Union (Withdrawal) Act 2018' for further details. Changes under EUWA should be read in conjunction with the draft PRA transitional direction published in CP18/19 'UK withdrawal from the EU: Changes following extension of Article 50'.[3]

- The draft SS and draft SoP attached to this CP should be read in conjunction with SS1/19 'Non-binding PRA materials: The PRA's approach after the UK's withdrawal from the EU'.[4]

2 Important business services

2.1 This chapter sets out the PRA's proposal to introduce Operational Resilience Parts and new rules in the Group Supervision Part in the PRA Rulebook and expectations in a draft SS for firms to identify their important business services.

Business services

2.2 A 'business service' is a service that a firm provides to an external end user.[5] 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.

2.3 As set out in the DP, avoiding disruption to particular systems is a contributing factor to operational resilience, but it is ultimately a business service that needs to be resilient – and needs to continue to be provided. A business services approach is an effective way to prioritise improvements to systems and processes. Looking at systems and processes on the basis of the business services they support may bring more transparency to, and improve the quality of, decision making, thereby improving operational resilience.

2.4 The PRA proposes that firms would consider the chain of activities which make up the business service, from taking on an obligation to delivery of the service, and determine which part of the chain is critical to delivery. This would vary by business service. Sometimes the chain will be long, and certain early stages, for example when an obligation is accepted, may not be critical to the final delivery of a service. In other cases, the process of delivering a service may be more integrated and origination may be a key part of this. The PRA considers that the most critical parts of the service should be operationally resilient, and that firms would accordingly focus their work on the resources necessary to deliver those activities in the chain.

---

3 https://www.bankofengland.co.uk/prudential-regulation/publication/2019/uk-withdrawal-from-the-eu-changes-following-extension-of-article-50.

4 April 2019: https://www.bankofengland.co.uk/prudential-regulation/publication/2019/non-binding-pra-materials-the-pras-approach-after-the-uks-withdrawal-from-the-eu-ss.

5 Operational Resilience – CRR Firms Part 1 Operational Resilience – Solvency II Firms Part 1.

2.5 The PRA would not expect internal services such as those provided by human resources or payroll teams to be identified as business services for the purposes of the proposed policy. Failure to deliver internal services would only give rise to concerns from the PRA's perspective when it affected the delivery of outward-facing business services which have direct consequences for safety and soundness, financial stability or the appropriate degree of policyholder protection. Internal services, if necessary for the delivery of important business services, would be included in the mapping work firms would be required to perform (see Chapter 4).

2.6 A focus on business services drives specific and measurable activities, including investment in contingency arrangements, which increase operational resilience. The PRA considers that firms should assume that individual systems and processes that support important business services would be disrupted and increase the focus on back-up plans, effective responses and recovery options.

Prioritising important business services

2.7 The PRA proposes that a business service is 'important' if its disruption could pose a risk to the firm's safety and soundness or financial stability, or in the case of insurers, the appropriate degree of policyholder protection (see draft Operational Resilience Parts[6] and paragraph 2.2 of the draft SS).

2.8 When determining the level of granularity at which to define an important business service, the PRA proposes that firms should also consider whether their definition will allow:

- an impact tolerance to be applied to the important business service which can be tested; and
- boards and senior management to make prioritisation and investment decisions.

2.9 The PRA would expect firms to consider a range of risks when identifying their important business services. Examples of potential risks are provided below.

2.10 Examples of risks posed to financial stability would include:

- for deposit takers, preventing a significant number of payments to be made to the extent that financial stability is undermined; and
- for insurers, sudden removal of cover for businesses' compulsory insurance across an industry.

6 Definition of important business service in the draft Operational Resilience Parts.

2.11 Examples of risks posed to firms' safety and soundness include:

- for all firms, the potential for operational disruption to have a material adverse impact on profitability or viability; and
- additionally for deposit takers, the potential for reputational damage to the extent it could undermine depositors' confidence.

2.12 Examples of risks posed to policyholder protection include:

- policyholders relying on annuity payments to pay bills; and
- if insurance is compulsory for a small business to continue to operate.

2.13 Identifying a business service as important will be a matter of judgement for boards and senior management. The PRA does not propose to introduce definitive lists or taxonomies of important business services, as specifying certain services as important in all circumstances is unlikely to be proportionate. For example, because firms have differing business models, the same business service may be important for one firm but not another. A prescriptive taxonomy may inadvertently exclude some important business services, including as innovation sees new services developed over time. The PRA considers that the proposed approach will require firms to embed the concept of important business services into their operations.

2.14 Important business services will be different for banks and insurers. Important business services could include:

- a bank's payments services;
- a life insurer's payment of annuities;
- a general insurer's policy issuance, from receiving payment to providing coverage;
- a building society's disbursement of mortgages;
- an investment bank's ability to provide currency hedging services; or
- a retail bank's provision of ATM cash withdrawals to customers.

Governance

2.15 The proposed policy would require boards and senior management to approve the important business services identified for their firm. The identification should enable the board to approve the impact tolerances set and make prioritisation and investment decisions.

3 Impact tolerances

3.1 The PRA proposes that firms set an impact tolerance for each of their important business services in the Operational Resilience Parts.[7] The impact tolerance would quantify the maximum acceptable level of disruption to an important business service.

---

7 Draft Operational Resilience – CRR Firms Part Rule 2.2, Operational Resilience – Solvency II Firms Part Rule 2.2.

3.2 The PRA proposes that impact tolerances should be set at the point at which disruption to a firm's important business services would pose a risk to either the firm's safety and soundness or financial stability or, in the case of insurers, the appropriate degree of policyholder protection.

3.3 The PRA proposes that the impact tolerance be expressed as a clear metric, which would include reference to the maximum tolerable duration for which the delivery of the important business service would be affected. The impact tolerance could also measure the extent of disruption by including the maximum value or number of transactions affected, the number of customers affected, or other relevant factors.

3.4 The impact tolerance would be set with reference to a single disruption rather than an aggregation of a number of disruptions. For example, the impact tolerance for an important business service could be two days in the event of a disruption, but should not be a cumulative two days based on multiple disruptions. This is because impact tolerances are designed to identify how quickly a firm should be able to restore delivery of service after disruption.

3.5 Impact tolerances provide a clear standard which the PRA would expect firms to be able to remain within, and which boards and senior management could use to drive improvements to their operational resilience.

3.6 The PRA proposes that impact tolerances should be set on the assumption that disruptions will occur. Chapter 3 of the draft SS sets out the proposed metrics that firms could consider when setting a tolerance and what qualitative and quantitative factors may be relevant to the PRA's objectives (at paragraph 3.2 of this CP above).

3.7 Chapter 3 of the draft SS sets out the PRA's proposed expectations for how firms may go about setting impact tolerances. The draft SS sets out the indicators firms may consider. Such indicators include:

- A challenger bank, focused solely on the provision of current accounts, may identify the ability for customers to check their balances as an important business service. The bank may judge that after four days in which they cannot provide customers with accurate account balance data, their reputation may be damaged to the point that: i) customers close their accounts or withdraw funds; or ii) investors stop funding the firm. The bank may judge that this could put its safety and soundness at risk. As such, it may set its impact tolerance for customer balance checking at a point before this level of impact is incurred. In this example, the tolerance should be less than four days of disruption, but should also be specific, eg 84 hours, to provide a clear standard.

- A large direct participant of Clearing House Automated Payment System (CHAPS) may identify the provision of correspondent banking services to indirect participants (IDP) as an important business service. If it were unable to make CHAPS payments on behalf of IDPs for more than one day, it may judge that this could: i) stop IDPs from conducting business, for example, making housing payments, foreign exchange payments or lending to corporates; ii) lead IDPs to withdraw from certain markets as they cannot make their wholesale payments; or iii) lead to a drop in market confidence due to the widespread impact of the disruption. Accordingly, it may judge that this could potentially pose a risk to financial stability. As such, the firm may set its impact tolerance for the provision of CHAPS correspondent banking to be resumed before the end of the current business day.

- An insurance firm may identify annuity payments as an important business service. The firm

may judge that more than two days of disruption to its provision of annuity payments could pose a risk to vulnerable customers who are reliant on these payments to buy basic goods. It may judge that this is an unacceptable level of impact to policyholders. Accordingly, it may set its tolerance for disruption to annuity payments below two days. Again, the tolerance should be specific, eg 36 hours.

Governance

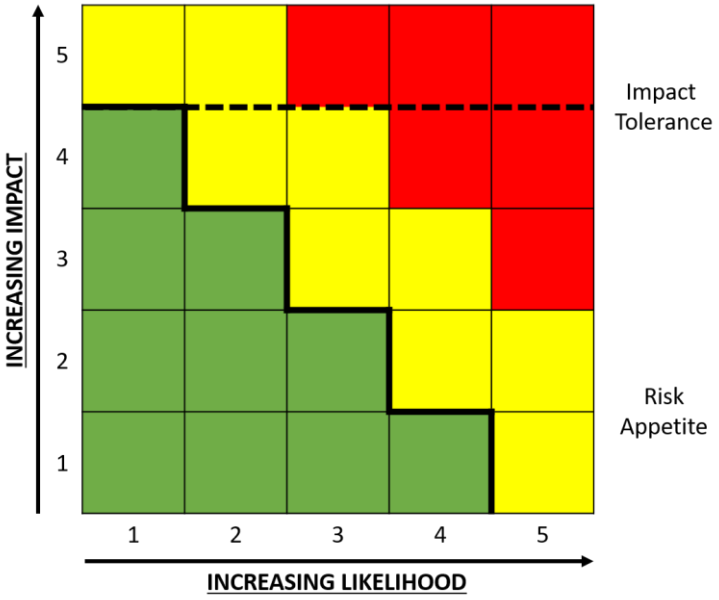
3.8 The proposed policy would introduce in the Operational Resilience Parts[8] a requirement for boards and senior management to approve the impact tolerances which have been set for each of their firm's important business services.

Risk appetite and impact tolerances

3.9 The impact tolerances that the PRA proposes to introduce differ from risk appetites. One key difference is that impact tolerances assume a particular risk has crystallised rather than 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 (as Figure 2 below illustrates). A second important difference is that impact tolerances are set in relation to the potential impact on disruption to financial stability, the firm's safety and soundness and, in the case of insurers, the appropriate degree of policyholder protection, whereas risk appetites tend to be set with specific reference to firms' corporate objectives.

8 Operational Resilience – CRR Firms Part Rule 7.2, Operational Resilience – Solvency II Firms Part Rule 7.2.

Figure 2: Risk appetite and impact tolerance



3.10 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. Figure 2 should be interpreted as follows:

- The thick solid black 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 black 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.

The Financial Policy Committee's (FPC) impact tolerance

3.11 In the March 2019 Record,[9] the FPC restated its agreement from June 2018 'that as part of establishing clear baseline expectations, it would set tolerances for how quickly critical financial companies must be able to restore vital financial services following a severe but plausible cyber incident. Consistent with the FPC's remit, these would be calibrated to ensure financial stability and avoid material economic harm. As such, the tolerances would not imply zero tolerance for disruption'.

3.12 The FPC is considering specific impact tolerances for the vital services, which have not been finalised. However, when these are published, the PRA will consult on them as necessary. The PRA may propose introducing policy under which firms that are identified as important contributors to these vital services are required to set their impact tolerances to meet the proposed operational resilience rules.

9 https://www.bankofengland.co.uk/financial-policy-summary-and-record/2019/march-2019.

4 Ability to remain within impact tolerances

4.1 The PRA's proposed new Operational Resilience Parts of the PRA Rulebook would require firms to be able to remain within impact tolerances. This would mean that boards and senior management would need to take action to improve operational resilience where the firm was not able to remain within the set tolerance for an important business service in a severe but plausible scenario. This would include taking action to address vulnerabilities in legacy systems. In addition, the draft SS sets out the PRA's expectations for firms, indicating different considerations and activities for firms that would enable them to meet the PRA's requirements, such as how firms should prioritise work or approach the use of third parties. The PRA will expect prompt and effective work to be undertaken when firms find they may be unable to remain within an impact tolerance. Firms whose important business services may pose a significant risk to financial stability would be expected to be particularly proactive at addressing vulnerabilities.

4.2 In order to improve the likelihood of firms being able to remain within impact tolerances, the PRA also proposes that some specific activities would be required by firms, including mapping, testing and preparing a self-assessment. The PRA considers that mapping would equip firms to understand the resources necessary to deliver important business services and decide how to manage them to support service delivery in the event of disruption. Testing would provide evidence as to whether the planned arrangements for disruption are likely to be effective in enabling the firm to remain within its impact tolerances. The work undertaken would need to be summarised in a self-assessment, which would be provided to the PRA on request.

Reasonable time to be able to remain within impact tolerances

4.3 The PRA is proposing rules to require firms to set, and take action to meet, standards of operational resilience that incorporate the public interest. To achieve this, the proposed Operational Resilience Parts would require firms to take action so that they are able to remain within their impact tolerance for each important business service in severe but plausible scenarios.

4.4 The DP indicated that the supervisory authorities will be proportionate in their approach to the implementation of operational resilience policy. The PRA recognises that some firms may currently have limitations in their ability to deliver important business services within impact tolerances. Accordingly, the PRA is proposing that firms must comply with the rule[10] within a reasonable time of it coming into effect, up to a maximum of three years.

4.5 The PRA considers that a 'reasonable time' will depend on a range of factors including the scale of the firm and its importance to the wider financial sector. These factors are unlikely to be outweighed by the complexity of operations, and the PRA would expect systemically-important financial institutions to be very active in addressing vulnerabilities they identify and consistent with this a 'reasonable time' would typically mean that prompt action was appropriate. The PRA considers that firms should agree the appropriate approach with their supervisory contact when the policy first comes into effect.

4.6 The PRA also recognises that circumstances may change as technology develops which might result in a firm no longer being able to remain within its impact tolerances for a period. The PRA would expect firms to agree an appropriately rapid remediation plan with their supervisory contact to restore their ability to remain within impact tolerances.

10 Operational Resilience – CRR Firms Part Rule 2.5, Operational Resilience – Solvency II Firms Part Rule 2.5.

4.7 Firms may identify vulnerabilities through the mapping and scenario testing work this policy would require (described below and in the draft SS) or from other information such as that relating to capacity specifications, recovery time objectives, or recovery point objectives. Firms should be able to demonstrate internally and to the PRA that the vulnerabilities they identify are managed and mitigated. The actions firms take to improve operational resilience, including through their investment decisions, should be prioritised based on factors such as the potential impact of disruptions, time criticality, and progress required to be able to remain within impact tolerances. This is set out in paragraph 4.5 of the draft SS.

4.8 Firms should prepare themselves for when disruptions occur. Paragraph 4.8 of the draft SS sets out that firms should develop communication strategies to prepare in advance how they can minimise the impact of disruptions. Firms should be ready to act quickly and effectively to reduce the amount of disruption caused by operational disruptions with the provision of clear, timely and relevant communications to their counterparties and other market participants. An effective communication strategy can help to prevent or mitigate the impact of a disruption to a firm's safety and soundness and to the appropriate degree of policyholder protection.

4.9 Paragraph 2.7 of the Appendix to CP30/19[11] sets out that the PRA would expect firms to consider outsourcing requirements when taking action to remain within impact tolerances. Firms should be able to remain within impact tolerance for important business services, irrespective of whether or not they use third parties in the delivery of these services.

Mapping

4.10 To ensure that an important business service could remain within its impact tolerance, firms would need to understand how the service is delivered and how it could be disrupted. This could become quite complex for some firms, especially where the people, processes, technology, facilities and information (resources) used to deliver important business services come from across business areas, entities, or different jurisdictions.

4.11 The proposed Operational Resilience Parts would require firms to identify and document resources required to deliver each of their important business services. This process is referred to as 'mapping'. The purpose of mapping is to identify the resources that are critical to delivering a service. This would help identification of business services, as well as facilitating robust scenario testing (see the section on scenario testing below) as it enables firms to design test scenarios that disrupt different combinations of an important business service's resources. Through this process firms could identify vulnerabilities in the delivery of their important business services.

4.12 Firms' mapping could highlight vulnerabilities in how important business services are being delivered, such as limited substitutability of resources, high complexity, single points of failure, and concentration risk. The proposed Operational Resilience Parts[12] would require firms to take action to remediate these vulnerabilities so that important business services could be delivered within impact tolerances.

4.13 Paragraph 5.2 in the draft SS would introduce the expectation that mapping should enable firms to identify vulnerabilities and test their ability to remain within impact tolerances.

4.14 Paragraph 5.3 in the draft SS sets out the PRA's proposed expectation that firms must take action where a vulnerability is identified or testing highlights a limitation to remaining within impact

11 CP30/19, 'Outsourcing and third party risk management', December 2019: https:/www.bankofengland.co.uk/prudential-regulation/publication/2019/outsourcing-and-third-party-risk-management.
12 Operational Resilience – CRR Firms Part Rule 2.5, Operational Resilience – Solvency II Firms Part Rule 2.5.

tolerances. Firms should use mapping for their own purposes and so are expected to develop their own methodology and assumptions to best fit their business.

4.15 Mapping information should be accessible and usable for the firm. Firms should document their mapping in a way proportionate to their size, scale and complexity. Documentation could take the form of a tool, application or database. This should be made available to the firm's supervisor on request.

Scenario testing

4.16 The proposed Operational Resilience Parts would require firms to test their ability to deliver important business services within impact tolerances in severe but plausible scenarios. This would help inform firms of vulnerabilities which might mean they are unable to remain within impact tolerances. Testing would also help firms to consider how they would respond to disruptions when they occur, including their incident management procedures, which would inform them about their ability to remain within impact tolerances.

4.17 Chapter 6 in the draft SS sets the expectation that firms should focus testing on response and recovery actions rather than focusing exclusively on preventing incidents from occurring. This is because impact tolerances assume a disruption has occurred, and the approach is designed to focus firms on how they would continue to deliver important business services in those circumstances.

4.18 Paragraph 6.5 in the draft SS sets out the PRA's proposed expectation that firms should develop a testing plan that details how they would gain assurance that they are able to remain within impact tolerances for their important business services. When considering the design and frequency of tests, the PRA proposes that firms should have regard to the potential impact on financial stability, safety and soundness, and policyholder protection of failure to deliver their important business services.

4.19 The nature and frequency of a firm's testing should be proportionate to its size and complexity. When developing a testing plan, the PRA proposes firms should consider the following:

- the type of scenario testing: this 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 undergo 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;
- 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.

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

4.21 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 would undertake is likely to be useful in informing them how their scenarios could be made more difficult.

4.22 The PRA recognises that it would not be proportionate to require firms to be able to remain within impact tolerances in all circumstances. There will be extreme 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.

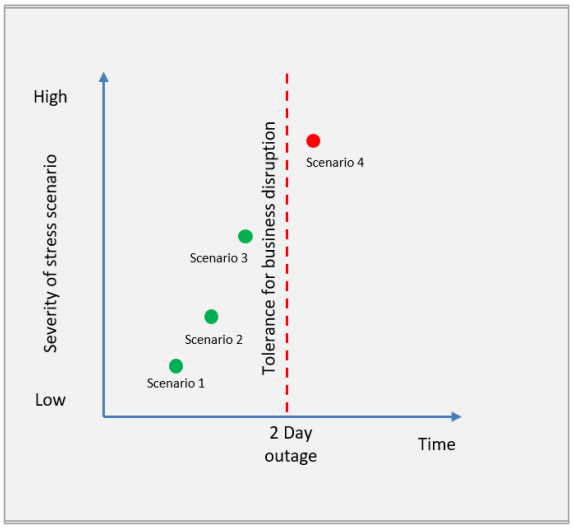
4.23 Impact tolerances are set on the assumption that disruptions will occur and we do not propose that firms devote too much time to considering the relative probability of incidents occurring. However, plausibility could be considered by modelling incidents or near misses that have occurred within a firm's organisation, across the financial sector, or in other sectors and jurisdictions.

4.24 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 would provide useful information to firms' management and to their supervisory contact. This is illustrated in Figure 3 below. 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.

4.25 The PRA does not currently propose to set scenarios for firms to use when testing their ability to remain within the impact tolerance for their important business services. However, it may do so at a future date if it considers it necessary.

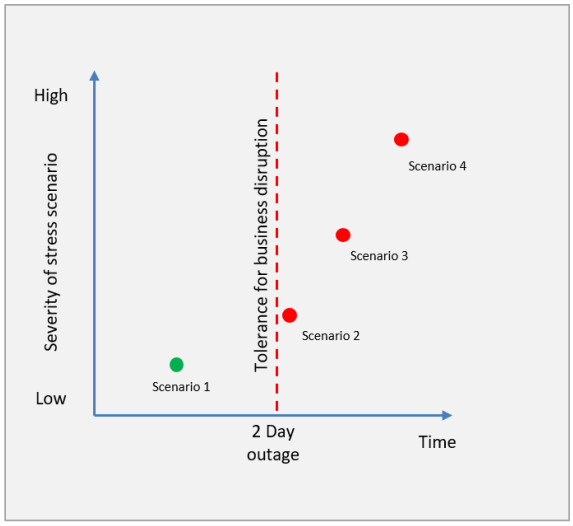
Figure 3: Some scenarios would see impact tolerances being exceeded

Case one: A firm considers its impact tolerance against severe but plausible scenarios. Operational resilience is sufficient – it is disproportionate to expect the firm not to breach its impact tolerance in the extreme scenario of scenario 4 .



Key
- Scenario recovered within tolerance
- Scenario not recovered within tolerance

Case two: A firm considers its impact tolerance against severe but plausible scenarios. In this case, operational resilience is not sufficient – the firm should take steps to improve operational resilience.



Key
- Scenario recovered within tolerance
- Scenario not recovered within tolerance

Governance

4.26 In addition to the specific requirements for boards to approve the important business services and the impact tolerances that have been set (outlined in the preceding chapters), the PRA would expect boards to satisfy themselves that their firm was meeting the requirements for having suitable strategies, processes and systems for identifying the important business services and setting the tolerances, and to perform mapping and testing.

4.27 Paragraph 7.2 of the draft SS sets out the PRA's proposals to expect a firm's board to have sufficient knowledge, skills and experience to meet its operational resilience responsibilities. This should ensure the board can challenge senior management constructively on the firm's operational resilience and the board will meet its oversight responsibilities.

4.28 The board would also be responsible under the proposed Operational Resilience Parts[13] for approving and regularly reviewing the firm's written self-assessment (see 'Self-assessment' below).

Self-assessment

4.29 The proposed Operational Resilience Parts would require firms to document a self-assessment of their compliance with the Operational Resilience Part. Firms would also be expected to document the methodology they have used to meet these requirements, such as how they have identified important business services and how they have set impact tolerances. The PRA proposes to expect firms to: summarise the vulnerabilities they have identified to the delivery of their important business services; and outline the scenario testing performed and the findings from the tests. The PRA would expect firms to indicate what actions are planned to improve their ability to remain within impact tolerances and demonstrate that the timing for these is reasonable and in proportion to the systemic importance of the firm's important business service. The PRA defines this documentation as self-assessment. Firms' boards and senior management would be accountable for,

13 Operational Resilience – CRR Firms Part Rule 7.3, Operational Resilience – Solvency II Firms Part Rule 7.3.

and should approve, the self-assessment. In line with Chapter 8 of the draft SS, firms would be expected to provide this to the PRA on request.

4.30 The self-assessment would enable firms to capture their work to test and build operational resilience. It would also, where requested by the PRA, enable supervisors to gain assurance of the operational resilience of firms, compare peers and scope the use of other tools and assessments.

4.31 Chapter 5 of the draft SS would set the expectation that firms map their important business services. The PRA does not propose to expect firms to include detailed mapping data as part of their self-assessment. The mapping approach would be included in the self-assessment to the extent necessary to meet the outcomes in paragraph 5.2 of the draft SS.

5 Groups

5.1 The PRA stated in CP19/17 'Groups Policy and Double Leverage'[14] that the principle for its overall approach to groups policy was that 'Banking groups should be resilient'. The PRA considers the same principle applicable to insurance groups. The principle is relevant to both operational and financial resilience. Therefore when applying the operational resilience policy set out in the proposed Operational Resilience Parts[15] and draft SS, the PRA proposes that it would expect a firm's self-assessment to cover the group.[16]

5.2 Taking a group-level view of operational resilience ensures the risks of the whole group, including those parts that are not subject to individual requirements, are taken into account. This would allow the PRA to understand the risks to the UK financial sector originating from groups.

5.3 Many of the PRA's existing relevant policies outlined in the draft SoP (see Appendix 4) apply at the level of the group, as well as on a solo level. These policies advance the group's overall operational resilience, however they do not achieve the same outcomes as the operational resilience policy. Therefore the PRA proposes to require firms to identify a proportionate number of important group business services[17] and respective impact tolerances at the level of the group.

5.4 Important group business services are provided to external group end users[18] by any part of the group, as set out in the proposed Operational Resilience Parts. In particular, boards and senior management should consider those services which, if disrupted, could (through their impact on the group as a whole) pose a risk to financial stability in the UK, the UK firm's safety and soundness, or (in the case of PRA-regulated insurers) the appropriate degree of protection for those who are or may become the firm's policyholders.

5.5 Impact tolerances should be set in the same way as they are for an individual firm. Boards and senior management should consider the level of disruption that would represent a threat to the viability of the group and therefore pose a risk to financial stability in the UK, a firm's safety and

14 December 2017 (page 2 of 2): www.bankofengland.co.uk/prudential-regulation/publication/2017/groups-policy-and-double-leverage.
15 Operational Resilience – CRR Firms Part 6, Operational Resilience – Solvency II Firms Part 6.
16 In the case of banks, this means the consolidation group of which the firm is a member on the basis of the consolidation situation of the UK parent undertaking. In the case of insurers it means the Solvency II group where the PRA is group supervisor.
17 Operational Resilience – CRR Firms Part 1, Operational Resilience – Solvency II Firms Part 1.
18 Definition of group external end user in Operational Resilience – CRR Firms Part and Operational Resilience – Solvency II Firms Part.

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.

5.6 Proposed Operational Resilience Parts[19] require that firms ensure that the strategies, processes and systems at the level of their group enable the firm to assess whether important group business services are able to remain within their impact tolerances in severe but plausible scenarios. A firm would be expected to work with other members of its group to take action should it be likely that an important group business service could not be delivered within its impact tolerance. Firms would be required to include this analysis in their self-assessments.

5.7 In addition, when applying the operational resilience policy at the solo level, the proposed Operational Resilience Parts would require firms that are a member of a group to identify and manage any risks that arise elsewhere in the group (not restricted to the consolidated group) that could impact the firm's ability to remain within its impact tolerances in the event of a severe but plausible disruption.

6 The PRA's statutory obligations

6.1 In carrying out its policy-making functions, the PRA is required to comply with several legal obligations. Before making any rules, FSMA[20] requires the PRA to publish a draft of the proposed rules accompanied by:

- a cost benefit analysis;
- an explanation of the PRA's reasons for believing that making the proposed rules is compatible with the PRA's duty to act in a way that advances its general objective,[21] insurance objective[22] (if applicable), and secondary competition objective;[23]
- an explanation of the PRA's reasons for believing that making the proposed rules are compatible with its duty to have regard to the regulatory principles;[24] and
- a statement as to whether the impact of the proposed rules will be significantly different to mutuals than to other persons.[25]

6.2 The Prudential Regulation Committee (PRC) should have regard to aspects of the Government's economic policy as recommended by HM Treasury.[26]

19 Operational Resilience – CRR Firms Part Rule 8.4, Group Supervision Part Rule 22.5.
20 Section 138J of FSMA.
21 Section 2B of FSMA.
22 Section 2C of FSMA.
23 Section 2H(1) of FSMA.
24 Sections 2H(2) and 3B of FSMA.
25 Section 138K of FSMA.
26 Section 30B of the Bank of England Act 1998.

6.3 The PRA is also required by the Equality Act 2010[27] to have due regard to the need to eliminate discrimination and to promote equality of opportunity in carrying out its policies, services and functions.

Cost benefit analysis

Introduction

6.4 The proposals made in this CP would drive firms to make changes in their approach to managing key aspects of their operational resilience. Firms would be required to identify their important business services, set clear standards for managing their resilience and ensure they meet those standards. Boards and senior management would be expected to consider operational resilience when making strategic decisions (including at the group level where appropriate). Because important business services and impact tolerances would be set with reference to: (i) firms' safety and soundness; (ii) financial stability; and (iii) in the case of insurers, the appropriate degree of policyholder protection, benefits would accrue in these areas.

6.5 This cost benefit analysis (CBA) sets out what types of change the PRA expects to see if the proposals were to be implemented, the benefits that would be likely to arise and indicates some of the costs that firms might incur as a result of the proposed policy.

Changes firms might make

6.6 Firms' work to meet the proposed policy requirements would provide them with a clear view of the important business services they provide. Their mapping and testing would give firms valuable insight into how these services are delivered and how risks to their delivery can be most effectively addressed in the event of disruption. Firms would need to be able to remain within impact tolerance. Boards and senior leadership would need to consider operational resilience when making strategic decisions. To remain within impact tolerance, firms are likely to need to take a variety of actions, such as renewing legacy IT infrastructure, providing more staff training, improving their communication plans, or strengthening existing processes for their governance or operations, including where they use third parties to help deliver important business services.

Benefits

(i) Safety and soundness: Requiring firms to remain within impact tolerances for their important business services would help mitigate the impact of operational disruptions on firms themselves. While firms already mitigate the financial cost of operational failure with operational risk capital, the PRA's proposals would ensure due attention is also paid to the potential operational effects. The policy would be implemented in a proportionate way. Managers at small and large firms would frequently be taking different actions to be able to remain within impact tolerance for their important business service. However, the outcome would be that their firms are better placed from their advanced preparations to respond to disruptions, and less likely to fail.

Financial stability: Improvements to firms' operational resilience would support the orderly functioning of the financial sector and increase confidence in the financial sector. A more operationally-resilient financial sector would be better placed to serve the UK economy. When implemented, the proposals made in this CP are designed to reduce the impact of operational disruptions, including severe but plausible ones, on firms. For example, these events could be of the magnitude of the TSB migration failure in 2018 (a loss of £330.2 million including post

[27] Section 149.

migration costs, fraud and foregone income),[28] the RBS IT failure in 2012 (10% of the UK population affected),[29] or greater.

The aligned approach being taken by the PRA, FCA and the Bank is expected to amplify the benefits of the proposals in this CP for financial stability, as firms will be able to have more confidence in the operational resilience arrangements of those within the scope of the proposals.

(ii) Policyholder protection: Evidence from past operational failures shows that consumers are often the first to suffer the consequences.[30] We expect benefits from these proposals to also accrue to consumers, including insurance policyholders. For example, insurers' important business services could include the payment of annuities, and improvements to the resilience of these would help protect policyholders' interests.

Costs

Method

6.7 We have made estimates for the cost of implementing the policy for 'small' and 'large' PRA-regulated firms. These estimates have been calculated using survey data submitted by PRA-regulated firms to the FCA and we have analysed the detailed responses from 46 firms. We categorised the sample into 'small' and 'large' using a combination of metrics provided in the survey data and regulatory returns. The categories of 'small' and 'large' are for the purposes of this CBA specifically, and therefore do not directly correspond to other categorisations such as medium and large in the FCA's CBA in CP19/32: 'Building operational resilience: impact tolerances for important business services and feedback to DP18/04'. Differences are a reflection of the different firms in scope of the PRA and the FCA proposals for operational resilience. Each Authority has checked its findings and concluded that our respective results are consistent with one another.

6.8 For dual-regulated firms, these costs are aligned with those presented in the FCA's CBA and do not reflect additional costs on top of the FCA's costs. Rather, these solely reflect the costs of the PRA's proposals.

6.9 Our CBA estimates are subject to several uncertainties and assumptions:

- Firms might have found it difficult when responding to the FCA's costs survey to envisage costs of operating and implementing the proposed policy framework without having sight of the final policy. In particular, firms may not have considered the costs incurred by the parts of the policy that apply to groups.

- Some firms may have misinterpreted how the requirements will apply or the extent to which they will replace existing compliance activities, thereby resulting in inaccurate cost estimations.

28 https://www.tsb.co.uk/news-releases/tsb-announces-2018-full-year-results/.
29 Paragraph 2.8, https://www.fca.org.uk/publication/final-notices/rbs-natwest-ulster-final-notice.pdf.
30 For example, 10% of the UK population was impacted by the RBS IT failure in 2012 (Paragraph 2.8, https://www.fca.org.uk/publication/final-notices/rbs-natwest-ulster-final-notice.pdf), Tesco Bank had to refund £2.5 million to 9,000 consumers following the 2018 cyber attack (https://www.bbc.co.uk/news/business-37915755), and the TSB migration failure in 2018 resulted in at least 204,000 consumer complaints (https://www.tsb.co.uk/news-releases/tsb-announces-2018-full-year-results/).

One-off and ongoing costs

6.10 In each size bracket there is also a long tail of responses that report high costs (well in excess of the confidence intervals for Table 1). This probably reflects their business models and the number of important business services that they operate.

Table 1: Average total costs per firm[31]

Size of firm	One-off costs	Ongoing costs (annual)
Large	£850,000 to £1.9 million	£400,000 to £850,000
Small	£100,000 to £500,000	£50,000 to £200,000

6.11 In assessing the data, the PRA has considered that there are likely to be costs related to making the policy operational (eg identifying important business services and setting impact tolerances), but also costs that are incurred to build operational resilience in order to be able to remain within tolerances (eg upgrading IT infrastructure). The latter types of costs will vary from firm to firm. In our assessment, we have considered that costs incurred to build operational resilience could far exceed the data presented in Table 1, but have not attempted to quantify them.

6.12 The PRA expects that in future years, costs related to important business service identification, mapping, and impact tolerance setting will decrease for firms, because of the embedding of processes and acquired experience. Costs related to testing may remain constant or grow as firms become sophisticated in their approaches to testing. Governance costs are expected to remain stable.

6.13 The proposals would apply to Capital Requirements Regulations (CRR) and Solvency II firms. The PRA does not anticipate that costs will vary because of the type of business a firm provides, for example, insurance or banking services.

Summary

6.14 The PRA considers that both firms and financial stability will materially benefit from more operationally-resilient firms. In the context of an increasing risk environment, the proposals will mitigate the impact of large operational failures.

6.15 Overall, comparing the costs and benefits from the proposals, the PRA considers that the benefits outweigh the costs.

Compatibility with the PRA's objectives

6.16 The PRA considers that the proposals in this CP advance its general objective to promote the safety and soundness of PRA-authorised firms; and in the context of insurance, to contribute to securing an appropriate degree of policyholder protection. When identifying important business services and setting impact tolerances, firms are expected to consider the impact of disruption on safety and soundness and the wider financial sector. The proposals would require firms to test and demonstrate their ability to remain within these impact tolerances, and would require them to address vulnerabilities that could affect their safety and soundness or impact on the wider financial sector.

6.17 In the context of insurance firms, important business service identification should also take into consideration the protection a policyholder requires from a business service. Setting an impact

31 95% confidence interval constructed using sample data and rounded to nearest £50,000.

tolerance for the delivery of this business service will contribute to policyholder protection, in addition to the overall safety and soundness of the insurance firm.

6.18 When discharging its general functions in a way that advances its objectives, the PRA has, as a secondary objective, a duty, as far as reasonably possible, to act in a way that facilitates effective competition in markets for services provided by PRA-regulated firms carrying on regulated activities. The PRA is proposing to apply the new rules and expectations to CRR and Solvency II firms. Within the scope of CRR and Solvency II firms the costs of the policy will be proportionate to the size and complexity of the firm, which facilitates competition. Larger and more complicated firms will be expected to identify more important business services and have more complex business services that require mapping.

Regulatory principles

6.19 In developing the proposals in this CP, the PRA has had regard to the regulatory principles set out in FSMA. Three principles of particular relevance are:

(i) The principle that a burden or restriction which is imposed on a person should be proportionate to the benefits which are expected to result from the imposition of that burden.

- The PRA has followed this principle when developing the proposals outlined in this CP. In particular, larger and more complex firms are expected to identify more important business services than smaller and simpler firms. The latter will therefore have less work to perform not only around identifying important business services but also around setting impact tolerances, mapping and testing them. The PRA has also been proportionate as the requirements for solo entities would not all apply at the group level.

(ii) The principle that the PRA uses its resources the most efficient and economic way.

- The proposed policy would support the PRA in supervising firms in an efficient and economic way, as clear standards would exist against which operational resilience management would be assessed.

(iii) The principle that the PRA should exercise its functions as transparently as possible.

- In this CP, the PRA consults on more details of its expectations for operational resilience, building upon other publications such as DP01/18[32] and the shared policy document. The proposals are consistent with responses to the DP and other industry engagement.

Impact on mutuals

6.20 The PRA considers that the impact of the proposed rules and expectations on mutuals would not differ from the impact on other firms.

---

32 July 2018: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.

HM Treasury recommendation letter

6.21 HM Treasury has made recommendations to the PRC about aspects of the Government's economic policy to which the PRC should have regard when considering how to advance the PRA's objectives and apply the regulatory principles.[33] These are: competition, growth, competitiveness, innovation, trade and better outcomes for consumers. The PRA has considered these in relation to these proposals. Of particular relevance is the impact on competition which is considered in the proposed scope of the policy, which excludes smaller firms from additional regulatory burden, and also as the identification of important business services would be proportionate. The recommendation of better outcomes for consumers would be achieved through firms investing in their operational resilience to be able to remain within impact tolerances.

6.22 The government's economic strategy set out in the HM Treasury letter includes 'continuing to strengthen the wider financial sector, improving the regulatory framework to reduce risks to the taxpayer and building resilience, so that it can provide finance and financial services to the real economy.' The proposals set out here would support that strategy as they are designed to strengthen the wider financial sector, improve the regulatory framework and build resilience.

Equality and diversity

6.23 The PRA considers that the proposals do not give rise to equality and diversity implications.

33 HM Treasury's recommendations are available on the Bank's website at https://www.bankofengland.co.uk/about/people/prudential-regulation-committee.

Appendices

Appendix 1: Draft Operational Resilience Parts

PRA RULEBOOK: CRR FIRMS, SOLVENCY II FIRMS: OPERATIONAL RESILIENCE INSTRUMENT 2020

Powers exercised

A. The Prudential Regulation Authority ("PRA") makes this instrument in the exercise of the following powers and related provisions in the Financial Services and Markets Act 2000 ("the Act"):

(1) section 137G (The PRA's general rules); and
(2) section 137T (General supplementary powers)

B. The rule-making powers referred to above are specified for the purpose of section 138G(2) (Rule-making instrument) of the Act.

Pre-conditions to making

C. In accordance with section 138J of the Act (Consultation by the PRA), the PRA consulted the Financial Conduct Authority. After consulting, the PRA published a draft of proposed rules and had regard to representations made.

PRA Rulebook: CRR Firms, Solvency II Firms: Operational Resilience Instrument 2020

D. The PRA makes the rules in Annexes to this instrument.

Part	Annex
Operational Resilience – CRR Firms	A
Operational Resilience – Solvency II Firms	B
Group Supervision	C

Commencement

E. This instrument comes into force on [DATE].

Citation

F. This instrument may be cited as the PRA Rulebook: CRR Firms, Solvency II Firms: Operational Resilience Instrument 2020.

By order of the Prudential Regulation Committee
[DATE]

Annex A

In this Annex, the text is all new and is not underlined.

Part

OPERATIONAL RESILIENCE – CRR FIRMS

Chapter content

1 APPLICATION AND DEFINITIONS

1.1 Unless otherwise stated, this Part applies to every *firm* that is a *CRR firm*.

1.2 In this Part, the following definitions shall apply:

external group end user

means a person who receives services and who is not a member of the firm's *consolidation group* on the basis of the *consolidated situation* of the *firm's UK parent undertaking*.

impact tolerance

means the maximum acceptable level of disruption for an *important business service* or an *important group business service.*

important business service

means a service provided by a *firm* to another *person* which, if disrupted, could pose a risk to:

(1) the stability of the *UK* financial system; or

(2) the *firm's* safety and soundness.

important group business service

means a service provided by a member of the *firm's consolidation group* (other than the *firm*) on the basis of the *consolidated situation* of the *UK parent undertaking* of that *consolidation group*, to an *external group end user* which, if disrupted, could pose a risk to:

(1) the stability of the *UK* financial system; or

(2) the *firm's* safety and soundness.

UK parent undertaking

means a *UK undertaking,* which is any of:

(1) a *financial holding company* which is not itself a *subsidiary* of an *institution* authorised in the *UK*, or of a *financial holding company* or *mixed financial holding company* also set up in the *UK*.

(2) a *mixed financial holding company* which is not itself a *subsidiary* of an *institution* authorised in the *UK*, or of a *financial holding company* or *mixed financial holding company* also set up in the *UK*.

(3) an *institution* authorised in the *UK* which has an *institution* or *financial institution* as a *subsidiary* or which holds a *participation* in such an *institution* or *financial institution*, and which is not itself a *subsidiary* of another *institution* also authorised in the *UK* or of a *financial holding company* or *mixed financial holding company* also set up in the *UK*.

1.3 Unless otherwise defined, any italicised expression used in this Part and in the *CRR* has the same meaning as in the *CRR*.

2 OPERATIONAL RESILIENCE REQUIREMENTS

2.1 A *firm* must identify its *important business services* and, where 8.2 applies, its *important group business services*.

2.2 A *firm* must, for each of its *important business services* and, where 8.2 applies, its *important group business services*, set an *impact tolerance*.

2.3 The *impact tolerance* set for each *important business service* or *important group business service* must specify the first point at which a disruption to the *important business service* or *important group business service* would pose a risk to:

(1) the stability of the *UK* financial system; or

(2) the *firm's* safety and soundness.

2.4 The *impact tolerance* set for each *important business service* or *important group business services* must, at a minimum, specify the length of time for which a disruption to that *important business service or important group business services* can be accepted.

2.5 A *firm* must ensure it can remain within its *impact tolerance* for each *important business service* in the event of a severe but plausible disruption to its operations.

2.6 A *firm* must comply with 2.5 within a reasonable time of the rule coming into effect and in any event by no later than [DD MM 2024].

3 STRATEGIES, PROCESSES AND SYSTEMS

3.1 A *firm* must have in place sound, effective and comprehensive strategies, processes and systems that enable it adequately to:

(1) identify its *important business services* and, where 8.2 applies, *important group business services*;

(2) set an *impact tolerance* for each *important business service* and, where 8.2 applies, each *important group business service*; and

(3) identify and address any risks to its ability to comply with the obligation under 2.5.

3.2 The strategies, processes and systems required by 3.1 must be proportionate to the nature, scale and complexity of the *firm's* activities.

4 MAPPING

4.1 As part of its obligation under 3.1, a *firm* must identify and document the necessary people, processes, technology, facilities and information required to deliver each of its *important business services*.

5 SCENARIO TESTING

5.1 As part of its obligation under 3.1, a *firm* must carry out regular scenario testing of its ability to remain within its *impact tolerance* for each of its *important business services* in the event of a severe but plausible disruption of its operations.

5.2 In carrying out the scenario testing required by 5.1, a *firm* must identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the risks to delivery of the *firm's important business services* in those circumstances.

5.3 The scenario testing required by 5.1 must be proportionate to the nature, scale and complexity of the *firm's* activities.

6 SELF-ASSESSMENT

6.1 A *firm* must prepare and regularly update a written self-assessment of its compliance with this Part.

6.2 The content and level of detail of a *firm's* written self-assessment must be proportionate to the nature, scale and complexity of the *firm's* activities, and where applicable to the activities of the *consolidation group* of which the firm is a member.

6.3 A *firm* must maintain, and be able to provide to the PRA on request, a current version of its written self-assessment, together with all versions produced during the preceding three years.

7 GOVERNANCE

7.1 A *firm* must ensure that its *management body* approves the *important business services* and *important group business services* identified by the *firm* in compliance with 2.1 and 8.2.

7.2 A *firm* must ensure that its *management body* approves the *impact tolerances* set by the *firm* in compliance with 2.2 and 8.2.

7.3 A *firm* must ensure that its *management body* approves and regularly reviews the self-assessment required by 6.1.

8 GROUP ARRANGEMENTS

8.1 Where a *firm* is a member of a *group*, the *firm* must ensure it accounts for any additional risks arising elsewhere in the *group* that may affect the *firm's* ability to comply with the obligation under 2.5.

8.2 Where a firm is a member of a *consolidation group*, the *firm* must also comply with 2.1 and 2.2 in relation to its *important group business services* on the basis of the *consolidated situation* of the *UK parent undertaking of the consolidation group*.

8.3 With the exception of 3.1.3, where a firm is a member of a *consolidation group*, the *firm* must ensure that the strategies, processes and systems at the level of the *consolidation group* of which it is a member comply with the obligations set out in 3 of this Part on the basis of the *consolidated situation* of the *UK parent undertaking of the consolidation group*.

8.4 Where a firm is a member of a *consolidation group*, the *firm* must ensure that the strategies, processes and systems at the level of its *consolidation group* enable the *firm* to assess on the basis of the *consolidated situation* of the *UK parent undertaking of the consolidation group* whether the member of that *consolidation group* providing each *important group business service* could remain within the *impact tolerance* in the event of a severe but plausible disruption to its operations.

8.5 The strategies, processes and systems required by this chapter must be proportionate to the nature, scale and complexity of the *consolidation group's* activities.

Annex B

In this Annex, the text is all new and is not underlined.

Part

OPERATIONAL RESILIENCE – SOLVENCY II FIRMS

Chapter content

1 APPLICATION AND DEFINITIONS

1.1 Unless otherwise stated, this Part applies:

(1) a *UK Solvency II firm*;

(2) in accordance with Insurance General Application 3, the *Society*, as modified by 9; and

(3) in accordance with Insurance General Application 3, *managing agents*, as modified by 9.

1.2 In this Part, the following definitions shall apply:

external group end user

means a person who receives services and who is outside of the *group* of which the *firm* is a member.

impact tolerance

means the maximum acceptable level of disruption for an *important business service* or an *important group business service.*

important business service

means a service provided by a *firm* to another *person* which, if disrupted, could pose a risk to:

(1) the stability of the *UK* financial system;

(2) the *firm's* safety and soundness; or

(3) an appropriate degree of protection for those who are or may become the *firm's policyholders.*

important group business service

means a service provided by a member of a *group* (other than the *firm*) to an *external group end user* which, if disrupted, could pose a risk to:

(1) the stability of the *UK* financial system;

(2) the *firm's* safety and soundness; or

(3) an appropriate degree of protection for those who are or may become the *firm's policyholders*.

1.3 Unless otherwise defined, any italicised expression used in this Part and in the *Solvency II Directive* has the same meaning as in the *Solvency II Directive*.

2 OPERATIONAL RESILIENCE REQUIREMENTS

2.1 A *firm* must identify its *important business services* and, where Group Supervision 22.2 applies, its *important group business services*.

2.2 A *firm* must, for each of its *important business services* and, where Group Supervision 22.2 applies, its *important group business services*, set an *impact tolerance*.

2.3 The *impact tolerance* set for each *important business service* or *important group business service* must specify the first point at which a disruption to the *important business service* or *important group business service* would pose a risk to:

(1) the stability of the *UK* financial system;

(2) the *firm's* safety and soundness; or

(3) an appropriate degree of protection for those who are or may become the *firm's policyholders*.

2.4 The *impact tolerance* set for each *important business service* or *important group business services* must, at a minimum, specify the length of time for which a disruption to that *important business service* or *important group business service* can be accepted.

2.5 A *firm* must ensure it can remain within its *impact tolerance* for each *important business service* in the event of a severe but plausible disruption to its operations.

2.6 A *firm* must comply with 2.5 within a reasonable time of the rule coming into effect and in any event by no later than [XX DD 2024].

3 STRATEGIES, PROCESSES AND SYSTEMS

3.1 A *firm* must have in place sound, effective and comprehensive strategies, processes and systems that enable it adequately to:

(1) identify its *important business services* and, where Group Supervision 22.2 applies, its *important group business services*;

(2) set an *impact tolerance* for each *important business service* and, where Group Supervision 22.2 applies, each *important group business service*; and

(3) identify and address any risks to its ability to comply with the obligation in 2.5.

3.2 The strategies, processes and systems required by 3.1 must be proportionate to the nature, scale and complexity of the *firm's* activities.

4 MAPPING

4.1 As part of its obligation under 3.1, a *firm* must identify and document the necessary people, processes, technology, facilities and information required to deliver each of its *important business services*.

5 SCENARIO TESTING

5.1 As part of its obligation under 3.1, a *firm* must carry out regular scenario testing of its ability to remain within its *impact tolerance* for each of its *important business services* in the event of a severe but plausible disruption of its operations.

5.2 In carrying out the scenario testing required by 5.1, a *firm* must identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the risks to delivery of the *firm's important business services* in those circumstances.

5.3 The scenario testing required by 5.1 must be proportionate to the nature, scale and complexity of the *firm's* activities.

6 SELF-ASSESSMENT

6.1 A *firm* must prepare and regularly update a written self-assessment of its compliance with this Part and Group Supervision 22.

6.2 The content and level of detail of a *firm's* written self-assessment must be proportionate to the nature, scale and complexity of the *firm's* activities and, where applicable, to the activities of the *group* of which the firm is a member.

6.3 A *firm* must maintain, and be able to provide to the PRA on request, a current version of its written self-assessment, together with all versions produced during the preceding three years.

7 GOVERNANCE

7.1 A *firm* must ensure that its *management body* approves the *important business services* and *important group business services* identified by the *firm* in compliance with 2.1 and Group Supervision 22.3.

7.2 A *firm* must ensure that its *management body* approves the *impact tolerances* set by the *firm* in compliance with 2.2 and Group Supervision 22.3.

7.3 A *firm* must ensure that its *management body* approves and regularly reviews the self-assessment required by 6.1.

8 GROUP ARRANGMENTS

8.1 Where a *firm* is a member of a *group*, the *firm* must ensure it accounts for any additional risks arising elsewhere in the *group* that may affect the *firm's* ability to comply with 2.5.

9 LLOYDS

9.1 This Part applies to the *Society* and *managing agents* separately.

Annex C

Amendments to the Group Supervision Part

In this Annex new text is underlined.

Part

GROUP SUPERVISION

Chapter content

...

22. OPERATIONAL RESILIENCE REQUIREMENTS

1 APPLICATION AND DEFINITIONS

…

1.2 In this Part, the following definitions shall apply:

…

external group end user

means a person who receives services and who is outside of the *group* of which the *firm* is a member.

…

important group business service

means a service provided by a member of a *group* (other than the *firm*) to an *external group end user* which, if disrupted, could pose a risk to:

(1) the stability of the *UK* financial system;

(2) the *firm's* safety and soundness; or

(3) an appropriate degree of protection for those who are or may become the *firm's policyholders*.

…

…

22 GROUP OPERATIONAL RESILIENCE

22.1 Rules 22.2 to 22.5 apply to any *UK Solvency II firm* that is a member of a *group* for which the *PRA* is the *group supervisor*.

22.2 Where a *firm* is a member of a *group* covered by 2.1(1), 2.1(2) or, subject to 22.5, 2.1(3), the *firm* must also comply with Operational Resilience – Solvency II Firms 2.1 and 2.2 in relation to its *important group business services*.

22.3 Where a *firm* is a member of a *group* covered by 2.1(1), 2.1(2) or, subject to 22.5, 2.1(3), with the exception of Operational Resilience – Solvency II Firms 3.1(3), the *firm* must ensure that the strategies, processes and systems at the level of the *group* of which it is a member comply with the obligations set out in Operational Resilience – Solvency II Firms 3.

22.4 Where a *firm* is a member of a *group* covered by 2.1(1), 2.1(2) or, subject to 22.5, 2.1(3) the *firm* must ensure that the strategies, processes and systems at the level of the *group* of which it is a member enable the *firm* to assess whether *important group business services* at the level of the *group* could remain within the *impact tolerance* in the event of a severe but plausible disruption to its operations.

22.5 Where a *firm* is a member of a *group* covered by 2.1(3), 22.2, 22.3 and 22.4 do not apply if, subject to 22.6, the third country in which the *group's parent undertaking* has its head office is assessed to be equivalent under Article 260 of the *Solvency II Directive*.

22.6 22.5 does not apply where, in the case of temporary equivalence under Article 260(5) of the *Solvency II Directive*, there is a *Solvency II undertaking* in the *group* that has a balance sheet total that exceeds the balance sheet total of the *parent undertaking* situated outside of the *EEA*.

EXTERNALLY DEFINED TERMS

Term	Definition source
consolidated situation	Article 4(1)(47) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
financial institution	Article 4(1)(26) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
financial holding company	Article 4(1)(20) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
institution	Article 4(1)(3) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
mixed financial holding company	Article 4(1)(21) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
subsidiary	Article 4(1)(16) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012

Appendix 2: Draft Operational Resilience Parts in the event of a no-deal Brexit

PRA RULEBOOK: CRR FIRMS, SOLVENCY II FIRMS: OPERATIONAL RESILIENCE INSTRUMENT 2020

Powers exercised

A. The Prudential Regulation Authority ("PRA") makes this instrument in the exercise of the following powers and related provisions in the Financial Services and Markets Act 2000 ("the Act"):

(3) section 137G (The PRA's general rules); and
(4) section 137T (General supplementary powers)

B. The rule-making powers referred to above are specified for the purpose of section 138G(2) (Rule-making instrument) of the Act.

Pre-conditions to making

C. In accordance with section 138J of the Act (Consultation by the PRA), the PRA consulted the Financial Conduct Authority. After consulting, the PRA published a draft of proposed rules and had regard to representations made.

PRA Rulebook: CRR Firms, Solvency II Firms: Operational Resilience Instrument 2020

D. The PRA makes the rules in Annexes to this instrument.

Part	Annex
Operational Resilience – CRR Firms	A
Operational Resilience – Solvency II Firms	B
Group Supervision	C

Commencement

E. This instrument comes into force on [DATE].

Citation

F. This instrument may be cited as the PRA Rulebook: CRR Firms, Solvency II Firms: Operational Resilience Instrument 2020.

By order of the Prudential Regulation Committee
[DATE]

Annex A

In this Annex, the text is all new and is not underlined.

Part

OPERATIONAL RESILIENCE – CRR FIRMS

Chapter content

1 APPLICATION AND DEFINITIONS

1.1 Unless otherwise stated, this Part applies to every *firm* that is a *CRR firm*.

1.2 In this Part, the following definitions shall apply:

external group end user

means a person who receives services and who is not a member of the firm's *consolidation group* on the basis of the *consolidated situation* of the *firm's UK parent undertaking*.

impact tolerance

means the maximum acceptable level of disruption for an *important business service* or an *important group business service.*

important business service

means a service provided by a *firm* to another *person* which, if disrupted, could pose a risk to:

(1) the stability of the *UK* financial system; or

(2) the *firm's* safety and soundness.

important group business service

means a service provided by a member of the *firm's consolidation group* (other than the *firm*) on the basis of the *consolidated situation* of the *UK parent undertaking* of that *consolidation group*, to an *external group end user* which, if disrupted, could pose a risk to:

(1) the stability of the *UK* financial system; or

(2) the *firm's* safety and soundness.

1.3 Unless otherwise defined, any italicised expression used in this Part and in the *CRR* has the same meaning as in the *CRR*.

2 OPERATIONAL RESILIENCE REQUIREMENTS

2.1 A *firm* must identify its *important business services* and, where 8.2 applies, its *important group business services*.

2.2 A *firm* must, for each of its *important business services* and, where 8.2 applies, its *important group business services*, set an *impact tolerance*.

2.3 The *impact tolerance* set for each *important business service* or *important group business service* must specify the first point at which a disruption to the *important business service* or *important group business service* would pose a risk to:

(3) the stability of the *UK* financial system; or

(4) the *firm's* safety and soundness.

2.4 The *impact tolerance* set for each *important business service* or *important group business services* must, at a minimum, specify the length of time for which a disruption to that *important business service or important group business services* can be accepted.

2.5 A *firm* must ensure it can remain within its *impact tolerance* for each *important business service* in the event of a severe but plausible disruption to its operations.

2.6 A *firm* must comply with 2.5 within a reasonable time of the rule coming into effect and in any event by no later than [XX DD 2024].

3 STRATEGIES, PROCESSES AND SYSTEMS

3.1 A *firm* must have in place sound, effective and comprehensive strategies, processes and systems that enable it adequately to:

(1) identify its *important business services* and, where 8.2 applies, *important group business services*;

(2) set an *impact tolerance* for each *important business service* and, where 8.2 applies, each *important group business service*; and

(3) identify and address any risks to its ability to comply with the obligation under 2.5.

3.2 The strategies, processes and systems required by 3.1 must be proportionate to the nature, scale and complexity of the *firm's* activities.

4 MAPPING

4.1 As part of its obligation under 3.1, a *firm* must identify and document the necessary people, processes, technology, facilities and information required to deliver each of its *important business services*.

5 SCENARIO TESTING

5.1 As part of its obligation under 3.1, a *firm* must carry out regular scenario testing of its ability to remain within its *impact tolerance* for each of its *important business services* in the event of a severe but plausible disruption of its operations.

5.2 In carrying out the scenario testing required by 5.1, a *firm* must identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the risks to delivery of the *firm's important business services* in those circumstances.

5.3 The scenario testing required by 5.1 must be proportionate to the nature, scale and complexity of the *firm's* activities.

6 SELF-ASSESSMENT

6.1 A *firm* must prepare and regularly update a written self-assessment of its compliance with this Part.

6.2 The content and level of detail of a *firm's* written self-assessment must be proportionate to the nature, scale and complexity of the *firm's* activities, and where applicable to the activities of the *consolidation group* of which the firm is a member.

6.3 A *firm* must maintain, and be able to provide to the PRA on request, a current version of its written self-assessment, together with all versions produced during the preceding three years.

7 GOVERNANCE

7.1 A *firm* must ensure that its *management body* approves the *important business services* and *important group business services* identified by the *firm* in compliance with 2.1 and 8.2.

7.2 A *firm* must ensure that its *management body* approves the *impact tolerances* set by the *firm* in compliance with 2.2 and 8.2.

7.3 A *firm* must ensure that its *management body* approves and regularly reviews the self-assessment required by 6.1.

8 GROUP ARRANGEMENTS

8.1 Where a *firm* is a member of a *group*, the *firm* must ensure it accounts for any additional risks arising elsewhere in the *group* that may affect the *firm's* ability to comply with the obligation under 2.5.

8.2 Where a firm is a member of a *consolidation group*, the *firm* must also comply with 2.1 and 2.2 in relation to its *important group business services* on the basis of the *consolidated situation* of the *UK parent undertaking of the consolidation group*.

8.3 With the exception of 3.1.3, where a firm is a member of a *consolidation group*, the *firm* must ensure that the strategies, processes and systems at the level of the *consolidation group* of which it is a member comply with the obligations set out in 3 of this Part on the basis of the *consolidated situation* of the *UK parent undertaking of the consolidation group*.

8.4 Where a firm is a member of a *consolidation group*, the *firm* must ensure that the strategies, processes and systems at the level of its *consolidation group* enable the *firm* to assess on the basis of the *consolidated situation* of the *UK parent undertaking of the consolidation group* whether the member of that *consolidation group* providing each *important group business service* could remain within the *impact tolerance* in the event of a severe but plausible disruption to its operations.

8.5 The strategies, processes and systems required by this chapter must be proportionate to the nature, scale and complexity of the *consolidation group's* activities.

Annex B

In this Annex, the text is all new and is not underlined.

Part

OPERATIONAL RESILIENCE – SOLVENCY II FIRMS

Chapter content

1 APPLICATION AND DEFINITIONS

1.1 Unless otherwise stated, this Part applies:

(1) a *UK Solvency II firm*;

(2) in accordance with Insurance General Application 3, the *Society*, as modified by 9; and

(3) in accordance with Insurance General Application 3, *managing agents*, as modified by 9.

1.2 In this Part, the following definitions shall apply:

external group end user

means a person who receives services and who is outside of the *group* of which the *firm* is a member.

impact tolerance

means the maximum acceptable level of disruption for an *important business service* or an *important group business service.*

important business service

means a service provided by a *firm* to another *person* which, if disrupted, could pose a risk to:

(1) the stability of the *UK* financial system;

(2) the *firm's* safety and soundness; or

(3) an appropriate degree of protection for those who are or may become the *firm's policyholders.*

important group business service

means a service provided by a member of a *group* (other than the *firm*) to an *external group end user* which, if disrupted, could pose a risk to:

(1) the stability of the *UK* financial system;

(2) the *firm's* safety and soundness; or

(3) an appropriate degree of protection for those who are or may become the *firm's policyholders*.

1.3 Unless otherwise defined, any italicised expression used in this Part and in the *Solvency II Directive* has the same meaning as in the *Solvency II Directive*.

2 OPERATIONAL RESILIENCE REQUIREMENTS

2.1 A *firm* must identify its *important business services* and, where Group Supervision 22.2 applies, its *important group business services*.

2.2 A *firm* must, for each of its *important business services* and, where Group Supervision 22.2 applies, its *important group business services*, set an *impact tolerance*.

2.3 The *impact tolerance* set for each *important business service* or *important group business service* must specify the first point at which a disruption to the *important business service* or *important group business service* would pose a risk to:

(4) the stability of the *UK* financial system;

(5) the *firm's* safety and soundness; or

(6) an appropriate degree of protection for those who are or may become the *firm's policyholders*.

2.4 The *impact tolerance* set for each *important business service* or *important group business services* must, at a minimum, specify the length of time for which a disruption to that *important business service* or *important group business service* can be accepted.

2.5 A *firm* must ensure it can remain within its *impact tolerance* for each *important business service* in the event of a severe but plausible disruption to its operations.

2.6 A *firm* must comply with 2.5 within a reasonable time of the rule coming into effect and in any event by no later than [XX DD 2024].

3 STRATEGIES, PROCESSES AND SYSTEMS

3.1 A *firm* must have in place sound, effective and comprehensive strategies, processes and systems that enable it adequately to:

(1) identify its *important business services* and, where Group Supervision 22.2 applies, its *important group business services*;

(2) set an *impact tolerance* for each *important business service* and, where Group Supervision 22.2 applies, each *important group business service*; and

(3) identify and address any risks to its ability to comply with the obligation in 2.5.

3.2 The strategies, processes and systems required by 3.1 must be proportionate to the nature, scale and complexity of the *firm's* activities.

4 MAPPING

4.1 As part of its obligation under 3.1, a *firm* must identify and document the necessary people, processes, technology, facilities and information required to deliver each of its *important business services*.

5 SCENARIO TESTING

5.1 As part of its obligation under 3.1, a *firm* must carry out regular scenario testing of its ability to remain within its *impact tolerance* for each of its *important business services* in the event of a severe but plausible disruption of its operations.

5.2 In carrying out the scenario testing required by 5.1, a *firm* must identify an appropriate range of adverse circumstances of varying nature, severity and duration relevant to its business and risk profile and consider the risks to delivery of the *firm's important business services* in those circumstances.

5.3 The scenario testing required by 5.1 must be proportionate to the nature, scale and complexity of the *firm's* activities.

6 SELF-ASSESSMENT

6.1 A *firm* must prepare and regularly update a written self-assessment of its compliance with this Part and Group Supervision 22.

6.2 The content and level of detail of a *firm's* written self-assessment must be proportionate to the nature, scale and complexity of the *firm's* activities and, where applicable, to the activities of the *group* of which the firm is a member.

6.3 A *firm* must maintain, and be able to provide to the PRA on request, a current version of its written self-assessment, together with all versions produced during the preceding three years.

7 GOVERNANCE

7.1 A *firm* must ensure that its *management body* approves the *important business services* and *important group business services* identified by the *firm* in compliance with 2.1 and Group Supervision 22.3.

7.2 A *firm* must ensure that its *management body* approves the *impact tolerances* set by the *firm* in compliance with 2.2 and Group Supervision 22.3.

7.3 A *firm* must ensure that its *management body* approves and regularly reviews the self-assessment required by 6.1.

8 GROUP ARRANGMENTS

8.1 Where a *firm* is a member of a *group*, the *firm* must ensure it accounts for any additional risks arising elsewhere in the *group* that may affect the *firm's* ability to comply with 2.5.

9 LLOYDS

9.1 This Part applies to the *Society* and *managing agents* separately.

Annex C

Amendments to the Group Supervision Part

In this Annex new text is underlined.

Part

GROUP SUPERVISION

Chapter content

1 APPLICATION AND DEFINITIONS

…

1.2 In this Part, the following definitions shall apply:

…

external group end user

means a person who receives services and who is outside of the *group* of which the *firm* is a member.

…

important group business service

means a service provided by a member of a *group* (other than the *firm*) to an *external group end user* which, if disrupted, could pose a risk to:

(1) the stability of the *UK* financial system;

(2) the *firm's* safety and soundness; or

(3) an appropriate degree of protection for those who are or may become the *firm's policyholders*.

…

…

22 GROUP OPERATIONAL RESILIENCE

22.1 Rules 22.2 to 22.5 apply to any *UK Solvency II firm* that is a member of a *group* for which the *PRA* is the *group supervisor*.

22.2 Where a *firm* is a member of a *group* covered by 2.1(1), 2.1(2) or, subject to 22.5, 2.1(3), the *firm* must comply with Operational Resilience – Solvency II Firms 2.1 and 2.2 in relation to its *important group business services*.

22.3 Where a *firm* is a member of a *group* covered by 2.1(1), 2.1(2) or, subject to 22.5, 2.1(3), with the exception of Operational Resilience – Solvency II Firms 3.1(3), the *firm* must ensure that the strategies, processes and systems at the level of the *group* of which it is a member comply with the obligations set out in Operational Resilience – Solvency II Firms 3.

22.4 Where a *firm* is a member of a *group* covered by 2.1(1), 2.1(2) or, subject to 22.5, 2.1(3) the *firm* must ensure that the strategies, processes and systems at the level of the *group* of which it is a member enable the *firm* to assess whether *important group business services* at the level of the *group* could remain within the *impact tolerance* in the event of a severe but plausible disruption to its operations.

22.5 Where a *firm* is a member of a *group* covered by 2.1(3), 22.2, 22.3 and 22.4 do not apply if, subject to 22.6, the third country in which the *group's parent undertaking* has its head office is assessed to be equivalent under provisions implementing Article 260 of the *Solvency II Directive,* Article 380 and 380A of the *delegated act*, or an equivalence determination under paragraph 12 of Schedule 1 of The Equivalence Determinations for Financial Services and Miscellaneous Provisions (Amendment etc) (EU Exit) Regulations 2019.

22.6 22.5 does not apply where, in the case of temporary equivalence under Article 260(5) of the *Solvency II Directive*, there is a *Solvency II undertaking* in the *group* that has a balance sheet total that exceeds the balance sheet total of the *parent undertaking* situated outside of the *UK* and Gibraltar.

EXTERNALLY DEFINED TERMS

Term	Definition source
consolidated situation	Article 4(1)(47) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
financial institution	Article 4(1)(26) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
financial holding company	Article 4(1)(20) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
institution	Article 4(1)(3) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
mixed financial holding company	Article 4(1)(21) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012
subsidiary	Article 4(1)(16) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012

Appendix 3: Draft Supervisory Statement 'Operational Resilience: Impact tolerances for important business services'

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 (defined in Chapter 2 and 3 respectively). The policy objective is to improve the resilience of both firms and the wider financial sector to operational disruptions.

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

1.3 The SS 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').

1.4 Banks and insurers are collectively referred to as 'firms' in this SS.

1.5 Operational resilience in this SS refers to the ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover 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'[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 The PRA has developed this policy jointly with the Bank of England (Bank), in its capacity as a supervisor of Financial Market Infrastructures (FMIs), and with the Financial Conduct Authority

[1] Operational Resilience – CRR Firms Part; Operational Resilience – Solvency II Firms Part and the Operational Resilience rules in the Group Supervision Part.

(FCA). A discussion of the aligned approach the supervisory authorities intend to take to operational resilience is set out in the covering paper 'Building operational resilience: Impact tolerances for important business services'.[2] This SS complements, and should be read in conjunction with, the:

- PRA's approach to banking supervision or the PRA's approach to insurance supervision;[3]
- Fundamental Rules part of the PRA Rulebook;[4]
- Operational Resilience Parts of the PRA Rulebook;
- PRA's Statement of Policy on Operational resilience;
- SSxx/xx 'Outsourcing and third-party risk management'; and
- FCA's [rules and guidance in SS XX/XX].

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 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,[5] 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 financial stability. The Operational Resilience Parts[6] 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, the firm's safety and soundness and, in the case of insurers, policyholder protection.

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, the firm's safety and soundness and, in the case of insurers, 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 December 2019: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.
3 Available at: https://www.bankofengland.co.uk/prudential-regulation/publication/pras-approach-to-supervision-of-the-banking-and-insurance-sectors.
4 Fundamental rule 2, 3, 5 and 6 are particularly relevant for this example.
5 Operational Resilience – CRR Firms Part Rule 2.1, Operational Resilience – Solvency II Firms Part Rule 2.1.
6 Definition of 'important business service' in Operational Resilience – Solvency II Firms Part.

- the potential to inhibit the functioning of the wider economy, in particular the economic functions listed in SS19/13 'Recovery planning';[7]

- 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 policyholders affected by a disruption to the service including consideration for:

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

- the significance to the policyholder of the risk insured;

- 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, employees or business units of the regulated entity, 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 (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 work the PRA requires firms to perform.

2.8 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.

---

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

3 Impact tolerances

Setting an impact tolerance

3.1 The Operational Resilience Parts[8] 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 acceptable level of disruption to an important business service.

3.2 The Operational Resilience Parts[9] 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 financial stability of the UK, the firm's safety and soundness, or, in the case of insurers, policyholder protection.

3.3 Some firms may conclude there is no level of disruption to an important business service which could pose a risk to financial stability.

3.4 Impact tolerances provide a standard which boards and senior management should use for prioritising investment and making contingency 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.

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 should, in all cases, state the maximum time for which the firm can tolerate disruption to an important business service. Impact tolerances may also state additional metrics such as the volume or value of transactions that the firm can tolerate being missed or delayed for that period of disruption.

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 put the firm's safety and soundness, financial stability or policy holder protection at risk, the firm could consider the impact of a longer disruption. If, for example, after an important business service has been unavailable for five days, the firm judges that financial stability would be at risk, 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, financial stability or policyholder protection is at risk, firms should consider identifying indicators. In identifying indicators, firms should consider the factors identified in paragraph [2.4] of this SS.

3.9 Impact tolerances are defined as the maximum acceptable amount of disruption and should apply at peak times as well as in normal circumstances. As such, when setting 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.

---

8 Operational Resilience – CRR Firms Part Rule 2.1, Operational Resilience – Solvency II Firms Part Rule 2.1.
9 Operational Resilience – CRR Firms Part Rule 2.3, Operational Resilience – Solvency II Firms Part Rule 2.3.

3.11 The PRA expects firms to use a time-based metric for all impact tolerances, but in some cases, firms may find it suitable to use this in combination with other metrics. 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 time. 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.

3.12 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.

3.13 Setting an impact tolerance enables firms to 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 its important business service within its impact tolerance.

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

3.15 The PRA's fundamental rules[10] 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 under which they may decide not to resume functioning of their important business services within the specified time.

4 Actions to remain within impact tolerance

4.1 The Operational Resilience Parts[11] 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 remain within an impact tolerance – these factors are themselves vulnerabilities that the PRA expects firms to address.

4.3 However, the PRA intends to apply the principle of proportionality, including where it may take time to improve the resilience of important business services to ensure they are delivered within impact tolerances. Firms may require time to improve the operational resilience of important business services in the face of rapid technological change for example. When the policy first comes into force, the firms will have reasonable time to take action up to a maximum of three years.

4.4 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

10 Fundamental rule 2, 3, 5 and 6 are particularly relevant for this example.
11 Operational Resilience – CRR Firms Part Rule 2.5, Operational Resilience – Solvency II Firms Part Rule 2.5.

prompt action where they cannot remain within impact tolerance, so these plans should include appropriate timing for the necessary improvements.

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

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

4.6 Paragraph 2.8 of SSxx/xx sets out that 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.

4.7 Although firms could 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.

4.8 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.

5 Mapping

5.1 The Operational Resilience Parts[12] require firms to identify and document the necessary people, processes, technology, facilities and information (the 'resources') required to deliver each of its 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 and ascertain what would happen if resources were to become unavailable.

12 Operational Resilience – CRR Firms Part 4.1, Operational Resilience – Solvency II Firms Part 4.1.

(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 Operational Resilience Parts[13], 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 them being provided by a third party, which may be external or another entity in the group. Paragraph 9.5 of SSxx/xx sets out that firms should also, at a minimum, monitor sub-outsourced service providers involved in the provision of important business services as part of their mapping, including their ability to deliver the firm's important business services within the firm's impact tolerances.

5.6 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.

5.7 Firms should update their mapping annually at a minimum or following significant change if sooner.

6 Scenario testing

6.1 The Operational Resilience Parts[14] require firms to test 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 response and recovery actions.

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

13 Operational Resilience – CRR Firms Part Rule 2.5, Operational Resilience – Solvency II Firms Part Rule 2.5.
14 Operational Resilience – CRR Firms Part 5, Operational Resilience – Solvency II Firms Part 5.
15 Operational Resilience – CRR Firms Part 6, Operational Resilience – Solvency II Firms Part 6.

6.5 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 disruption could cause. When developing a testing plan, firms should consider the following:

- 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.

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

6.7 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.

6.8 The PRA recognises that it would not be proportionate to require firms to be able to remain within impact tolerances in all circumstances. 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.

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

6.10 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.

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[16] 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.[17]

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,[18] the Chief Operations role 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'[19] and paragraph 2.22L of SS35/15 'Strengthening individual accountability in insurance',[20] 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 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.[21]

8 Self-assessment

8.1 The Operational Resilience Parts[22] 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

16 Operational Resilience – CRR Firms Part 7, Operational Resilience – Solvency II Firms Part 7.
17 General Organisational Requirements 5.2 (CRR firms), Conditions Governing Business 2.7 (Solvency II firms).
18 Senior Management Functions – 3.8 (CRR firms), Insurance – Senior Management Functions 3.7 (Solvency II firms) s).
19 Available at: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-banking-ss.
20 Available at: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/strengthening-individual-accountability-in-insurance-ss.
21 Operational Resilience – CRR Firms Part 7, Operational Resilience – Solvency II Firms Part 7.
22 Operational Resilience – CRR Firms Part 6, Operational Resilience – Solvency II Firms Part 6.

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.[23] 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.[24] 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,[25] 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 their supporting resources 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; and
- 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 systemically-important firms to take prompt action.

9 Groups

9.1 The PRA expects firms to identify a proportionate number of important group business services and respective impact tolerances at the level of the group. Taking a group level view of operational resilience ensures the risks to the whole group, including those parts that are not subject to individual requirements, are taken into account.

9.2 An important group business service[26] is a service provided by a member of the firm's group to an external end user[27] which, if disrupted could (via their impact on the group as a whole) pose a risk to financial stability in the UK, the UK 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.

23 Operational Resilience – CRR Firms Part 6, Operational Resilience – Solvency II Firms Part 6.
24 Operational Resilience – CRR Firms Part 6, Operational Resilience – Solvency II Firms Part 6.
25 Operational Resilience – CRR Firms Part 6, Operational Resilience – Solvency II Firms Part 6.
26 Definition of important group business services in Operational Resilience – CRR Firms Part and Group Supervision Part.
27 Definition of group external end user in Operational Resilience – CRR Firms Part and Operational Resilience – Solvency II Firms Part.

9.3 Impact tolerances should be set in the same way as they are for an individual firm. Boards and senior management should consider the level of disruption that would represent a threat to the viability of the group and therefore pose a risk to financial stability in 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 Operational Resilience Parts[28] require that firms ensure that the strategies, processes and systems at the level of their group enable the firm to assess whether important group business services are able to remain within their impact tolerances in severe but plausible scenarios. A firm would be expected to work with other members of its group to take action should it be likely that an important group business service could not be delivered within its impact tolerance. Firms are required to include this analysis in their self-assessments.

28 Operational Resilience – CRR Firms Part Rule 8.4, Group Supervision Rule 22.5.

Appendix 4: Draft Statement of Policy: Operational Resilience

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[2] and SSXX/XX 'Operational Resilience: Impact tolerances for important business services' requires and expects firms respectively 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[3] within their impact tolerances.[4] 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.

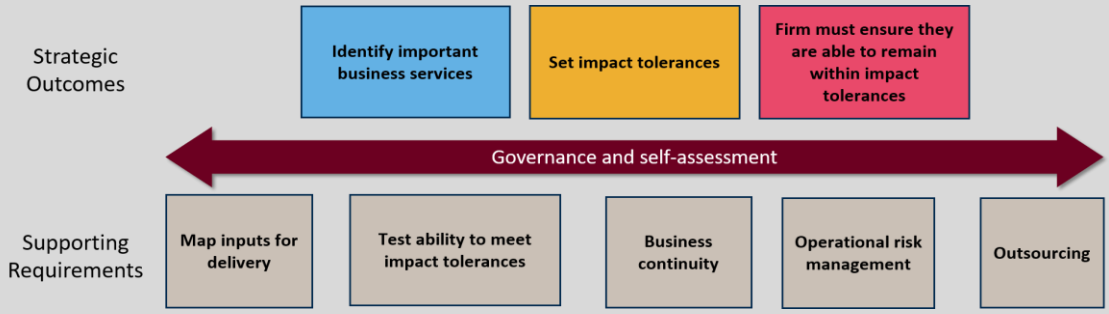
1.6 The SoP clarifies how the PRA's operational resilience policy affects its approach to four key areas of the regulatory framework in particular (the relationship between these policies is depicted in Figure 1 below):

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

1 As explained in PRA DP01/18 '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 Part; Operational Resilience – Solvency II Firms Part and the Operational Resilience rules in the Group Supervision Part.
3 'Important business service' as described in Chapter 2 of SSXX/XX.
4 'Impact tolerance' as described in Chapter 3 of SSXX/XX.

1.7 There is a valuable set of other relevant existing policies and guidelines (eg EBA's guidelines on ICT risks[5] 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.

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

5 The EBA's 'Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process' (ICT SREP) (EBA/GL/2017/05): https://eba.europa.eu/sites/default/documents/files/documents/10180/1841624/ef88884a-2f04-48a1-8208-3b8c85b2f69a/Final%20Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20%28EBA-GL-2017-05%29.pdf.

6 The EBA 'Guidelines on ICT and security risk management' (EBA/GL/2019/04): https://eba.europa.eu/documents/10180/2522896/EBA+BS+2018+431+%28Draft+CP+on+Guidelines+on+ICT+and+security+risk+management%29.pdf.

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 the PRA 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 its 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 Senior Management Function (SMF) 24 role, 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:

- 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.

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

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

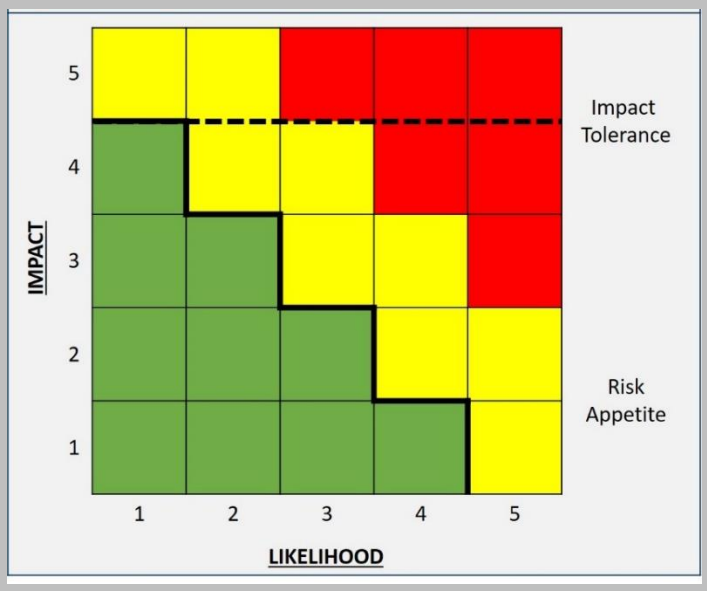


Figure 2 shows the relationship between impact and likelihood for a firm's risk appetite and impact tolerance. Both risk appetite and impact tolerances help ensure a firm's operational resilience.

- 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

8 For banks CRR Firms – Internal Capital Adequacy Assessment 10.1, for insurers Solvency Capital Requirement – General Provisions 3.3.

9 Notifications Part, Rule 2.1.

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,[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
- 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 (SSYY/YY) complements the PRA's operational resilience policy. SSYY/YY reflects the

10 CRR firms, Internal Capital Adequacy Assessment, 10.2.
11 Solvency II Firms, Conditions Governing Business, Rule 2.6.
12 'Internal governance', available at: https://www.bankofengland.co.uk/prudential-regulation/publication/2015/internal-governance-ss.
13 Paragraph 2.1(b), SS 21/15.
14 PRA rule, CRR Firms, Outsourcing; and PRA rule, Solvency II Firms, Conditions Governing Business 7.

increased importance to firms of cloud computing and other new technologies. The PRA's approach is to consider SSYY/YY and the PRA's operational resilience policy in combination.