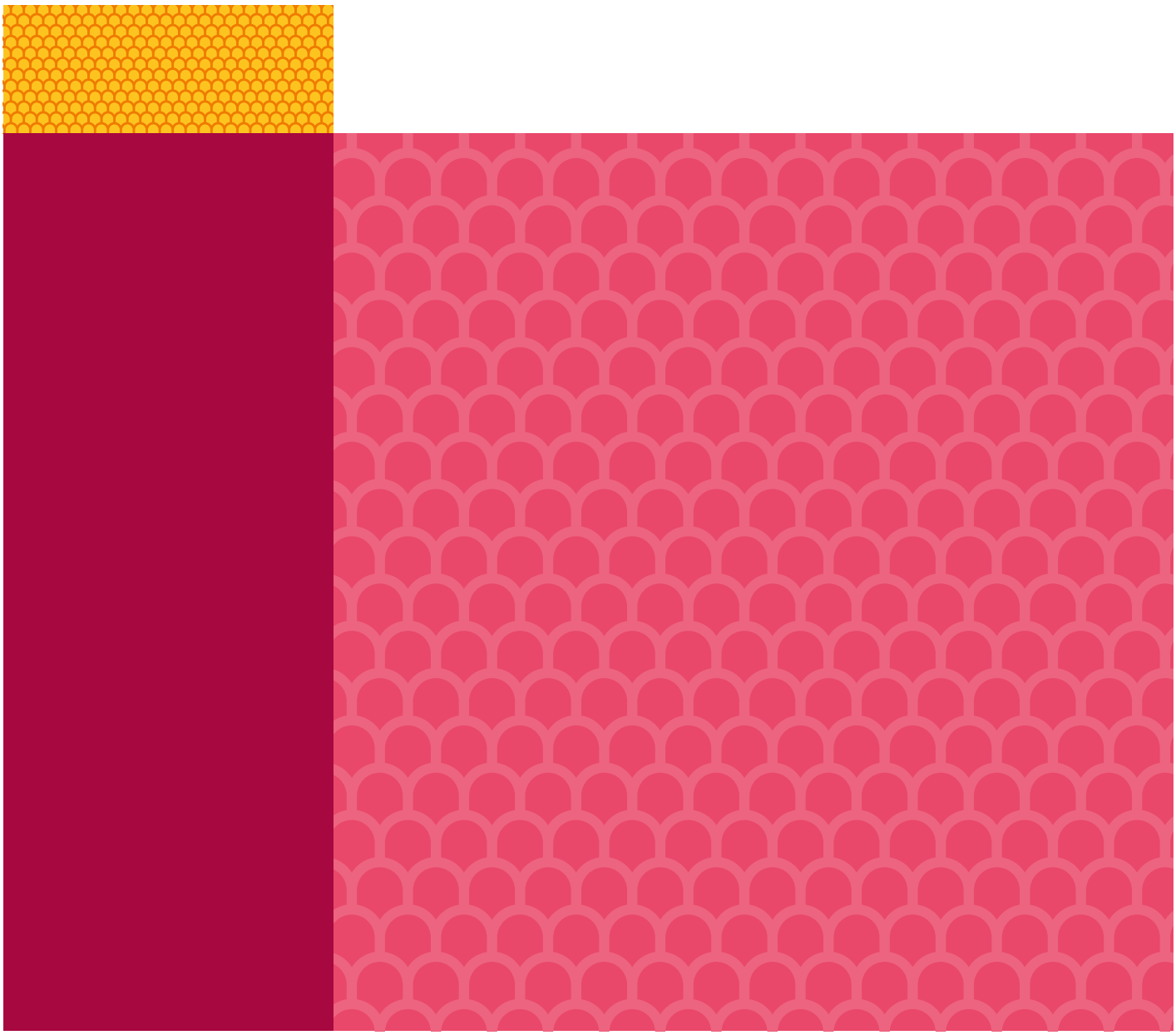
BANK OF ENGLAND

Financial Market Infrastructure

Consultation Paper

Operational Resilience: Recognised Payment System Operators and Specified Service Providers

December 2019



Consultation Paper

Operational Resilience: Recognised Payment System Operators and Specified Service providers

December 2019

The Bank of England (the Bank) invites comments on this Consultation Paper. Comments should reach the Bank by 3 April 2020.

Comments may be sent by email to FMIFeedback@bankofengland.co.uk.

Alternatively, please send comments in writing to:

Operational Resilience (Recognised payments systems and specified service providers)
Financial Market Infrastructure Directorate
Bank of England
20 Moorgate
London EC2R 6DA

Information provided in response to this consultation, including personal information may be published or disclosed in accordance with access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998, the Environmental Information Regulations 2004 and the General Data Protection Regulation 2018) or otherwise as required by law or in discharge of our statutory functions.

If you would like the information that you provide to be treated as confidential, please mark this clearly in your response. Under the FOIA, there is a Statutory Code of Practice with which public authorities must comply and which deals, among other things, with obligations of confidence. In view of this, it would be helpful if you could explain why you regard the information you provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give assurance that confidentiality can be maintained in all circumstances.

In the case of electronic responses, general confidentiality disclaimers that often appear at the bottom of emails will be disregarded unless an explicit request for confidentiality is made in the body of the response.

Copies of this consultation paper are available to download from the Bank's website at www.bankofengland.co.uk. Responses are requested by 3 April 2020.

Contents

1 Overview

1.1 This consultation paper (CP) sets out proposals for the Bank of England's (the Bank's) requirements and expectations for the Operational Resilience Framework for operators of payments systems recognised (RPSOs) under section 184 of the Banking Act 2009 (the Act) and specified service providers (SSPs) under section 206A of the Act. The Bank is proposing to develop an operational resilience part to add to the Code of Practice ('the Code') published in June 2017 under section 189 of the Act.[1] This part of the Code will apply to relevant RPSOs and SSPs. This draft part of the Code is attached in Appendix 1.

1.2 The Bank is also proposing to introduce a set of supervisory expectations to complement the Code. The Bank is consulting on a draft Supervisory Statement (SS) that establishes these expectations. The draft SS in Appendix 2 establishes the expectations and sets out what meeting the expectations being consulted on may look like. These expectations are not in themselves binding, but they will provide RPSOs and SSPs with guidance on how the Bank intends to assess compliance with the Code.

1.3 The Bank proposes, however, that the operational resilience part of the Code of Practice will not apply to a recognised payment system that is operated by a central counterparty (CCP) or central securities depository (CSD). This is because the CCP or CSD will be subject to the Bank's expectations as set out in the Bank's CP 'Operational Resilience: Central Counterparties' and the Bank's CP 'Operational Resilience: Central Securities Depositories'. The Bank accepts that a CCP or CSD meeting those expectations will produce the desired outcome in respect of operational resilience of its embedded payment systems.

1.4 In respect of a RPSO based overseas, we do not consider that these requirements and functions require us to bring such a RPSO within the scope of the code in circumstances where we consider that: the RPSO is subject to a domestic regime for supervision or oversight with the objective of promoting financial stability and which implements the PFMI; and arrangements for international co-operation are in place that enable us to discharge our statutory requirements and supervisory functions in respect of the RPSO. We will assess this for any overseas RPSO on an ongoing basis.

1.5 The Bank intends to set more specific requirements or provide more detailed guidance to RPSOs and SSPs than is contained within the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs).[2] The Bank adopted the PFMIs as a published set of principles in 2012 to which recognised payment systems operators are to have regard, as set out in Section 188 in the Act, and these will continue to apply. Section 188 of the Act also gives power to the Bank to publish principles to which service providers are to have regard. In addition, the Bank requires service providers specified under the Act to have regard to Annex F (Oversight expectations applicable to critical service providers) of the CPMI-IOSCO PMFIs (Annex F). This will continue to apply.

1.6 The proposed new part of the Code will provide transparency on the minimum requirements that must be met by all RPSOs and SSPs to which the Code applies. The new part of the Code will be issued under Section 189 of the Act; this means that it will be binding on RPSOs and SSPs to which it applies. If a RPSO or SSP fails to comply with its requirements, the Bank may take enforcement

---

1 Code of Practice and supervisory statement relating to governance of recognised payment system operators, June 2017: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-market-infrastructure-supervision/code-of-practice-relating-to-governance-of-recognised-payment-system-operators.

2 CPMI-IOSCO Principles of Financial Market Infrastructures

action against a RPSO or SSP. The Bank's enforcement powers are set out in Sections 196-202A of the Act.

1.7 These draft requirements and expectations have been developed following the publication of Discussion Paper (DP) 1/18: 'Building the UK financial sector's operational resilience'.[3] The Bank, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) have developed a joint document which addresses the feedback received to this DP and the outcomes associated with an Operational Resilience Framework. This Consultation Paper should be read in conjunction with this joint document.

1.8 The policy objective is for RPSOs and SSPs to be resilient to operational disruption events. The Bank considers disruption to the transfer of payments or payment systems' safety and efficiency to be a financial stability issue, meaning that improving resilience among RPSOs and SSPs would therefore support the Bank's financial stability objective.[4] The Bank therefore considers that improvements in operational resilience should be facilitated by a Code of Practice and supervisory expectations.

1.9 The Bank considers that operational resilience of payment systems is a key part of the task of protecting and enhancing financial stability. Payments systems should be both efficient and operationally risk-robust in order to play the critical role required of them within the UK economy. This is to ensure that they are both not a cause of financial instability and do not transmit and exacerbate financial instability that originates elsewhere.

1.10 As a result the Bank expects that RPSOs' and SSPs' risk management frameworks should incorporate actions to minimise the likelihood of an operational risk event; and actions to mitigate the impact of, and recover from, an operational disruption event. These risk management frameworks should actively integrate with the development of appropriate impact tolerances for important business services.

Responses and next steps

1.11 This consultation closes on 3 April 2020. The Bank invites feedback on the proposals set out in this consultation. Please address any comments or enquires to FMIFeedback@bankofengland.co.uk.

1.12 The proposed implementation date for the proposals is autumn 2021.

Summary of proposals

1.13 The policy proposals included in this CP are:

(i) the introduction of an operational resilience part to the Code of Practice; and

(ii) the introduction of a Supervisory Statement explaining how the Bank expects RPSOs and SSPs to comply with the Code .

1.14 Consistent with the approach set out in the DP 1/18, the proposals aim to ensure that RPSOs and SSPs deliver improvements to their operational resilience in three main areas:

---

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

4 'Financial stability objective' means the objective set out in section 2A of the Bank of England Act 1998.

(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). This may 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 identifiable participants (identifying important business services);

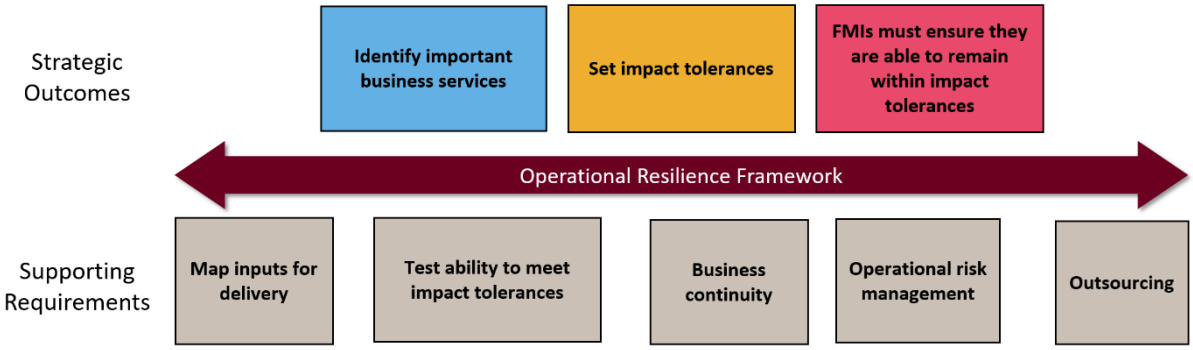
(ii) **setting clear standards for operational resilience**: RPSOs should articulate specific maximum levels of disruption within which they will be able to resume the delivery of important business services following extreme but plausible disruptions (setting impact tolerances); and

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

1.15 The terminology used in this CP, corresponding draft SS and draft Code of Practice is consistent with the terminology used in those draft SSs relating to operational resilience published by the Bank, PRA and FCA. This is to ensure the UK authorities have a consistent supervisory approach to operational resilience across regulated firms.

1.16 Figure 1 below illustrates the key elements in the Bank's proposed approach.

Figure 1: Strategic outcomes and supporting requirements for the Operational Resilience Framework



Structure of the CP

1.17 This CP proceeds as follows:

- Chapter 2 consults on the Bank's proposed requirements and expectations regarding a RPSO's and SSP's Operational Resilience Frameworks.
- Appendix 1 is the Draft Operational Resilience Code of Practice.
- Appendix 2 is the Draft Operational Resilience Supervisory Statement: Recognised Payment Systems and Specified Service Providers.

2 The Bank's proposed requirements and expectations regarding a RPSO's or SSP's Operational Resilience Framework

2.1 This chapter sets out the Bank's requirements and expectations for RPSOs and SSPs to produce an 'Operational Resilience Framework'. The Bank proposes to align the definition of operational resilience with that published in Discussion Paper (DP) 1/18 Building the UK financial sector's operational resilience. DP1/18 stated: Operational resilience is the ability of an FMI and the sector as a whole to prevent, respond to, recover and learn from operational disruptions.

2.2 The Bank proposes that a RPSO and SSP should produce an Operational Resilience Framework and associated material. The Bank suggests that this Framework is an approach which will establish how these RPSOs and SSPs will meet the operational resilience requirements set out in the Draft Operational Resilience Code of Practice. The Bank proposes that the Framework should ensure that a RPSO and a SSP identify and target for investment, where necessary, those aspects of their business most sensitive to an operational disruption. The Bank considers the Operational Resilience Framework as distinct to the business continuity management and disaster recovery plans that a RPSO and SSP are expected to produce in accordance with Principle 17 of the PFMIs and Annex F (3) of the PFMIs, respectively. This is because the Bank views operational resilience as the ability to prevent, as well as respond to and recover from, operational disruption. The Bank proposes that the extent of the work required to develop the Operational Resilience Framework should be comprehensive but proportionate to the outcomes expected by the Bank.

2.3 The Bank suggests that the Framework should focus on a RPSO's or a SSP's ability to:

- minimise the likelihood of an operational disruption event; and
- mitigate the impact of, and recover from, an operational disruption event.

2.4 The Code proposes a RPSO or SSP must have in place sound, effective and comprehensive strategies, process and systems that enable it to adequately identify important business services, set an impact tolerance for each important business service; and identify and address any risks to its ability to remain within its impact tolerance for each important business service. The Bank proposes further guidance in the SS that an Operational Resilience Framework should include as a minimum, policies and procedures:

- for the identification of important business services;
- in relation to the approval of impact tolerances for important business services;
- aligned to its broader operational risk framework, for the identification and mapping of people, processes, technology, facilities and information underlying each important business service;
- for identifying risk of disruption to important business services;
- to ensure that important business services, if disrupted can be recovered within the set impact tolerance; and

- for utilising the results of such testing to make improvements to its procedures and capabilities for minimising the likelihood of, and facilitating recovery from, disruption to important business services.

2.5 The Bank suggests that an Operational Resilience Framework should include communications planning. The Bank proposes that this should take into consideration the potential impact of operational resilience disruption on interdependent FMIs, or the effect of disruption across multiple jurisdictions and products.

Identification of important business services and risks to important business services

2.6 As set out in DP1/18, avoiding disruption to particular systems is a contributing factor to operational resilience, but it is ultimately an important business service that needs to continue to be provided. A focus on important business services will allow appropriate assessment of end-to-end risks to those important business services, thereby increasing operational resilience.

What is a business service?

2.7 The SS proposes to clarify that a business service is a service that a RPSO or SSP provides, delivering a specific outcome or utility to an identifiable end-user. 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 operational resilience decision making, thereby improving operational resilience.

2.8 The Bank suggests that a RPSO and SSP should consider the chain of activities which make up the business service, from taking on an obligation, to delivery of the service, and determine which parts of the chain are essential 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 essential 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. The Bank considers that the most essential 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.

2.9 The Bank 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 Bank's perspective when it affected the delivery of outward-facing business services which have direct consequences for financial stability. Internal services, if necessary for the delivery of important business services, should be included in the mapping work a RPSO and SSP should be performing.

What makes a business service important?

2.10 The draft Code proposes how the Bank will define important business services in respect of a RPSO and SSP. The Bank intends to consider that a business service in respect of an RPSO is an 'important business service' if a prolonged disruption of that business service could significantly threaten the transfer of payments or safety and efficiency of the payment system, thereby impacting financial stability.

2.11 In respect of an SSP, the Bank proposes it will consider a business service to be an 'important business service' if a prolonged disruption of that business service could significantly threaten the transfer of payments or the safety and efficiency of the payment system or systems to which the SSP provides services, thereby impacting financial stability. The introduction of important business services will enable the Bank to prioritise its supervision of RPSOs and SSPs so as to foster financial stability.

2.12 RPSOs and SSPs important business services may differ depending on their specific business models. The Bank proposes that a RPSO and SSP will be expected to identify important business services by considering a variety of factors. Examples of factors that are relevant to the identification of a business service might be:

- the relevant market share of a RPSO and SSP;
- the volume and value of transactions;
- the number of end-users a RPSO serves;
- the nature of the payment; or
- the substitutability of the business service.

2.13 The Bank suggests that this identification process should take into account each type of payment that a RPSO provides but it must also consider operational activities that support or comprise elements of market or product business services, which could also be deemed important business services. Such operational activities could include:

- tokenisation;
- settlement instructions;
- debit payments;
- credit payments;
- interbank payments; or
- cash withdrawals.

2.14 The Code proposes that a RPSO and SSP must be capable of identifying all types of important business services. This is in order to understand both the implications of disruption of a particular business process to an end-user as well as the interrelationship and interdependency between important business services in the way they support an end-user.

2.15 The Bank proposes that each RSPO and SSP should use its own risk assessment based upon its own circumstances, products, and operational structure to understand which operational risks are relevant, and where operational resilience issues exist.

2.16 The Bank proposes to include a non-exhaustive set of examples of the types of risks that the Bank might expect to be considered by a RSPO or SSP, for instance:

- **Data breach:** end-user or other business data compromised, for example through a cyber

attack.

- **Internal fraud:** transactions intentionally mis-reported.
- **External fraud:** theft/robbery.
- **Employment Practices**: compensation, benefit, termination issues, organised labour activity.
- **Clients, Products & Business Practices**: legal breaches, regulatory breaches, breach of privacy, misuse of confidential information.
- **Damage to physical assets**: natural disaster losses, human losses.
- **Business disruption and system failures**: hardware or software failure, telecommunications or utilities outages.
- **Execution delivery and process management**: miscommunication, system mis-operation or delivery that result in failure or lead to unexpected outcomes.

Setting the impact tolerance for important business services

2.17 The draft Code proposes how the Bank will define impact tolerance. The draft SS suggests further guidance for this definition. The Bank proposes that an impact tolerance should be defined as the maximum tolerable level of disruption for an important business service, whereby further disruption could significantly threaten the transfer of payments or the safety and efficiency of the payment system.

2.18 Impact tolerances provide a clear standard which the Bank would expect a RPSO and SSP to remain within, and which boards and senior management could use to drive improvements to their operational resilience.

2.19 The Bank suggests that impact tolerances should be set on the assumption that disruptions will occur. The draft SS sets out some proposed metrics that a RPSO and SSP could consider when setting a tolerance.

2.20 The impact tolerances that the Bank 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. A RPSO or SSP that is able to remain within its impact tolerances increases its ability to withstand extreme but plausible disruptions, whereas risk appetites are likely to be exceeded in these disruptions.

2.21 The Bank proposes that the impact tolerance must be set by a RPSO. RPSOs must consider a range of possible measures by which to judge the appropriate impact tolerance for a given important business service. These factors could include for example: the length of time of an outage, the number of end-users impacted, the nature of the payment, or the volume and values of payments disrupted.

2.22 The Bank suggests that a SSP must set an impact tolerance for each of its important business services in taking into account its obligations to a RPSO. The Bank expects that a SSP's obligations to a RPSO will be defined in service level agreements between the two parties.

2.23 The Code proposes that a RSPO must set an impact tolerance for each of its important business services. The SS suggests that this should be done in order to set a measure for each important business service in respect of which procedures can be developed and testing carried out. The Bank proposes that a RPSO should ensure that each important business service remains within the impact tolerance which has been set for it. A RSPO may be unable to meet the impact tolerance in all circumstances; in this instance the Bank proposes that a RPSO should take steps to return the important business service to within its impact tolerance where there has been a breach of that important business service's impact tolerance.

2.24 The Bank proposes that a RPSO's impact tolerance for an important business service is distinct to the two hour maximum recovery time for a service established in the PFMIs relating to business continuity planning. The Bank suggests that impact tolerances should include the maximum tolerable duration of disruption, taking into account the criticality of the important business service. However, on its own a metric based on time may not be enough. The Bank proposes that a RPSO or SSP should also set out the metrics that it will consider and monitor when setting a tolerance, which should include at least one qualitative or quantitative metric for disruption to the important business service. The Bank proposes that these metrics could be based on financial loss to an end-user impacted as a result of disruption. The Bank does not propose any specific metrics for this purpose. However RPSOs and SSPs might consider the length of an outage, the number of end-users impacted, the nature of the payment, or the volume and values of payments disrupted.

2.25 The Bank suggests that in setting an impact tolerance for important business services, a RPSO should leverage existing risk management frameworks to determine the acceptable level of disruption it is able to tolerate. RPSOs and SSPs may already be setting their own risk appetites based on their existing risk management framework.

2.26 The Bank proposes that a RPSO or SSP should take reasonable actions to evidence that it can operate within the impact tolerance for each important business service in the event of disruption to its operations.

Mapping and identification of dependencies

2.27 A RPSO's and SSP's mapping could highlight vulnerabilities in how important business services are being delivered, such as limited substitutability of resources, single points of failure, and concentration risk. The proposed Operational Resilience Framework would require a RPSO or SSP to take action to remediate these vulnerabilities so that important business services could be delivered within impact tolerances.

2.28 The Bank intends that a RPSO and SSP should map dependencies of important business services. This may involve an element of co-ordination between a RPSO and its SSP. The Code proposes that mapping of dependencies must entail identifying and documenting the necessary people, processes, technology, facilities and information required to deliver each of a RPSO's or SSP's important business services. The Bank proposes that this mapping should facilitate the gathering of evidence to diagnose and remedy vulnerabilities in a RPSO's or SSP's important business services. The Bank considers this a necessary step to ensure a thorough understanding of the ways in which operational disruption could occur.

2.29 This will help a RPSO or SSP plan to reduce the probability of an operational resilience risk crystallising. This is not be a new requirement for RPSOs. Under Part 1 of the existing Code (provision 2.3(1)) the board of an RPSO must 'ensure that it has sufficient understanding of the risks to the end-to-end flow of payments across the payment system'.

2.30 The Bank suggests that the mapping of the dependencies within important business services should allow a RPSO or SSP to comprehensively understand how interconnected or concentrated its important business services and products are. The Bank proposes this is necessary in order to design, understand and evaluate the full implications of scenarios (as described in 2.34-2.41 below). This will help a RPSO or SSP to prioritise its mitigation and recovery actions by identifying specific vulnerabilities.

2.31 The Bank considers the following dependencies could be mapped by RPSOs and SSPs: authorisations, settlements; redirection tables; and sort code databases. This list is non-exhaustive.

2.32 The Bank proposes that the mapping of dependencies process should include any outsourced providers, including critical service providers that a RPSO or SSP considers to be involved in the supply of important business services. RPSOs or SSPs should review the risks to its important business services from other parties as a result of inter-dependencies, and develop appropriate risk management tools.

Testing, Monitoring and Reporting

2.33 The Bank proposes that a RSPO or SSP, having identified its important business services, should undertake an assessment of the operational risks that are relevant to these important business services. The Bank suggests that the list of relevant operational risks should be used in the design of disruption scenarios for the purposes of testing, but should also have wider usage in the RSPO or SSP for the purposes of managing operational resilience.

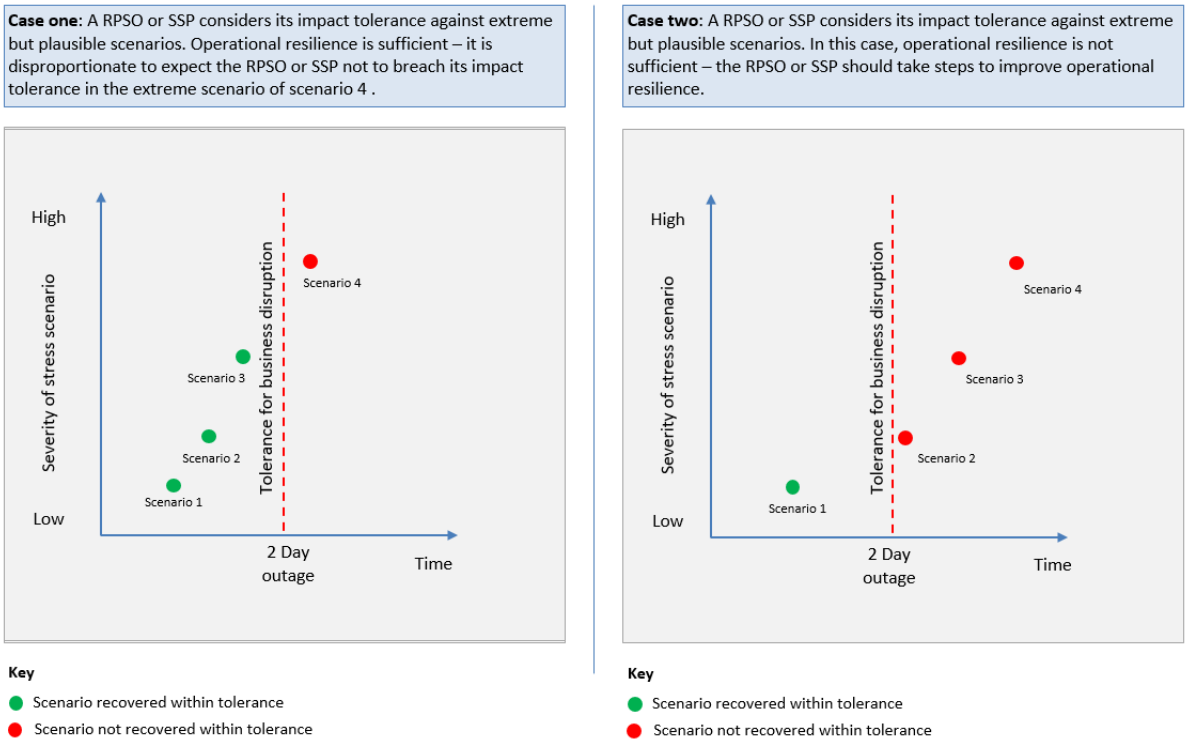
2.34 The Bank suggests that a RPSO and SSP must test its important business services against a range of extreme but plausible disruption scenarios to establish whether these important business services can remain within their impact tolerances. Testing, monitoring and reporting may involve RPSOs and SSPs cooperating to execute this requirement. The Bank proposes that once a RPSO or SSP has established what its important business services are, and an impact tolerance for each important business service, it can more precisely define the types of scenarios which will cause disruption to a specific important business service and, therefore, the capacity to recover from the disruption event.

2.35 Section 5 of the draft Code sets out the Bank's requirement that a RPSO and SSP should develop a testing plan that details how it would assure itself that it is able to remain within impact tolerances for its important business services. The entire chain of activities that have been identified as the important business service should be considered when developing testing plans.

2.36 The severity of scenarios used by a RPSO or SSP for 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 a RPSO or SSP could undertake is likely to be useful in informing it of how its scenarios could be made more difficult.

2.37 RPSOs and SSPs should test a range of scenarios, including those in which they anticipate exceeding their impact tolerance. This is illustrated in figure 2 below. The Bank does not currently propose to set scenarios for RPSOs or SSPs to use when testing their ability to remain within the impact tolerance for their important business services.

Figure 2: Some scenarios may see impact tolerances exceeded



2.38 The Bank proposes that a RPSO and SSP should:

(i) conduct scenario analyses of its ability to meet its impact tolerance for each of its important business services in the event of extreme but plausible disruption to its operations;

(ii) identify an appropriate range of adverse scenarios of varying nature, severity and duration, relevant to its business and risk profile, and

(iii) consider the risks to delivery of its important business services in those scenarios.

2.39 Where the impact tolerance cannot be met for any important business service, or where there is uncertainty as to whether it can be met, the Bank suggests that a RPSO or SSP should be able to provide an explanation as to why this has happened and what remedial actions will be undertaken to ensure the impact tolerance can be met in future. In such situations, the Bank proposes that a RPSO or SSP should explain what mitigating actions will be taken to ensure the important business service can be brought within a RPSO's and SSP's impact tolerance should disruption occur. In addition, the Bank proposes that the relevant important business services should be prioritised when a RPSO or SSP makes choices about remediation or improvements in its systems, processes and technologies.

2.40 The Bank suggests that in setting an impact tolerance for important business services, a RPSO and SSP will be expected to incorporate these impact tolerances into the monitoring and reporting procedures of key qualitative and quantitative measures and processes which support delivery of these services, so as to guide management in taking actions to control risks to their ability to stay within the defined impact tolerance.

Documentation

2.41 The Code proposes that a RPSO or SSP should make a written record of the assessments as a result of the Operational Resilience Framework procedures and to share this with the Bank only if requested to do so.

2.42 In particular, the Code proposes that a RPSO or SSP must make a written record of the determinations made in respect of the:

- identification of its important business services;
- setting of its impact tolerances for those important business services;
- mapping and identification of interdependencies in relation to those important business services; and
- testing, monitoring and reporting of its important business services ability to stay within their impact tolerance.

Governance Arrangements

2.43 The Bank considers that a credible Operational Resilience Framework will not only take into account testing and improvement of the Framework, but will also be subject to a RPSO's or SSP's governance process.

2.44 The Bank proposes that a RPSO's or SSP's board must assure itself that the Operational Resilience Framework is fit for purpose through its usual processes. The Code proposes that a RPSO's and SSP's board must ensure that it regularly reviews and approves the written record (Operational Resilience Framework), and key elements identified by the relevant subcommittee, at intervals it deems appropriate. The draft SS recommends that such a review should take place following events where an impact tolerance has been breached.

2.45 The SS provides further guidance on the above requirement. The Bank proposes that the body designated by the board of directors with responsibility for risk management should:

- approve a RPSO's or SSP's identified list of important business services;
- approve a RPSO's or SSP's impact tolerances for the important business services;
- be satisfied that a RPSO's or SSP's important business services are mapped effectively;
- review the results of impact tolerance testing; and
- be satisfied that appropriate risk mitigation steps have been undertaken.

2.46 The Bank proposes that a RPSO's or SSP's Operation Resilience Framework should be subject to assessment by the body designated by the board of directors with responsibility for audit periodically, in line with its audit approach but taking into consideration material changes to the Framework.

2.47 The Bank proposes that this internal audit assessment should cover: i) the extent to which the Operational Resilience Framework satisfies the Bank's expectations and requirements as laid out in this SS and the Code; and ii) the effectiveness of a RPSO's or SSP's operational resilience processes.

2.48 The Bank proposes that this assessment should be reviewed by a RPSO's or SSP's body designated by the board of directors with responsibility for audit.

Appendices

1 Operational Resilience part of the Code of Practice

CODE OF PRACTICE ABOUT THE OPERATION OF RECOGNISED PAYMENT SYSTEMS

Powers exercised

A. This amended code of practice is published under section 189 of the Banking Act 2009.

B. A failure to comply with this code will constitute a "compliance failure" under section196 of the Banking Act 2009, which can result in the imposition of a sanction under section198 to 200 of the Banking Act 2009 (financial penalty, management disqualification, and in certain specified circumstances, a closure order). It can also involve publication of the details of the compliance failure and any sanction imposed (section197 Banking Act 2009).

Commencement

C. These amendments to the code of practice come into force on [DATE].

Citation

D. The part of the code of practice set out in Annex B may be cited as the Bank of England Recognised Payment Systems Code of Practice: Operational Resilience.

[DATE]

Annex A

In this annex new text is underlined and deleted text is struck through

PART 1: GOVERNANCE

1 APPLICATION AND DEFINITIONS

1.1 This part of the code of practice applies to a *RPSO* that is not operated by a recognised clearing house or a central securities depository unless 1.2 applies.

1.2 The Bank of England may notify a *RPSO* that this part of the code shall not apply to it where:

…

1.3 The following definitions shall apply to the entire code and are not limited to this part:

…

Annex B

In this annex, all text is new.

PART 2: OPERATIONAL RESILIENCE

1 APPLICATION AND DEFINITIONS

1 .1 This part of the code of practice applies to a *RPSO* that is not operated by a recognised clearing house or a central securities depository, and also to a *specified service provider (SSP)*.

1.2 The Bank of England may notify a *RPSO* or *SSP* that this part of the code shall not apply to it where:

(1) the *RPSO* or *SSP* is not incorporated in the UK; and

(2) the Bank of England considers that:

(a) the *RPSO* or *SSP* is subject to a domestic supervisory or oversight regime that has the objective of protecting and enhancing financial stability and which implements the Committee for Payment and Market Infrastructure and the International Organization of Securities Commissions 'Principles for financial market infrastructures'; and

(b) arrangements in place for international cooperation enable it to discharge its statutory requirements and supervisory functions in respect of the *RPSO* or *SSP*.

1.3 In this part, the following definitions shall apply:

important business service

means;

- in respect of a *RPSO*, a service provided by a *RPSO* to an end user which, if disrupted, could threaten the transfer of payments or safety and efficiency of a payment system.
- in respect of a *SSP*, a service provided by a *SSP* to a *RPSO* which, if disrupted, could threaten the transfer of payments or safety and efficiency of the *RPSO*.

impact tolerance

means the maximum tolerable level of disruption for an *important business service.*

specified service provider or *SSP*

means a service provider to a payment system specified in a Treasury order made under section 206A of the Banking Act 2009.

2 OPERATIONAL RESILIENCE REQUIREMENTS

2.1 A *RPSO* or SSP must identify its *important business services*.

2.2 A *RPSO* or *SSP* must, for each of its *important business services*, set an *impact tolerance*.

2.2.1 The *impact tolerance* set for each *important business service* must be set at the maximum level of disruption to the *important business service* which can be tolerated prior to such disruption threatening the safety and efficiency of the payment system.

2.2.2 A RPSO must set an *impact tolerance* taking into account of the recovery times specified in the CPSS/IOSCO Principles for Financial Market Infrastructures, the nature of the *important business service* and any contractual arrangements made in relation to it.

2.2.3 A SSP must set an *impact tolerance* for each of its *important business services* taking into account its obligations to any relevant *RPSO*.

2.3 A *RPSO* or *SSP* must take all reasonable actions to ensure it remains within its *impact tolerance* for each *important business service* in the event of an extreme but plausible disruption to its operations.

2.4 A *RPSO* or *SSP* must comply with the rule in 2.3 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 *RPSO* or *SSP* must have in place sound, effective and comprehensive strategies, processes and systems that enable it adequately to:

3.1.1. identify its *important business services;*

3.1.2. set an *impact tolerance* for each *important business service;* and

3.1.3. identify and address any risks to its ability to comply with the obligation under the rule in 2.3.

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

4 MAPPING

4.1 As part of its obligation under the rule in 3.1, a *RPSO* or *SSP* 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 the rule in 3.1, a *RPSO* or *SSP* must carry out regular scenario testing of its ability to meet its *impact tolerance* for each of its *important business services* in the event of an extreme but plausible disruption of its operations.

5.2 In carrying out the scenario testing required by the rule in 5.1, a *RPSO* or *SSP* 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 *RPSO* or *SSP's important business services* in those circumstances.

5.3 The scenario testing required by the rule in 5.1 must be proportionate to the nature, scale and complexity of the *RPSO* or *SSP's* activities, and informed by its previous experience.

6 WRITTEN RECORDS

6.1 A *RPSO* or *SSP* must prepare and regularly update a written record of the assessments made as a result of its compliance with the requirements of this Part.

6.2 The content and level of detail of a *RPSO* or *SSP's* written record produced in compliance with 6.1 must be proportionate to the nature, scale and complexity of the *RPSO* or *SSP's* activities but should include as a minimum:

i) the identification of *important business services*;

ii) the setting of its *impact tolerance* for those *important business services*;

iii) the mapping and identification of interdependencies in relation to those *important business services*; and

iv) the testing, monitoring and reporting of its *important business services'* ability to stay within their *impact tolerance*.

6.3 A *RPSO* or *SSP* must maintain, and be able to provide to the Bank on request, a current version of its written record, produced in compliance with 6.1, together with all versions produced during the preceding three years.

7 GOVERNANCE

7.1 A *RPSO* or *SSP* must ensure that its *board* approves the *important business services* identified by the *RPSO* or *SSP* in compliance with the rule in 2.1.

7.2 A *RPSO* or *SSP* must ensure that its *board* approves the *impact tolerances* set by the *RPSO or SSP* in compliance with the rule in 2.2.

7.3 A *RPSO* or *SSP* must ensure that its *board* approves and regularly reviews the written record required by the rule in 6.1.

2 Draft Operational Resilience Supervisory Statement: Recognised Payment System Operators and Specified Service Providers

1 Introduction

1.1 This Supervisory Statement (SS) on operational resilience is relevant to the operators of payments systems recognised (RPSOs) under section 184 of the Banking Act 2009 (the Act) and specified service providers under section 206A of the Act (SSPs). The Operational Resilience part of the Code of Practice (the Code) will not apply to a recognised payment system that is operated by a central counterparty (CCP) or central securities depository (CSD). This is because the CCP or CSD will be subject to the Bank's expectations as set out in the Bank's SS 'Operational Resilience: Central Counterparties' and the Bank's SS 'Operational Resilience: Central Securities Depositories'. The Bank accepts that a CCP or CSD meeting those expectations will produce the desired outcome in respect of operational resilience of its embedded payment systems.

1.2 In respect of a RPSO or SSP that is incorporated outside of the UK, the Bank will determine on a case-by-case basis whether these RPSOs or SSPs will be subject to the Bank's requirements and expectations, taking into account factors such as systemic importance in the UK and the extent to which the local (home-country) regulatory and supervisory framework delivers an equivalent outcome in terms of operational resilience.

1.3 This SS explains the Bank's supervisory approach to operational resilience, which is relevant to many areas of a RPSO's and SSP's operations. It provides guidance as to how the Bank expects RPSOs and SSPs to meet their regulatory obligations under the Code. The Bank considers disruption to payments operations to be a financial stability issue, meaning that a lack of resilience amongst RPSOs and SSPs therefore represent a threat to the Bank's financial stability objective. The Bank therefore considers that improvements in operational resilience should be facilitated by the Code of Practice.

1.4 The Code provides transparency on the minimum requirements that must be met by all RPSOs and SSPs to which the Code applies. The Code is issued under section 189 of the Act; this means that it is binding on RPSOs and SSPs to which it applies. If a RPSO or SSP fails to comply with its requirements, the Bank may take enforcement action against a RPSO or SSP. The Bank's enforcement powers are set out in the sections 196-202A of the Act.

1.5 The policy objective of this SS is for RPSOs and SSPs to be operationally resilient to disruption events. This SS contains a set of actions that the Bank expects RPSOs and SSPs to undertake in order to achieve a level of operational resilience which, in the Bank's view, is sufficient. Taken together, the aim of this framework is to ensure that RPSO and SSP's risk management frameworks cover both minimising the likelihood of an operational disruption occurring and mitigating and recovering from an operational disruption once such disruption crystallises.

1.6 The Bank considers operational resilience of payment systems to be a key part of the task of protecting and enhancing financial stability. Payments systems should be both efficient and operationally risk-robust in order to play the critical role required of them within the UK economy. This is to ensure that they are both not a cause of financial instability and do not transmit and exacerbate financial instability that originates elsewhere.

1.7 The Bank will supervise the operational resilience policy in line with its existing supervisory approach for FMIs. The Bank's supervision of FMIs is judgement-based and forward-looking. It is carried out using a supervisory risk assessment framework to identify risks that FMIs may be exposed to and the mitigants that FMIs have in place to guard against those risks.

1.8 RPSOs must continue to have regard for the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs), as set out in s188 in the Act. SSPs must continue to have regard for Annex F (Oversight expectations applicable to critical service providers) of the CPMI-IOSCO PFMIs.

1.9 This SS should be read in conjunction with the Code.

Contents

1.10 Chapter 2 establishes the definitions and concepts used in the SS

1.11 Chapter 3 sets out the Bank's expectations regarding a RPSO's and SSP's Operational Resilience Framework.

1.12 Chapter 3 explains the Bank's requirements and expectations regarding operational resilience.

2 Definitions and Concepts

Use of terminology

2.1 The terminology used in this SS is consistent with the terminology used in those SSs relating to operational resilience published by the Bank, PRA and FCA. This is to ensure the UK authorities have a consistent supervisory approach to operational resilience across regulated firms.

Operational Resilience

2.2 Operational resilience is the ability of FMIs and the sector as a whole to prevent, respond to, recover and learn from operational disruptions.

Important business services

2.3 The Code defines an important business services in respect of a RPSO and SSP. A business service is a service that a RPSO or SSP provides, delivering a specific outcome or utility to an identifiable end-user. The Bank considers that a business service in respect of an RPSO is an 'important business service' if a prolonged disruption of that business service could significantly threaten the transfer of payments or the safety and efficiency of the payment system, thereby impacting financial stability. In respect of an SSP, the Bank considers a business service to be an 'important business service' if a prolonged disruption of that business service could significantly threaten the transfer of payments or safety and efficiency of a RPSO, thereby impacting financial stability.

2.4 This identification process should take into account each type of payment that a RPSO provides but it must also consider operational activities that support or comprise elements of market or product business services, which could also be deemed important business services. Such operational activities could include:

- tokenisation;
- settlement instructions;
- debit payments;
- credit payments;
- interbank payments; or
- cash withdrawals.

2.5

2.6 RPSOs and SSPs are expected to identify important business services by considering a variety of factors. Examples of factors that are relevant to the identification of whether a business service is important might be:

- the market share of a RPSO and SSP;
- the volume and value of transactions;
- the number of end-users a RPSO serves;
- the nature of the payment; or
- the substitutability of the business service.

Impact tolerance

2.7 The Code defines an impact tolerance. Impact tolerance is the maximum tolerable level of disruption for an important business service, whereby further disruption could significantly threaten the transfer of payments or the safety and efficiency of the payment system. An impact tolerance must be set by a RPSO. RPSOs should consider a range of possible measures by which to judge the appropriate impact tolerance for a given important business service. These factors could include for example: the length of time of an outage, the number of end-users impacted, or the volume and value of payments disrupted.

2.8 The Code requires a SSP to set an impact tolerance for each of their important business services in accordance with their obligations to a RPSO. The Bank expects that the SSP's obligations to a RPSO will be defined in service level agreements between the two parties.

2.9 A RPSO's impact tolerance for an important business service is distinct to the two hour maximum recovery time for a service established in the PFMIs (3.17.14), which should continue to apply where applicable.[5] An impact tolerance should not only be considered as a time metric. Other factors could include the number of end-users impacted, or the volume and value of payments disrupted. The impact tolerance is expected to drive various behaviours within a RPSO and SSP, such as investment behaviour, change management processes and internal governance.

---

5 Recovery time objective (RTO) or recovery point objective is the maximum desired length of time allowed between an unexpected failure or disaster and the resumption of normal operations and service levels.

3 The Bank's requirements and expectations regarding a RPSO's and SSP's Operational Resilience Framework

3.1 A RPSO and SSP should produce an Operational Resilience Framework and associated material. This Framework is an approach which will establish how a RPSO and SSP will meet the operational resilience objectives set out in this SS and the Code. The Framework should ensure that a RPSO and SSP identifies and targets for investment where necessary those aspects of its business most sensitive to an operational disruption. The extent of the work required to develop the Operational Resilience Framework should be comprehensive but proportionate to the outcomes expected by the Bank.

3.2 The Bank considers the Operational Resilience Framework as distinct to the business continuity management and disaster recovery plans that a RPSO and SSP are expected to produce in accordance with Principle 17 of the PFMIs and Annex F (3) of the PFMIs, respectively. This is because the Bank views operational resilience as the ability to prevent, as well as respond to and recover from, operational disruption.

3.3 The Framework should focus on a RPSO's and SSP's ability to:

- minimise the likelihood of an operational disruption event; and
- mitigate the impact of, and recover from, an operational disruption event.

3.4 The Code requires a RPSO or SSP to have in place sound, effective and comprehensive strategies, process and systems that enable it to adequately identify important business services, set an impact tolerance for each important business service; and identify and address any risks to its ability to remain within its impact tolerance for each important business service. An Operational Resilience Framework, containing details of strategies, processes and systems, should include as a minimum, policies and procedures:

- for the identification of important business services;
- in relation to the approval of impact tolerances for important business services;
- aligned to its broader operational risk framework, for the identification and mapping of people, processes, technology, facilities and information underlying each important business service;
- for identifying risk of disruption to important business services;
- to ensure that important business services, if disrupted can be recovered within the set impact tolerances; and
- for utilising the results of such testing to make improvements to its procedures and capabilities for minimising the likelihood of, and facilitating recovery from, disruption to important business services.

3.5 The Bank further expects an Operational Resilience Framework to include communications planning. This should take into consideration the potential impact of operational resilience disruption on interdependent FMIs, or the effect of disruption across multiple jurisdictions and products.

Identification of important business services and risks to important business services

3.6 The Code requires that a RPSO and SSP must be capable of identifying all types of important business services. The Bank considers this necessary in order to understand both the implications of disruption of a particular business process to an end-user, as well as the interrelationship and interdependency between important business services in the way they support an end-user.

3.7 The Bank expects a RPSO and SSP, having identified its important business services, to undertake an assessment of the operational risks that are relevant to these important business services. The list of relevant operational risks is expected to be used in the design of disruption scenarios for the purposes of testing, but should also have wider usage in a RPSO or SSP for the purposes of managing operational resilience. Each RPSO or SSP is expected to use its own risk assessment based upon its own circumstances, products, and operational structure to understand which operational risks are relevant, and where operational resilience issues exist.

3.8 A non-exhaustive set of examples of the types of risks that the Bank might expect to be considered by a RPSO or SSP are listed below.

- **Data breach:** end-user or other business data compromised, for example through a cyber attack.
- **Internal fraud:** transactions intentionally mis-reported.
- **External fraud:** Theft/robbery.
- **Employment Practices:** Compensation, benefit, termination issues, organised labour activity.
- **Clients, Products & Business Practices**: Fiduciary breaches, regulatory breaches, breach of privacy, account churning, misuse of confidential information.
- **Damage to physical assets:** Natural disaster losses, human losses.
- **Business disruption and system failures:** hardware or software failure, telecommunications or utilities outages.
- **Execution delivery and process management:** Miscommunication, system mis-operation or delivery that result in failure or lead to unexpected outcomes.

Setting the impact tolerance for important business services

3.9 The Code requires that a RSPO must set an impact tolerance for each of its important business services. A RSPO should define an impact tolerance in order to set a measure for each important business service in respect of which procedures can be developed and testing carried out. The Bank expects a RPSO to ensure that each important business service remains within the impact tolerance which the RSPO has set for it. A RPSO may be unable to meet the impact tolerance in all circumstance; in this instance the Bank expects a RSPO to take steps to return the important business service to within its impact tolerance where there has been a breach of that important business service's impact tolerance.

3.10 A SSP must set an impact tolerance for each of its important business services taking into account its obligations to a RPSO. The Bank expects that the SSP's obligations to a RPSO will be defined in service level agreements between the two parties.

3.11 The Bank considers that a RPSO's impact tolerance for an important business service is distinct to the two hour maximum recovery time for a service established in the PFMIs relating to business continuity planning. The Bank considers that impact tolerances must include the maximum tolerable duration of disruption, taking into account the criticality of the important business service. However, on its own a metric based on time may not be enough. The Bank expects that a RPSO or SSP should also set out the metrics that it will consider and monitor when setting a tolerance, which should include at least one qualitative or quantitative metric for disruption to the important business service. These metrics could be based on financial loss to end-users impacted as a result of market disruption. The Bank does not propose any specific metrics for this purpose, however RPSOs and SSPs might consider the length of time of an outage, the number of end-users impacted, the nature of the payment, or the volume and values of payments disrupted.

3.12 The Bank expects that in setting an impact tolerance for important business services, a RPSO or SSP should leverage existing risk management frameworks to determine the acceptable level of disruption it is able to tolerate. RPSOs and SSPs may already be setting their own risk appetites based on their existing risk management framework.

3.13 A RPSO or SSP must take reasonable actions to evidence that it can operate within the impact tolerance for each important business service in the event of disruption to its operations.

Mapping and identification of dependencies

3.14 A RSPO and SSP should map dependencies. This may involve an element of co-ordination between a RPSO and its SSP. The Code requires that mapping of dependencies must entail identifying and documenting the necessary people, processes, technology, facilities and information required to deliver each of a RPSO or SSP's important business services. This mapping should facilitate the gathering of evidence to diagnose and remedy vulnerabilities in a RPSO's or SSP's important business services. The Bank considers this a necessary step to ensure a thorough understanding of the ways in which operational disruption could occur.

3.15 This will help a RPSO or SSP plan to reduce the probability of an operational resilience risk crystallising. This will help a RPSO or SSP plan to reduce the probability of an operational resilience risk crystallising. This is not be a new requirement for RPSOs. Under Part 1 of the Code (provision 2.3(1)) the board of an RPSO must 'ensure that it has sufficient understanding of the risks to the end-to-end flow of payments across the payment system'.

3.16 Mapping of the dependencies within important business services should allow a RPSO or SSP to comprehensively understand how interconnected or concentrated its important business services and products are. This is necessary in order to design, understand and evaluate the full implications of scenarios. This will help a RPSO or SSP to prioritise its mitigation and recovery actions by identifying specific vulnerabilities.

3.17 The Bank considers the following dependencies could be mapped by RPSOs and SSPs: authorisations, settlements; redirection tables; and sort code databases. This list is non-exhaustive.

3.18 The mapping of dependencies process should include any outsourced providers, including critical service providers that a RPSO or SSP considers to be involved in the supply of important business services. RPSO or SSP should review the risks to its important business services from other parties as a result of inter-dependencies, and develop appropriate risk management tools.

Testing, Monitoring and Reporting

3.19 The Code requires a RPSO or SSP to test its important business services against a range of extreme but plausible disruption scenarios to establish whether these important business services can remain within impact tolerances. Testing, monitoring and reporting may involve RPSOs and SSPs cooperating to execute this requirement. Once a RPSO or SSP has established what its important business services are, and an impact tolerance for each important business service, a RPSO or SSP can more precisely define the types of scenarios which will cause disruption to a specific important business service and, therefore, the capacity to recover from the disruption event.

3.20 A RPSO or SSP should:

(i) conduct scenario analyses of its ability to meet its impact tolerance for each of its important business services in the event of extreme but plausible disruption to its operations;

(ii) identify an appropriate range of adverse scenarios of varying nature, severity and duration, relevant to its business and risk profile, and

(iii) consider the risks to delivery of its important business services in those scenarios.

3.21 Within any operational risk scenario identified, where the impact tolerance cannot be met for any important business service, or where there is uncertainty as to whether it can be met, the Bank expects a RPSO or SSP to be able to provide an explanation as to why this has happened and what remedial actions a RPSO or SSP will undertake to ensure the impact tolerance can be met in future. In such situations, the Bank expects that a RPSO or SSP should explain how such risks will be managed as part of their risk management framework and what mitigating actions will be taken or how business continuity planning and disaster recovery will be enhanced to ensure the important business service can be brought within the firms impact tolerance should disruption occur. In addition, the Bank expects the relevant important business service to be prioritised when a RPSO or SSP makes choices about remediation or improvements in its systems, processes and technologies.

Documentation

3.22 The Code requires that a RPSO or SSP must make a written record of the assessments made as a result of the Operational Resilience Framework procedures and to share this with the Bank only if requested to do so.

3.23 In particular, a RPSOs or SSP should make a written record of the determinations made in respect of:

- the identification of its important business services;
- the setting of its impact tolerances for those important business services;
- the mapping and identification of interdependencies in relation to those important business services; and
- the testing, monitoring and reporting of its important business services ability to stay within their impact tolerance.

Governance Arrangements

3.24 The Bank expects that a credible Operational Resilience Framework will not only take into account testing and improvement of the Framework, but will also be subject to a RPSO's or SSP's governance process.

3.25 A RPSO's or SSP's board must assure itself that the Operational Resilience Framework is fit for purpose through its usual processes. The Code requires a RPSO's and SSP's board to ensure that it regularly reviews and approves the written record (the Operational Resilience Framework) and key elements identified by the relevant subcommittee, at intervals it deems appropriate. The Bank considers that such a review should take place following events where an impact tolerance has been breached.

3.26 In addition, the Bank considers that the body designated by the board of directors with responsibility for risk management should:

- approve a RPSO's or SSP's identified list of important business services;
- approve a RPSO's or SSP's impact tolerances for the important business services;
- be satisfied that a RPSO's or SSP's important business services are mapped effectively;
- review the results of impact tolerance testing; and
- be satisfied that appropriate risk mitigation steps have been undertaken.

3.27 A RPSO's or SSP's Operational Resilience Framework should be subject to assessment by the body designated by the board of directors with responsibility for audit periodically, in line with its audit approach but taking into consideration material changes to the Framework.

3.28 This internal audit assessment should cover: i) the extent to which the Operational Resilience Framework satisfies the Bank's expectations and requirements as laid out in this SS and the Code; and ii) the effectiveness of a RPSO's and SSP's operational resilience processes.

3.29 This assessment should be reviewed by a RPSO's or SSP's body designated by the board of directors with responsibility for audit.