



BANK OF ENGLAND

Financial Market
Infrastructure



Supervisory Statement

Operational Resilience: Recognised Payment System Operators and Specified Service Providers

March 2021





BANK OF ENGLAND

Supervisory Statement

Operational Resilience: Recognised Payment System Operators and Specified Service Providers

March 2021

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's 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 financial market infrastructure firms (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 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, Prudential Regulation Authority and Financial Conduct Authority. 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 service 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 a 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 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

2.6 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.

2.7 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. The Bank also expects RPSOs and SSPs to consider the implications for their impact tolerance should more than one important business service be disrupted at the same time.

2.8 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 PFMI (3.17.14), which should continue to apply where applicable.¹ 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.

¹ 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 PFMI and Annex F (3) of the PFMI, 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, and 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 RPSO must set an impact tolerance for each of its important business services. A RPSO 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 RPSO has set for it. The Bank also expects a RPSO to consider the implications for their impact tolerance should more than one important business service be disrupted at the same time. A RPSO may be unable to meet the impact tolerance in all circumstances; in this instance the Bank expects a RPSO 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. The Bank also expects a SSP to

consider the implications for their impact tolerance should more than one important business service be disrupted at the same time.

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 PFMI 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 RPSO 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's 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 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.

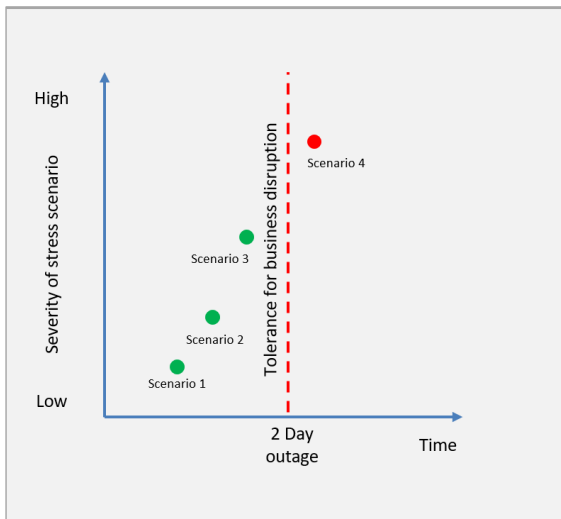
3.18 The mapping of dependencies process should include any outsourced providers, including critical service providers that a RPSO or SSP considers to be involved in the supply of important business services. RPSO or SSP should review the risks to its important business services from other parties as 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. This is illustrated in **Figure 1**. 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.

Figure 1 – Extreme but plausible disruption scenarios

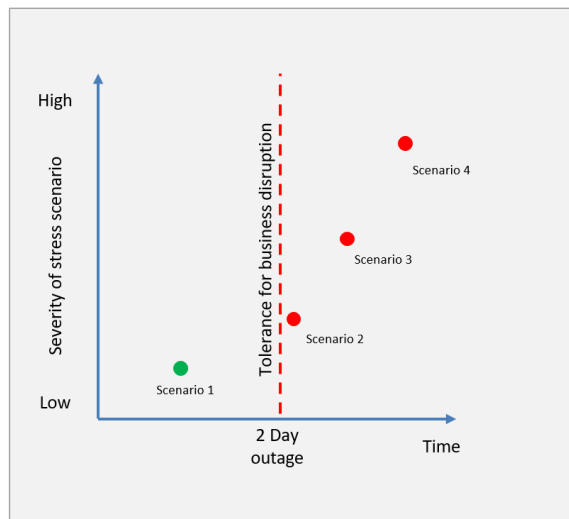
Case one: A RPSO or SPP considers its impact tolerance against extreme but plausible scenarios. Operational resilience is sufficient – it is disproportionate to expect the RPSO or SPP not to breach its impact tolerance in the extreme scenario of scenario 4 .



Key

- Scenario recovered within tolerance
- Scenario not recovered within tolerance

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



Key

- Scenario recovered within tolerance
- Scenario not recovered within tolerance

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 its risk management framework and what mitigating actions will be taken or how

business continuity planning and disaster recovery will be enhanced to ensure that the important business service can be brought within the firm's impact tolerance should disruption reoccur. 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 processes.

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.

Implementation

3.30 Under the amended Code, which applies from 31 March 2022, RPSOs and SSPs must identify important business services; set appropriate impact tolerances; and regularly test their ability to meet tolerances with due regard to the mapping of dependencies. Within a reasonable time after 31 March 2022 and in any event no later than 31 March 2025, RPSOs and SSPs must take all reasonable actions to ensure they remain within impact tolerance for each important business service in the event of an extreme but plausible disruption. RPSOs and SSPs must not wait until 31 March 2025 to take action to ensure they remain within impact tolerance.

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 section 196 of the Banking Act 2009, which can result in the imposition of a sanction under section 198 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 (section 197 Banking Act 2009).

Commencement

- C. These amendments to the code of practice come into force on 31 March 2022.

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

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

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 the recovery times specified in the CPMI-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 31 March 2025.

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

- 5.4 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.
- 5.5 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*.
- 5.6 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 rule 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.