Commission Delegated Regulation (EU) 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 (Text with EEA relevance)

CHAPTER X

OPERATIONAL RISKS

(Article 45(1) to (6) of Regulation (EU) No 909/2014)

SECTION 1

Identifying operational risks

Article 66

General operational risks and their assessment

1 The operational risks referred to in Article 45(1) of Regulation (EU) No 909/2014 comprise the risks caused by deficiencies in information systems, internal processes, and personnel's performance or disruptions caused by external events that result in the reduction, deterioration or interruption of services provided by a CSD.

2 A CSD shall identify all potential single points of failure in its operations and assess the evolving nature of the operational risk that it faces, including pandemics and cyber-attacks, on an ongoing basis.

Article 67

Operational risks that may be posed by key participants

1 A CSD shall, on an ongoing basis, identify the key participants in the securities settlement system that it operates based on the following factors:

a their transaction volumes and values;

b material dependencies between its participants and its participants' clients, where the clients are known to the CSD, that might affect the CSD;

c their potential impact on other participants and the securities settlement system of the CSD as a whole in the event of an operational problem affecting the smooth provision of services by the CSD.

For the purposes of point (b) in the first subparagraph, the CSD shall also identify the following:

(i) the participants' clients responsible for a significant proportion of transactions processed by the CSD;

(ii) the participants' clients whose transactions, based on their volumes and values, are significant relative to the respective participants' risk-management capacity.

2 A CSD shall review and keep the identification of the key participants up-to-date on an ongoing basis.

3 A CSD shall have clear and transparent criteria, methodologies and standards in order to ensure that key participants meet the operational requirements.

4 A CSD shall, on an ongoing basis, identify, monitor, and manage the operational risks that it faces from key participants.

For the purposes of the first subparagraph, the operational risk-management system referred to in Article 70 shall also provide for rules and procedures to gather all relevant information about their participants' clients. The CSD shall also include in the agreements with its participants all terms necessary to facilitate the gathering of that information.

Article 68

Operational risks that may be posed by critical utilities and critical service providers

1 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.

2 A CSD shall take appropriate actions to manage the dependencies referred to in paragraph 1 through adequate contractual and organisational arrangements, as well as through specific provisions in its business continuity policy and disaster recovery plan, before any relationship with those providers becomes operational.

3 A CSD shall ensure that its contractual arrangements with any providers identified in accordance with paragraph 1 require a prior approval of the CSD for the service provider to further subcontract any elements of the services provided to the CSD.

Where the service provider outsources its services in accordance with the first subparagraph, the CSD shall ensure that the level of service and its resilience is not impacted and full access by the CSD to the information necessary for the provision of the outsourced services is preserved.

4 A CSD shall establish clear lines of communication with the providers referred to in paragraph 1 to facilitate the exchange of information in both ordinary and exceptional circumstances.

5 A CSD shall inform its competent authority about any dependencies on utilities and service providers identified under paragraph 1 and take measures to ensure that authorities can obtain information about the performance of those providers, either directly from utilities or service providers or through the CSD.

Article 69

Operational risks that may be posed by other CSDs or market infrastructures

1 A CSD shall ensure that its systems and communication arrangements with other CSDs or market infrastructures are reliable, secure and designed to minimise operational risks.

2 Any arrangement that a CSD enters into with another CSD or another market infrastructures shall provide that:

a the other CSD or other financial market infrastructure discloses to the CSD any critical service provider on which the other CSD or market infrastructure relies;

b the governance arrangements and management processes in the other CSD or other market infrastructure do not affect the smooth provision of services by the CSD, including the risk-management arrangements and the non-discriminatory access conditions.

SECTION 2

Methods to test, address and minimise operational risks

Article 70

Operational risk-management system and framework

1 As part of the policies, procedures and systems referred to in Article 47, 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.

2 The management body and the senior management of a CSD shall determine, implement and monitor the risk-management framework for operational risks referred to in paragraph 1, identify all of the CSD's exposures to operational risk and track relevant operational risk data, including any cases where material data is lost.

3 A CSD shall 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.

4 A CSD shall ensure that its operational performance objectives and service-level targets referred to in paragraph 3 include both qualitative and quantitative measures of operational performance.

5 A CSD shall regularly monitor and assess whether its established objectives and service-level targets are met.

6 A CSD shall have rules and procedures in place that ensure that the performance of its securities system is reported regularly to senior management, members of the management body, relevant committees of the management body, user committees and the competent authority.

7 A CSD shall periodically review its operational objectives to incorporate new technological and business developments.

8 A CSD's operational risk-management framework shall include change-management and project-management processes to mitigate operational risk arising from modifications to operations, policies, procedures and controls put in place by the CSD.

9 A CSD's operational risk-management framework shall include a comprehensive framework for physical security and information security to manage the risks that the CSD faces from attacks, including cyber-attacks, intrusions and natural disasters. That comprehensive framework shall enable the CSD to protect the information at its disposal from unauthorised

access or disclosure, ensure data accuracy and integrity and maintain availability of the services provided by the CSD.

10 A CSD shall put in place appropriate procedures concerning human resources to employ, train and retain qualified personnel, as well as mitigate the effects of personnel turnover or overreliance on key personnel.

Article 71

Integration of and compliance with the operational and enterprise risk-management system

1 A CSD shall ensure that its operational risk-management system is part of its day-to-day risk-management processes and that their results are taken into account in the process of determining, monitoring and controlling the CSD's operational risk profile.

2 A CSD shall have in place mechanisms for regular reporting to the senior management of operational risk exposures and losses experienced from operational risks, and procedures for taking appropriate corrective action to mitigate those exposures and losses.

3 A CSD shall have in place procedures for ensuring compliance with the operational risk-management system, including internal rules on the treatment of failures in the application of that system.

4 A CSD shall have comprehensive and well-documented procedures to record, monitor and resolve all operational incidents, including:

a a system to classify the incidents taking into account their impact on the smooth provision of services by the CSD;

b a system for reporting material operational incidents to the senior management, the management body and the competent authority;

c a ‘post-incident’ review after any material disruption in the CSD's activities, to identify the causes and required improvements to the operations or business continuity policy and disaster recovery plan, including to the policies and plans of the users of the CSD. The result of that review shall be communicated to the competent authority and relevant authorities without delay.

Article 72

Operational risk-management function

As part of the risk-management function, the operational risk-management function of a CSD shall manage the CSD's operational risk. It shall in particular:

(a) develop strategies, policies and procedures to identify, measure, monitor and report on operational risks;

(b) develop procedures to control and manage operational risks, including by introducing any necessary adjustments in the operational risk-management system;

(c) ensure that the strategies, policies and procedures referred to in points (a) and (b) are properly implemented.

Article 73

Audit and testing

1 A CSD's operational risk-management framework and systems shall be subject to audits. The frequency of those audits shall be based on a documented risk assessment and shall be conducted at least once every two years.

2 The audits referred to in the previous paragraph shall include both the activities of the internal business units of the CSD and those of the operational risk-management function.

3 A CSD shall regularly evaluate and, where necessary, adjust the system for the management of operational risk.

4 A CSD shall periodically test and review the operational arrangements, policies and procedures with users. The testing and review shall also be performed where substantive changes occur to the securities settlement system operated by the CSD or after operational incidents that affect the smooth provision of services by the CSD.

5 A CSD shall ensure that data flows and processes associated with the operational risk-management system are accessible to the auditors without delay.

Article 74

Mitigation of operational risk through insurance

A CSD may only contract insurance to mitigate the operational risks referred to in this Chapter where the measures referred to in this Chapter do not fully mitigate operational risks.

SECTION 3

IT systems

Article 75

IT tools

1 A CSD shall ensure that its information technology (IT) systems are well-documented and that they are designed to cover the CSD's operational needs and the operational risks that the CSD faces.

The CSD IT systems shall be:

a resilient, including in stressed market conditions;

b have sufficient capacity to process additional information as a result of increasing settlement volumes;

c achieve the service level objectives of the CSD.

2 A CSD systems shall have sufficient capacity to process all transactions before the end of the day even in circumstances where a major disruption occurs.

A CSD shall have procedures for ensuring sufficient capacity of its IT systems, including in the case of the introduction of new technology.

3 A CSD shall base its IT systems on internationally recognised technical standards and industry best practices.

4 A CSD's IT systems shall ensure that any data at the disposal of the CSD is protected from loss, leakage, unauthorised access, poor administration, inadequate record-keeping, and other processing risks.

5 A CSD's information security framework shall outline the mechanisms that the CSD have in place to detect and prevent cyber-attacks. The framework shall also outline the CSD's plan in response to cyber-attacks.

6 The CSD shall subject its IT systems to stringent testing by simulating stressed conditions before those systems are used for the first time, after making significant changes to the systems and after a major operational disruption has occurred. A CSD shall, as appropriate, involve in the design and conduct of these tests:

a users;
b critical utilities and critical service providers;
c other CSDs;
d other market infrastructures;
e any other institutions with which interdependencies have been identified in the business continuity policy.

7 The information security framework shall include:

a access controls to the system;
b adequate safeguards against intrusions and data misuse;
c specific devices to preserve data authenticity and integrity, including cryptographic techniques;
d reliable networks and procedures for accurate and prompt data transmission without major disruptions; and
e audit trails.

8 The CSD shall have arrangements for the selection and substitution of IT third party service providers, CSD's timely access to all necessary information, as well as proper controls and monitoring tools.

9 The CSD shall ensure that the IT systems and the information security framework concerning the CSD's core services are reviewed at least annually and are subject to audit assessments. The results of the assessments shall be reported to the CSD's management body and to the competent authority.

Business continuity

Article 76

Strategy and policy

1 A CSD shall have a business continuity policy and associated disaster recovery plan that is:

a approved by the management body;

b subject to audit reviews that shall be reported to the management body.

2 A CSD shall ensure that the business continuity policy:

a identifies all its critical operations and IT systems and provides for a minimum service level to be maintained for those operations;

b includes the CSD's strategy and objectives to ensure the continuity of operations and systems referred to in point (a);

c takes into account any links and interdependencies to at least:

(i) users;

(ii) critical utilities and critical service providers;

(iii) other CSDs;

(iv) other market infrastructures;

d defines and documents the arrangements to be applied in the event of a business continuity emergency or major disruption of the CSD's operations in order to ensure a minimum service level of critical functions of the CSD;

e identifies the maximum acceptable period of time which critical functions and IT systems may be out of use.

3 A CSD shall take all reasonable steps to ensure that settlement is completed by the end of the business day even in case of a disruption, and that all the users' positions at the time of the disruption are identified with certainty in a timely manner.

Article 77

Business impact analysis

1 A CSD shall conduct a business impact analysis to:

a prepare a list with all the processes and activities that contribute to the delivery of the services it provides;

b identify and create an inventory of all the components of its IT system that support the processes and activities identified in point (a) as well as their respective interdependencies;

c identify and document qualitative and quantitative impacts of a disaster recovery scenario to each process and activity referred to in point (a) and how the impacts change over time in case of disruption;

d define and document the minimum service levels considered acceptable and adequate from the perspective of the users of the CSD;

c identify and document the minimum resource requirements concerning personnel and skills, work space and IT to perform each critical function at the minimum acceptable level.

2 A CSD shall conduct a risk analysis to identify how various scenarios affect the continuity of its critical operations.

3 A CSD shall ensure that its business impact analysis and risk analysis fulfil all of the following requirements:

a they are kept up to date;

b they are reviewed following a material incident or significant operational changes and, at least, annually;

c they take into account all relevant developments, including market and IT developments.

Article 78

Disaster recovery

1 A CSD shall have in place arrangements to ensure the continuity of its critical operations in disaster scenarios, including natural disasters, pandemic situations, physical attacks, intrusions, terrorist attacks, and cyber-attacks. Those arrangements shall ensure:

a the availability of adequate human resources;

b the availability of sufficient financial resources;

c the failover, recovery and resuming of operations in a secondary processing site.

2 The CSD's disaster recovery plan shall identify and include a recovery-time objective for critical operations and determine for each critical operation the most suitable recovery strategies. The recovery-time objective for each critical operation shall not be longer than two hours. The CSD shall ensure that back-up systems commence processing without undue delay unless this would jeopardise the integrity of the securities issues or the confidentiality of the data maintained by the CSD. A CSD shall ensure that two hours from a disruption, it is capable of resuming its critical operations. In determining the recovery times for each operation, the CSD shall take into account the potential overall impact on the market efficiency. Those arrangements shall at least ensure that, in extreme scenarios, agreed service levels are met.

3 A CSD shall maintain at least a secondary processing site with sufficient resources, capabilities, functionalities and staffing arrangements, which are adequate to the CSD's operational needs and risks that the CSD faces in order to ensure continuity of critical operations, at least in case the main location of business is not available.

The secondary processing site shall:

a provide the level of services necessary to ensure that the CSD performs its critical operations within the recovery time objective;

b be located at a geographical distance from the primary processing site that allows the secondary processing site to have a distinct risk profile and prevents it from being affected by the event affecting the primary processing site;

c is immediately accessible by the CSD's staff in order to ensure continuity of its critical operations where the primary processing site is not available.

4 A CSD shall develop and maintain detailed procedures and plans concerning:

a the identification, logging and reporting of all disruptive events for the operations of the CSD;

b response measures to operational incidents and emergency situations;

c the assessment of damages, and appropriate plans for activating the response measures referred to in point (b);

d 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;

e the activation and transition to alternative operational and business sites;

f IT recovery, including activation of the secondary IT processing site and failover.

Article 79

Testing and monitoring

A CSD shall monitor its business continuity policy and disaster recovery plan and test them at least annually. The CSD shall also test its business continuity policy and disaster recovery plan after substantive changes to the systems or related operations in order to ensure that the systems and operations achieve the CSD objectives. The CSD shall plan and document these tests, which shall include:

(a) scenarios of large scale disasters;

(b) switchovers between the primary processing site and secondary processing site;

(c) the participation of, as appropriate:

(i) users of the CSD;

(ii) critical utilities and critical service providers;

(iii) other CSDs;

(iv) other market infrastructures;

(v) any other institution with which interdependencies have been identified in the business continuity policy.

Article 80

Maintenance

1 A CSD shall regularly review and update its business continuity policy and disaster recovery plan. The review shall include all critical operations of a CSD and provide for the most suitable recovery strategy for those operations.

2 When updating the business continuity policy and disaster recovery plan, a CSD shall take into consideration the outcome of the tests and recommendations from the audit reviews and from the competent authority.

3 A CSD shall review its business continuity policy and disaster recovery plan after every significant disruption of its operations. That review shall identify the causes of the disruption and any required improvement to the CSD's operations, the business continuity policy and disaster recovery plan.

Changes to legislation:
Commission Delegated Regulation (EU) 2017/392, CHAPTER X is up to date with all changes known to be in force on or before 06 August 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations.
EUR 2017 No. 392 may be subject to amendment by EU Exit Instruments made by the Bank of England under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 3. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s.
View outstanding changes

Changes and effects yet to be applied to :

– Regulation revoked by 2023 c. 29 Sch. 1 Pt. 13