



BANK OF ENGLAND

Financial Market
Infrastructure



Supervisory Statement

Operational Resilience: Central Securities Depositories

March 2021





BANK OF ENGLAND

Supervisory Statement

Operational Resilience: Central Securities Depositories

March 2021

1 Introduction

1.1 This Supervisory Statement (SS) is relevant to all Bank of England (Bank) authorised central securities depositories (CSDs) and any CSDs seeking authorisation by the Bank. It explains the Bank's supervisory approach to operational resilience, which is relevant to many areas of a CSD's operations. The Bank considers disruption to settlement has the potential to be a financial stability issue, meaning that a lack of resilience amongst CSDs would therefore represent a threat to the Bank's financial stability objective.¹ The Bank therefore considers that improvements in operational resilience, consistent with the approach for other Financial Market Infrastructure firms (FMI), should be facilitated by supervisory expectations.

1.2 The policy objective of this SS is for CSDs to be resilient to operational disruption events. Consistent with the approach for other FMIs, this SS contains a set of actions that the Bank expects CSDs 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 CSDs' 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.

1.3 The final policy set out in this SS has been designed in the context of the UK having left the European Union and the transition period having come to an end. Unless otherwise stated, any references to EU or EU derived legislation refer to the version of that legislation which forms part of retained EU law.

Relationship with CSDR and associated technical standards

1.4 The actions that the Bank expects CSDs to take as a result of this SS are grounded in the requirements established in Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 ('CSDR') and Commission Delegated Regulation (EU) No 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories ('RTS 2017/392').

1.5 In particular, Article 70 of RTS 2017/392, which specifies further Article 47 of RTS 2017/392, establishes a requirement that a 'CSD shall have in place a well-documented framework for the management of operational risk with clearly assigned roles and responsibilities. A CSD shall have appropriate IT systems, policies, procedures and controls to identify, measure, monitor, report on and mitigate its operational risk.' This SS is consistent with this requirement. The Bank has developed expectations that a CSD should establish an 'Operational Resilience Framework', as part of which a CSD should identify its 'important business services', establish an 'impact tolerance' for these services and identify and map their dependencies, and use scenario testing to establish whether they can stay within their impact tolerances. Definitions for these terms are provided in Chapter 2.

1.6 This SS introduces the concept of important business services. The Bank views the concept of important business services as broader than the concept of 'critical operations' established in Article

¹ Financial stability objective' means the objective set out in section 2A of the Bank of England Act 1998.

22 (2) CSDR and Article 78(1) of RTS 2017/392. However, the Bank views the expectation that a CSD should identify its important business services and the risks to these business services as consistent with Article 66 (2) of RTS 2017/392, which requires a CSD to identify all potential single points of failure in its operations and assess the evolving nature of the operational risk that it faces. The requirement in Article 78 (2) and Article 77 (2) of RTS 2017/392, for a CSD to identify and include a recovery-time objective no longer than two hours for critical operations, and to conduct a risk analysis to identify how various scenarios affect the continuity of its critical operations, would only apply to an important business service that a CSD considers to be a 'critical operation'.

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 CSDs must continue to meet the requirements established by CSDR and its associated technical standards. No additional requirements are imposed by this SS beyond those imposed by CSDR and its associated technical standards and the Bank considers all expectations set out in this SS to be consistent with the general requirements of Article 45 of CSDR and Article 70 of CSDR RTS 2017/392, as set out above.

1.9 Relevant CSDR standards are italicised and embedded in the body in the text and following each relevant section:

(Article 22(2) of CSDR)

(Article 45 of CSDR)

(Article 70 of CSDR RTS 2017/392)

(Article 77(2) of CSDR RTS 2017/392)

(Article 78(2) of CSDR RTS 2017/392)

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 CSD's Operational Resilience Framework.

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 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. However, the relevant articles of CSDR and associated technical standards are referenced throughout.

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 A business service is a service that a CSD provides, delivering a specific outcome or utility to an identifiable participant. The Bank considers that a business service is an 'important business service' if a prolonged disruption of that business service would significantly disrupt the orderly functioning of a market which a CSD serves, thereby impacting financial stability.

2.4 This definition of important business services is broader than the concept of 'critical operations' established in Article 78 (1) of RTS 2017/392.

2.5 CSDs are expected to identify whether a business service is important by considering a variety of factors. Examples of factors that are relevant to the identification of a business service might be:

- the market share of the CSD;
- the number of members the CSD serves;
- the substitutability of the business service; or
- regulatory driven activity or external obligations.

2.6 This identification process should identify specific market or product business services that a CSD provides but it should 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:

- Issuance;
- settlement (by product type);
- custodian relations and management;
- credit risk management;
- collateral management; and
- reimbursement procedures and sanctioning rates.

(Article 78 (1) of CSDR RTS 2017/392)

Impact tolerance

2.7 Impact tolerance is the maximum tolerable level of disruption for an important business service, whereby further disruption would pose a significant impact to the market the CSD serves. A CSD 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 participants impacted, the volumes and values of transactions affected. The Bank also expects CSDs to consider the implications for their impact tolerance should more than one important business service be disrupted at the same time.

2.8 The Bank views a CSD's impact tolerance for an important business service as distinct to the recovery-time objective for a CSD's critical operations established in Article 78(2) of RTS 2017/392. This recovery-time objective for a CSD's critical operations must be met and should be identified and catered for in a CSD's disaster recovery plan.

2.9 As noted above, the Bank views the definition of important business services as broader than the concept of 'critical operations'. The recovery-time objective need not, therefore, apply to all important business services, but only to those that are also considered to be 'critical operations'.

(Article 78 (2) of CSDR RTS 2017/392)

3 The Bank's expectations regarding a CSD's Operational Resilience Framework

3.1 The Bank expects a CSD to produce an Operational Resilience Framework and associated material. This framework is an approach which will establish how the CSD will meet the operational resilience objectives set out in this SS. The framework should ensure that a CSD 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 views a CSD's production of an Operational Resilience Framework as consistent with the requirement in Article 70 (1) of CSDR RTS 2017/392 for a CSD to 'have in place a well-documented framework for the management of operational risk with clearly assigned roles and responsibilities.' The Bank views the Operational Resilience Framework as consistent with the business continuity policy and disaster recovery plan referred to in Article 57 (2) (j) of CSDR RTS 2017/392, and not in conflict with those requirements.

3.3 The Framework should focus on a CSD's ability to:

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

3.4 The Bank expects an Operational Resilience Framework to 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 (operational assets) 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 testing and utilising the results of such testing in order to make improvements to its procedures and capabilities for minimisation of the likelihood of and the mitigation of, and 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, markets and products.

3.6 The Bank views the expectation that a CSD carries out communications planning as consistent with the requirement in Article 78 (4) (d) of RTS 2017/392 that a CSD shall develop and maintain detailed procedures and plans concerning crisis management and communications, including appropriate contact points, to ensure that reliable and up to date information is transmitted to relevant stakeholders and the competent authority.

(Article 57 (2) (j) of CSDR RTS 2017/392)

(Article 70 (2) of CSDR RTS 2017/392)

(Article 78 (4) (d) of CSDR RTS 2017/392)

Identification of important business services and risks to important business services

3.7 A CSD 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.

3.8 The Bank expects a CSD to be capable of identifying all types of important business services in order to understand both the implications of disruption of a particular business process to a participant as well as the interrelationship and interdependency between important business services in the way they support a participant.

3.9 The Bank expects a CSD, 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 the CSD for the purposes of managing operational resilience. Each CSD is expected to use its own risk assessment based upon its own

circumstances, markets, products and operational structure to understand which operational risks are relevant, and where operational resilience issues exist.

3.10 The Bank views the concept of important business services as broader than the concept of 'critical operations' established in Article 78(2) of RTS 2017/392. However, the Bank views the expectation that a CSD should identify its important business services and the risks to these business services as consistent with Article 66 (2) of RTS 2017/392, which requires a CSD to identify all potential single points of failure in its operations and assess the evolving nature of the operational risk that it faces.

3.11 A non-exhaustive set of examples of the types of risks that the Bank might expect to be considered by a CSD are listed below.

- **Data breach:** participant or other business data compromised, for example through a cyber-attack.
- **Internal fraud:** transactions intentionally mis-reported.
- **External fraud:** theft/robbery.
- **Employment practices:** compensation and/or benefit failure, termination issues, organised labour activity.
- **Clients, Products & Business practices:** legal 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, model or system mis-operation, delivery failure, collateral management failure.

(Article 66 (2) of CSDR RTS 2017/392)

(Article 78 (2) of CSDR RTS 2017/392)

Setting the impact tolerance for important business services

3.12 The Bank expects a CSD to 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 CSD to ensure that each important business service remains within the impact tolerance which the CSD has set for it. The Bank expects a CSD to also consider the implications for their impact tolerance should more than one important business service be disrupted at the same time. A CSD may be unable to meet the impact tolerance in all circumstance, in this instance the Bank expects a CSD 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. The Bank views this expectation as consistent with the requirements laid out in Article 70 (3) of RTS 2017/392, for a CSD to 'define and document clear operational reliability objectives, including operational performance objectives and committed service-level targets for its services and securities settlement systems. It shall have policies and procedures in place to achieve those objectives'.

3.13 The Bank considers that an impact tolerance differs from a 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.

3.14 The Bank views the impact tolerance as distinct to the recovery time objective for a CSD's critical services established in Article 78(2) of RTS 2017/392. This is because the Bank views the definition of important business services as broader than the concept of 'critical operations'. The recovery time objective, therefore, only applies to those important business services that are considered to also be 'critical operations'. This two hour maximum recovery time for a CSD's 'critical operations' must be met and should be identified and catered for in a CSD's disaster recovery plan.

3.15 Further, the Bank views the expectation that a CSD should set an impact tolerance for its important business services as consistent with Article 49 (2) (third sub-paragraph) of RTS 2017/392, which requires that a CSD's board shall define, determine and document an appropriate level of risk tolerance and risk bearing capacity for the CSD. The Bank's expectations of a CSD's board are outlined in paragraphs 3.31-3.36.

3.16 The Bank expects that in setting an impact tolerance for important business services, a CSD should leverage existing risk management frameworks to determine the acceptable level of disruption it is able to tolerate. A CSD may already be setting its own risk appetites based on its existing risk management framework.

3.17 The CSD should also set out the metrics that it will consider and monitor when setting a tolerance, which may be qualitative or quantitative. These metrics need not necessarily be time-based, but could instead be based on financial loss to participants, or counterparties impacted as a result of market disruption. The Bank does not propose any specific metrics for this purpose. The Bank considers this expectation to be consistent with the requirement in Article 70 (4) of RTS 2017/392, which requires a CSD to 'ensure that its operational performance objectives and service-level targets...include both qualitative and quantitative measures of operational performance.'

3.18 The Bank expects a CSD to 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.

(Article 49 (2) (third sub-paragraph) of CSDR RTS 2017/392)

(Article 70 (3) of CSDR RTS 2017/392)

(Article 70 (4) of CSDR RTS 2017/392)

(Article 78 (2) of CSDR RTS 2017/392)

Mapping and identification of dependencies

3.19 The Bank expects a CSD to map dependencies. Mapping of dependencies should entail a CSD identifying and documenting the necessary people, processes, technology, facilities and information required to deliver each of the CSD's important business services. This mapping should facilitate the gathering of evidence to diagnose and remedy vulnerabilities in a CSD'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.

3.20 The Bank considers that the mapping and identification of dependencies is consistent with the requirement in Article 77 (1) (a) of RTS 2017/392 for a CSD to conduct a business impact analysis to

prepare a list with all the processes and activities that contribute to the delivery of the services it provides. However, the Bank expects this mapping exercise to be broader in scope and application as it encompasses important business services, whose definition is broader than the concept of ‘critical operations’ established in Article 78(2) of RTS 2017/392, as explained in paragraphs 1.6 and 2.9 above.

3.21 Mapping of the dependencies within important business services should allow a CSD to comprehensively understand how interconnected or concentrated its important business services, products, and markets are. This is necessary in order to design, understand and evaluate the full implications of scenarios (as described in 3.24 below). This will help the CSD to prioritise its mitigation and recovery actions by identifying specific vulnerabilities.

3.22 The Bank proposes that the mapping of dependencies should include any outsourced providers, including critical service providers that the CSD considers to be involved in the supply of important business services. A CSD should review the risks to its important business services from other parties as a result of inter-dependencies, and develop appropriate risk management tools. The Bank considers this expectation be consistent with the requirement under Article 68 (1) of RTS 2017/392, which states a CSD ‘shall identify critical utilities providers and critical service providers that may pose risks to CSD's operations due to its dependency on them’.

(Article 68 (1) of CSDR RTS 2017/392)

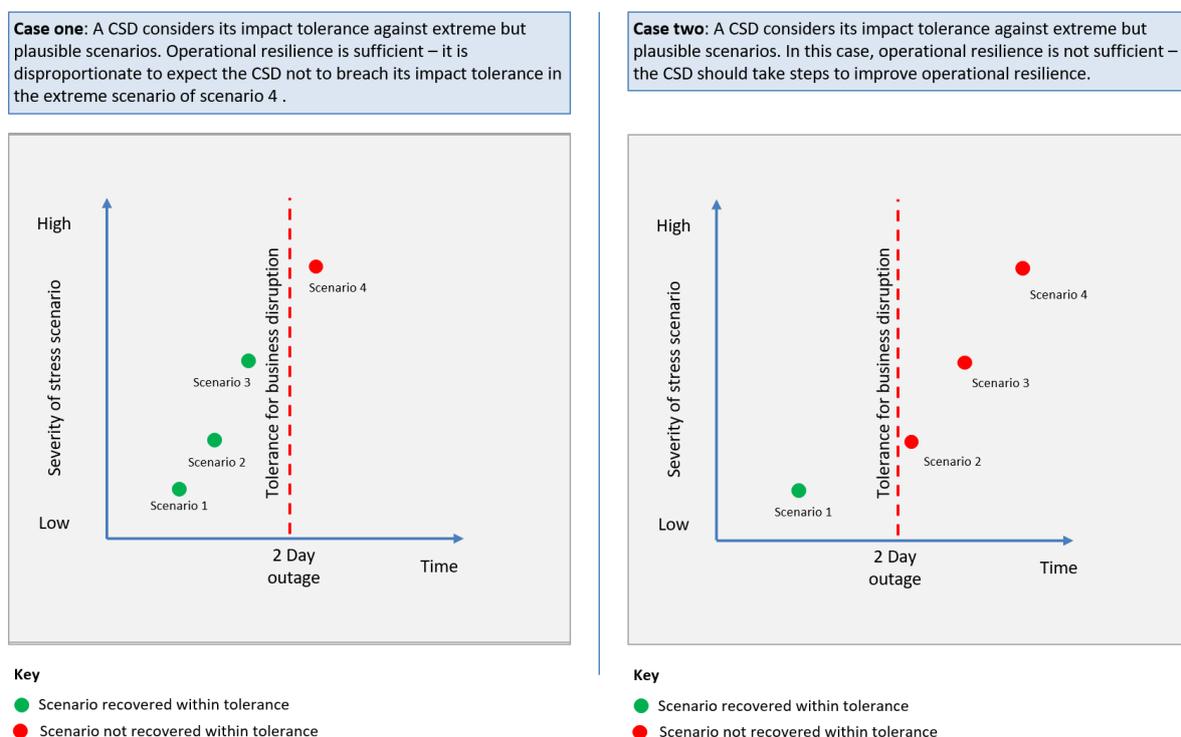
(Article 77 (1) (a) of CSDR RTS 2017/392)

(Article 78(2) of CSDR RTS 2017/392)

Testing, Monitoring and Reporting

3.23 The Bank expects that a CSD will 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**. Once a CSD has established what its important business services are, and an impact tolerance for each important business service, the CSD 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



3.24 The Bank considers that the testing of important business services against disruption scenarios is consistent with the requirement in Article 77 (2) of CSDR RTS 2017/392 for a CSD to identify how various scenarios affect the continuity of its critical operations. The Bank also considers that testing important business services against disruption scenarios is consistent with the requirement under Article 79 of RTS 2017/392 for a CSD to monitor its business continuity policy and disaster recovery plan and test them at least annually. However, the Bank's expectation of testing is broader in scope and application as it encompasses important business services, whose definition is broader than the concept of 'critical operations' established in Article 78(2) of RTS 2017/392.

3.25 A CSD 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 the CSD's important business services in those scenarios.

3.26 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 CSD to be able to provide an explanation as to why this has happened and what remedial actions the CSD will undertake to ensure the impact tolerance can be met in future. In such situations, the Bank expects that the CSD 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 CSD's impact tolerance should disruption occur. In addition, the Bank expects the relevant important business service to be prioritised when the CSD makes choices about remediation or improvements in its systems, processes and technologies.

3.27 In setting an impact tolerance for important business services, CSDs 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 a CSD's ability to stay within the defined impact tolerance.

(Article 77 (2) of CSDR RTS 2017/392)

(Article 78(2) of CSDR RTS 2017/392)

(Article 79 of CSDR RTS 2017/392)

Documentation

3.28 The Bank expects that a CSD will 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.

3.29 The Bank considers that this requirement for a CSD to maintain documentation relating to its Operational Resilience Framework is consistent with the requirement in Article 47(1) of RTS 2017/392 for a CSD to establish documented policies, procedures and systems that identify, measure, monitor, manage and enable reporting on the risks that the CSD may be exposed to and

the risks that the CSD poses to any other entities including its participants and their clients, as well as linked CSDs, banks, trading venues, payment systems, settlement banks, liquidity providers and investors. The Bank also considers this consistent with the requirement in Article 77(3) of RTS 2017/392 for a CSD to ensure its business impact analysis and risk analysis are kept up to date.

In particular, the CSD 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.

(Article 47 (1) of CSDR RTS 2017/392)

(Article 77 (3) of CSDR RTS 2017/392)

Governance arrangements

3.30 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 CSD's governance process.

3.31 The Bank considers that this expectation for a CSD's Operational Resilience Framework to be subject to a CSD's governance process is consistent with the requirement in Article 49(2) (third subparagraph) of RTS 2017/392 for the management body of a CSD to assume final responsibility for managing a CSD's risks.

3.32 The Bank expects a CSD's board to assure itself that the Operational Resilience Framework is fit for purpose. The Bank expects a CSD's board to ensure that it regularly reviews and approves the Operational Resilience Framework, at intervals it deems appropriate or following event where an impact tolerance has been breached.

3.33 The body with responsibility for risk management as designated by the board of directors should:

- approve the CSD's identified list of important business services;
- approve the CSD's impact tolerances for the important business services;
- be satisfied that the CSD'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.

3.34 A CSD's Operational Resilience Framework should be subject to periodic assessment by the body designated with responsibility for audit by the board of directors, in line with its audit approach

but taking into consideration material changes to the Framework. The Bank considers this expectation to be consistent with the requirement in Article 73 (1) of RTS 2017/392, which states that ‘a CSD’s operational risk-management framework and systems shall be subject to audits’.

3.35 This internal audit assessment should cover: i) the extent to which the Operational Resilience Framework satisfies the Bank’s expectations as laid out in this SS; and ii) the effectiveness of the CSD’s operational resilience processes.

(Article 49 (2) (third sub-paragraph) of CSDR RTS 2017/392)

(Article 73 (1) of CSDR RTS 2017/392)

Implementation

3.36 The policy takes effect from 31 March 2022, where CSDs are expected to identify important business services; set 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, CSDs are expected to take all reasonable actions to ensure they remain within their impact tolerances in the event of extreme but plausible disruption to operations. CSDs must not wait until 31 March 2025 to take action to ensure they remain within impact tolerance.