EUROPEAN
COMMISSION

Brussels, 11.11.2016
C(2016) 7159 final

COMMISSION DELEGATED REGULATION (EU) …/...

of 11.11.2016

supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

Regulation (EU) No 909/2014 ('the Regulation')[1] establishes the requirements and conditions under which Central Securities Depositories ('CSDs') provide their services in the Union. Against this background, it empowers the Commission to adopt, following submission of draft regulatory technical standards by the European Securities and Markets Authority ('ESMA') in accordance with Articles 10 to 14 of Regulation (EU) No 1095/2010 establishing ESMA[2], delegated Regulations specifying the requirements applicable to CSDs under the Regulation, including in particular requirements related to the authorisation and supervision of CSDs, prudential requirements applicable to CSDs and requirements related to non-discriminatory access of users to the services provided by CSDs.

In accordance with Article 10(1) of Regulation (EU) No 1095/2010, the Commission shall decide within three months of receipt of the draft standards whether to endorse the drafts submitted. The Commission may also endorse the draft standards in part only, or with amendments, where the Union's interests so require, having regard to the specific procedure laid down in this Article.

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

In accordance with the third subparagraph of Article 10(1) of Regulation (EU) No 1095/2010, ESMA carried out two public consultations: first on the initial Discussion Paper with the proposed options (during March-April 2014) and then on the draft regulatory technical standards submitted to the Commission in accordance with several empowering provisions of the Regulation. A Consultation Paper containing draft regulatory technical standards was published on 18 December 2014 on the ESMA internet site, and the consultation closed on 19 February 2015.

Moreover, ESMA's Securities and Markets Stakeholder Group set up in accordance with Article 37 of Regulation (EU) No 1095/2010 was also consulted on the draft regulatory technical standards.

Additionally, ESMA involved the European Banking Authority (EBA) and the members of the European System of Central Banks (ESCB) in the development of the relevant technical standards where close cooperation was required under the Regulation.

Alongside the draft technical standards, ESMA submitted a report on how the outcome of these consultations has been taken into account in the development of the final draft regulatory technical standards submitted to the Commission.

Together with the draft regulatory technical standards, and in accordance with the third subparagraph of Article 10(1) of Regulation (EU) No 1095/2010, ESMA submitted its impact assessment, including its analysis of the costs and benefits related to the draft technical standards submitted to the Commission. This analysis is available in Annex III to the Final Report on draft technical standards under the Regulation that can be found at:

---

[1] 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 Directive 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (OJ L 257, 28.8.2014, p. 1).

[2] Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

http://www.esma.europa.eu/system/files/2015-esma-1457_-_annex_iii_-_cba_csdr_ts_on_csd_requirements_and_internalised_settlement.pdf.

Additionally, the Members of the European Parliament in their capacity of the rapporteurs to the file have provided their feedback on the content of ESMA draft regulatory technical standards that were submitted to the Commission.

3. LEGAL ELEMENTS OF THE DELEGATED ACT

The power to adopt a delegated regulation is provided for under Articles 12(3), 17(9), 22(10), 25(12), 55(7), 18(4), 26(8), 29(3), 37(4), 45(7), 46(6), 33(5), 48(10), 49(5), 52(3) and 53(4) of Regulation (EU) No 909/2014.

The issues referred to under those empowerments are closely linked because they all deal with the elements required for the implementation of the measures laid down in Regulation (EU) No 909/2014. All requirements provided in this act were developed by ESMA and submitted to the Commission as draft regulatory technical standards. All those requirements should apply to CSDs and therefore are substantially linked and refer to the same set of definitions. It is, therefore, justified to include all those elements concerning measures under Regulation (EU) No 909/2014 in a single delegated act with regard to regulatory technical standards on authorisation, supervisory and operational requirements for CSDs.

3.1. Chapter II, Articles 2 - 3

The delegated regulation lays the details for co-operation between the CSD's competent authority and other supervisors. In particular, Chapter II specifies the rules on identifying the most relevant currencies in which settlement takes place, according to which the central banks that should be involved in CSDs' authorisation and supervision are determined. Under these rules, the most relevant currencies for a CSD will be identified when at least one of two threshold is met:

- the relative share of each Union currency in the total value of the settlement by a CSD of settlement instructions against payment, calculated over a period of one year, exceeds 1%; or
- the relative share of settlement instructions against payment settled by a CSD in a Union currency compared with the total value of settlement instructions against payment settled in that currency across all CSDs in the Union, calculated over a period of one year, exceeds 10%.

These thresholds ensure that those central banks which are concerned by CSD's activities would be involved in the authorisation and supervision of that CSD.

3.2. Chapter III, Articles 4 - 38

The delegated regulation lays down also the details of CSDs' authorisation and supervision. Chapter III of the delegated regulation specifies the information on CSDs' structure, governance and services, which need to be submitted by an applicant CSD for authorisation. The information to be submitted by a CSD should provide the competent authority with sufficient information to be able to get an overview of a CSD's compliance with the Regulation.

3.3. Chapter IV, Article 39

The delegated regulation provides also the detail of CSD's prudential requirements. Among those, Article 39 of the delegated regulation specifies the criteria to be taken into account by competent authorities when approving acquisitions by CSDs of capital in entities other than those that provide CSDs' core or non-banking type ancillary services. The criteria provided in

a delegated regulation ensure that a participation by a CSD in another entity does not increase significantly the CSD's risk profile.

3.4. Chapter V, Articles 41 - 45

The delegated regulation also specifies the information that a CSD should provide to the competent authority to enable it to review, on an ongoing basis, a CSD's arrangements, strategies, processes and mechanisms with respect to compliance with the Regulation and evaluate the risks to which a CSD is, or might be, exposed or which it creates for the smooth functioning of securities markets.

The delegated regulation sets out the details for co-operation between the CSD's competent authority and other supervisors. In particular, it specifies the information to be exchanged between the competent authorities for the purposes of review and evaluation of CSDs' compliance with the Regulation.

3.5. Chapter VI, Article 46

Chapter VI of the delegated regulation specifies the information to be submitted by third-country CSDs to ESMA when applying for recognition under the Regulation. This information is similar to the information that an EU-based CSD needs to provide for an authorisation but takes into account the fact that the supervision of a third-country CSD will be performed by the relevant supervisory authority of that third country.

3.6. Chapter VII, Articles 47 - 52

Chapter VII of the delegated regulation specifies - at the CSD level and at the group level - monitoring tools for the risks of CSDs and responsibilities of the key personnel with respect to those risks, as well as certain governance arrangements of CSDs (i.e. those related to conflict of interest and audit methods).

3.7. Chapter VIII, Articles 53 - 58

Chapter VIII of the delegated act specifies the requirements for record keeping to be maintained for the purpose of monitoring by the competent authority of CSD's compliance with the provisions of Regulation. According to the Regulation, a CSD should maintain such records on the services and activities for at least 10 years.

3.8. Chapter IX, Articles 59 - 65

As regards the requirements of the Regulation applicable to CSDs with respect to conduct of business, the delegated regulation (in Chapter IX) specifies the reconciliation measures a CSD needs to take in order to verify the integrity of the issue. Those measures include the CSD's rules, procedures and controls to prevent the unauthorised creation or deletion of securities and at least daily reconciliation of the securities accounts that a CSD maintains.

3.9. Chapter X, Articles 66 – 80

Chapter X specifies the operational risks for a CSD, such as those risks posed by key participants and by critical utilities and critical service providers. This Chapter also lays down provisions on CSD's methods to test, address and minimise those risks, including the requirements for operational risk management systems and function, audit and testing of those systems, as well as the need for a business continuity policy and disaster recovery plans, and their testing and monitoring.

3.10. Chapter XI, Articles 81 – 83

The delegated regulation specifies, in Chapter XI, certain requirements concerning a CSD's investment policy such as the financial instruments that can be considered to be highly liquid

with minimal market and credit risk, the appropriate timeframe for access to the CSD's assets and the concentration limits for the CSD's financial assets.

3.11. Chapter XII, Article 84 – 87

Chapter XII of the delegated regulation specifies the conditions under which each type of CSD link arrangement provides for adequate protection of the linked CSDs and their participants, in particular where a CSD intends to participate in the securities settlement system operated by another CSD, as well as other measures related to CSD links. Those measures include monitoring and management of additional risks resulting from the use of indirect links or intermediaries to operate CSD links.

3.12. Chapter XIII, Articles 88 - 90

With respect to rules on access to CSDs, the delegated regulation in Chapter XIII specifies the risks to be taken into account by CSDs when carrying out a comprehensive risk assessment following a request for access to that CSD's services by participants, issuers, other CSDs and other infrastructures (e.g. trading venues and central counterparties). These risks are also to be taken into account by the competent authority when assessing a CSD's refusal of access. These provisions ensure that CSDs provide fair and open access to their services with due regard to the risks to financial stability and the orderliness of the market.

3.13. Chapter XIV, Articles 91 - 94

Chapter XIV of the delegated regulation specifies the information that a CSD should submit when applying for an authorisation to provide banking-type ancillary services. The information required includes a banking licence and evidence confirming that a CSD meets the prudential requirements under Article 59 of the Regulation and that there are no adverse risks stemming from the banking activities of a CSD.

3.14. Chapter XV, Articles 95 – 96

The final and transitional provisions lay down the timeframes for application of certain requirements provided in the delegated act. In particular, the susbmission of certain information for the purposes of CSDs' authorisation process and the record keeping of some data is linked with the entry into force of substantial requirements to which such information relate (e.g. delegates act under Aricles 6(5) and 7(15) of the Regulation which cover measures to prevent and address settlement fails).

COMMISSION DELEGATED REGULATION (EU) …/...

of 11.11.2016

supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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[3], and in particular Article 12(3), Article 17(9), Article 22(10), Article 25(12), Article 55(7), Article 18(4), Article 26(8), Article 29(3), Article 37(4), Article 45(7), Article 46(6), Article 33(5), Article 48(10), Article 49(5), Article 52(3), and Article 53(4) thereof,

Whereas:

(1) The provisions in this Regulation are closely linked, since they all deal with the supervisory requirements applicable to central securities depositories (CSDs). To ensure coherence between these provisions, which should enter into force at the same time, and to facilitate a comprehensive view and easy access by persons that are subject to these provisions, it is desirable to include all the regulatory technical standards concerning the supervisory requirements under Regulation (EU) No 909/2014 in a single Regulation.

(2) In view of the global nature of financial markets and given the commitments undertaken by the Union in this field, due regard should be had to the Principles for Financial Market Infrastructures issued by the Committee on Payment and Settlement Systems and the International Organization of Securities Commissions (CPSS-IOSCO Principles) in April 2012.

(3) In order to ensure consistent application of rules concerning improving securities settlement in the Union, certain technical terms should be clearly defined.

(4) It is important to ensure appropriate authorisation and supervision of a CSD. As such, a list of the relevant authorities issuing the most relevant Union currencies in which settlement takes place to be involved in the process of authorisation and supervision of a CSD should be defined. This should be based on the share of the currencies that those authorities issue in the total value of settlement instructions against payment settled annually by a CSD and on the share of settlement instructions against payment

[3] OJ L 257, 28.8.2014, p. 1

settled by a CSD in a Union currency compared to the total value of settlement instructions against payment settled in that currency across all CSDs in the Union.

(5) In order to allow competent authorities to perform a thorough assessment, a CSD applying for authorisation should provide information on the structure of its internal controls and the independence of its governing bodies to enable the competent authority to assess whether the corporate governance structure ensures the independence of the CSD and whether that structure and its reporting lines, as well as the mechanisms adopted for managing possible conflicts of interest are adequate.

(6) To enable the competent authority to assess the good reputation and the experience and skills of the CSD's senior management and members of the management body, an applicant CSD should provide all relevant information to perform that assessment.

(7) Information on a CSD's branches and subsidiaries is necessary to enable the competent authority to clearly understand the CSD's organisational structure and evaluate any potential risk to the CSD due to the activity of those branches and subsidiaries.

(8) A CSD applying for authorisation should provide the competent authority with the relevant information to demonstrate that it has the necessary financial resources at its disposal and adequate business continuity arrangements for the performance of its functions on an ongoing basis.

(9) In addition to receiving information on the core activities, it is important for the competent authority to receive information on the ancillary services that the CSD applying for authorisation intends to offer to enable the competent authority to have a complete overview of the applicant CSD's services.

(10) In order for the competent authority to assess the continuity and orderly functioning of technological systems of an applicant CSD, that CSD should provide the competent authority with descriptions of the relevant technological systems and how they are managed, including if they are outsourced.

(11) Information concerning the fees associated with the core services provided by CSDs is important and should form part of the application for authorisation of a CSD in order to enable the competent authorities to verify whether those fees are proportionate, non-discriminatory and not bundled with the costs of other services.

(12) In order to ensure that the investors' rights are protected, and that conflict of laws issues are adequately managed, when assessing the measures that a CSD intends to take to allow its users to comply with the national laws referred to in Article 49(1) of Regulation (EU) No 909/2014, the CSD should take into account both issuers and participants, as appropriate, in accordance with the respective national laws.

(13) In order to secure fair and non-discriminatory access to the notary, central maintenance and securities settlement services within the financial market, issuers, other CSDs and other market infrastructures have been granted access to a CSD in accordance with Regulation (EU) No 909/2014. An applicant CSD should, therefore, provide the competent authority with information about its access policies and procedures.

(14) In order to carry out its authorisation duties effectively, the competent authority should receive all information from CSDs applying for authorisation and related third parties, including third parties to whom applicant CSDs have outsourced operational functions and activities.

(15) To ensure general transparency of governance rules of a CSD applying for authorisation, the competent authority should be provided with documents confirming that the applicant CSD has adopted the necessary arrangements for a non-discriminatory establishment of an independent user committee for each securities settlement system that it operates.

(16) To secure the orderly functioning of core infrastructure services within the financial market, a CSD applying for authorisation should provide the competent authority with all necessary information to demonstrate that it has adequate policies and procedures for ensuring reliable record-keeping systems as well as effective mechanisms for CSD services, including in particular the measures for preventing and addressing settlements fails, and the rules concerning the integrity of the issue, the protection of securities of participants and those of their clients, settlement finality, participant default and transfer of participants and clients' assets in case of a withdrawal of authorisation.

(17) The risk management models associated with the services provided by an applicant CSD are a necessary item in its application for authorisation so as to enable the competent authority to evaluate the reliability and integrity of the adopted procedures and help market participants make an informed choice.

(18) In order to verify the safety of the link arrangements of the CSD applying for authorisation, to assess the rules applied in the linked systems and evaluate the risks stemming from those links, the competent authority should receive from an applicant CSD any relevant information for the analysis, together with the CSD assessment of the link arrangements.

(19) When granting the approval of a CSD's participation in the capital of another entity, the competent authority of the CSD should take into consideration the criteria that ensure that the participation does not increase significantly the CSD's risk profile. In order to ensure its safety and continuity of its services, a CSD should not assume unlimited financial liabilities as a result of its participation in the capital of legal persons other than those providing the services set out in Regulation (EU) No 909/2014. A CSD should fully capitalise the risks resulting from any participation in the capital of another entity.

(20) In order for a CSD not to be dependent on other shareholders of the entities in which it holds a participation, including with regard to the risk management policies, it should have full control of those entities. This requirement should also facilitate the exercise of supervisory and oversight functions by competent authorities and relevant authorities by allowing easy access to relevant information.

(21) A CSD should have a clear strategic rationale for the participation beyond mere profit making, taking into account the interests of the issuers of securities issued with the CSD; its participants and its clients.

(22) In order to properly quantify and outline the risks stemming from its participation in the capital of another legal person, a CSD should provide independent risk analyses, approved by an internal or external auditor, for the financial risks and liabilities of the CSD resulting from that participation.

(23) Following the experience of the financial crisis, authorities should focus on ongoing rather than ex-post supervision. It is, therefore, necessary to ensure that for each review and evaluation under Regulation (EU) No 909/2014, the competent authority has sufficient access to information on a continuous basis. In order to determine the

scope of information to be delivered for each review and evaluation, the provisions of this Regulation should follow the requirements for authorisation with which a CSD has to comply under Regulation (EU) No 909/2014. This includes substantive changes to elements already submitted during the process of authorisation, information relating to periodic events and statistical data.

(24) To promote an effective bilateral and multilateral exchange of information between competent authorities, the results of the review and evaluation by one authority of the activities of a CSD should be shared with other competent authorities where this information is likely to facilitate their tasks, without prejudice to confidentiality and data protection requirements and in addition to any cooperation arrangements provided in Regulation (EU) No 909/2014. An additional exchange of information among competent authorities and relevant authorities or authorities in charge of markets in financial instruments should be organised allowing for a sharing of the findings of the competent authority in the course of the process of review and evaluation.

(25) Taking into account the possible burden of gathering and processing a vast amount of information related to the operation of a CSD, and in order to avoid duplications, only relevant modified documents should be provided in the context of the review and evaluation. Those documents should be delivered in a manner that enables the competent authority to identify all the relevant changes made to the arrangements, strategies, processes and mechanisms implemented by the CSD since authorisation or since the completion of the last review and evaluation.

(26) Another category of information that is useful for the competent authority to have in order to be able to perform the review and evaluation refers to events that by nature occur on a periodic basis and which are related to the operation of the CSD and the provision of its services.

(27) To carry out a comprehensive risk evaluation of a CSD, the competent authority will need to request statistical data on the scope of the CSD's business activities in order to evaluate the risks related to CSDs operation and to the smooth operation of securities markets. In addition, statistical data enable the competent authority to monitor the size and importance of securities transactions and settlements within the financial markets as well as to assess the ongoing and potential impact of a given CSD on the securities market as a whole.

(28) For the competent authority to monitor and evaluate the risks to which the CSD is or may be exposed to and which may arise for the smooth functioning of securities markets, it should be able to request additional information on the risks and activities of a CSD. The competent authority should therefore be able to define and request on its own initiative, or following a request submitted to it by another authority, any additional information which it considers necessary for each review and evaluation of the activities of a CSD.

(29) It is important to ensure that third-country CSDs that intend to provide the services pursuant to Regulation (EU) No 909/2014 do not disrupt the orderly functioning of Union markets.

(30) The ongoing assessment of the full compliance of a third-country CSD with the prudential requirements of a third country is the duty of the third country competent authority. The information to be provided to the European Securities and Markets Authority (ESMA) by an applicant CSD should not have the objective of replicating the assessment of the third country competent authority, but ensuring that the applicant

is subject to effective supervision and enforcement in that third country, thus guaranteeing a high degree of investor protection.

(31) To allow ESMA to perform a complete assessment of the application for recognition, the information provided by the applicant should be complemented by the necessary information to assess the effectiveness of the ongoing supervision, enforcement powers and actions taken by the third country competent authority. That information should be provided under a cooperation arrangement established in accordance with Regulation (EU) No 909/2014. The cooperation arrangement should ensure that ESMA is informed in a timely manner of any supervisory or enforcement action against the third-country CSD applying for recognition and any change of the conditions under which authorisation was granted to the relevant CSD and on any relevant update of the information originally provided by the CSD under the recognition process.

(32) In order to ensure that investors' rights are protected, and that conflict of laws issues are adequately managed, when assessing the measures that a third-country CSD intends to take to allow its users to comply with the national laws referred to in Article 49(1) of Regulation (EU) No 909/2014, that third-country CSD should take into account both issuers and participants, as appropriate, in accordance with the respective national laws referred to in Article 49(1) of that Regulation.

(33) To establish a sound risk-management framework, a CSD should take an integrated and comprehensive view of all relevant risks. This should include the risks that the CSD bears from any other entities and the risks that it poses to third parties, including its users and to the extent practicable their clients, as well as linked CSDs, central counterparties, trading venues, payment systems, settlement banks, liquidity providers and investors.

(34) To ensure that CSDs operate with the necessary level of human resources to meet all of their obligations and to ensure that competent authorities have the relevant contact points within the CSDs that they supervise, CSDs should have key dedicated staff that should be accountable for the CSD and their own individual performance, particularly at the level of senior management and management body.

(35) To ensure an adequate control of the activities performed by CSDs, independent audits covering the operations of the CSD, risk management processes, compliance and internal control mechanisms should be put in place and performed regularly. The independence of audits should not necessarily require the involvement of an external auditor, provided that the CSD demonstrates to the competent authority that the independence of its internal auditor is properly ensured. In order to ensure the independence of its internal audit function, the CSD should also establish an audit committee.

(36) A CSD should set up a risk committee in order to ensure that the management body of the CSD is advised at the highest technical level on its overall current and future risk tolerance and strategy. To ensure its independence from the CSD's executive management and a high degree of competence, the risk committee should be composed of a majority of non-executive members and it should be chaired by a person with an appropriate experience on risk management.

(37) When assessing potential conflicts of interest, a CSD should not only examine the members of the management body, senior management or staff of the CSD but also

any person directly or indirectly linked to those individuals or to the CSD, whether it is a natural or legal person.

(38) A CSD should have a chief risk officer, a chief compliance officer, a chief technology officer, as well as a risk management function, a technology function, a compliance and internal control function, and internal audit function. A CSD should in any case be able to organise the internal structure of those functions according to its needs. Different persons should fulfil the roles of chief risk officer, chief compliance officer and chief technology officer given that those functions are usually fulfilled by persons with different academic and professional profiles. In this respect, the provisions set out in this Regulation closely follow the system established by Regulation (EU) No 648/2012 of the European Parliament and the Council[4] for other market infrastructures.

(39) Records kept by a CSD should be structured and allow for easy access to the data stored by the competent authorities involved in the supervision of CSDs. A CSD should ensure that the data records it keeps, including the complete accounting of the securities it maintains, are accurate and up-to-date in order to serve as a reliable data source for supervision purposes.

(40) To facilitate the reporting and recording of a consistent set of information under different requirements, records kept by CSDs should cover each individual service provided by the CSD in accordance with Regulation (EU) No 909/2014, and should include at least all the details to be reported under the rules on settlement discipline provided in that Regulation.

(41) The preservation of the rights of issuers and investors is essential for the orderly functioning of a securities market. A CSD should therefore employ appropriate rules, procedures and controls to prevent the unauthorised creation or deletion of securities. It should also conduct at least daily reconciliation of the securities accounts that it maintains.

(42) A CSD should maintain robust accounting practices and perform audits to verify that its records of securities are accurate and that its measures ensuring the integrity of securities issues are adequate.

(43) In order to effectively ensure the integrity of the issue, the reconciliation measures provided in Regulation (EU) No 909/2014 should apply to all CSDs regardless of whether or not they provide the notary service or central maintenance service referred to in that Regulation in relation to a securities issue.

(44) With regard to other entities involved in the reconciliation process, several scenarios should be distinguished depending on the role of those entities. The reconciliation measures should reflect the specific roles of those entities. According to the registrar model, the registrar maintains records of securities which are also recorded in a CSD. According to the transfer agent model, the fund manager or transfer agent is responsible for an account that maintains a part of a securities issue recorded in a CSD. According to the common depository model, the common depository is used by CSDs that establish an interoperable link and the common depository should be responsible for the overall integrity of the securities issues initially recorded or centrally maintained by the CSDs that have established an interoperable link.

[4] Regulation (EU) No 648/2012 of the European Parliament and the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories, OJ, 27.7.2012, L201/1

(45) In order to mitigate operational risks, which comprise the risks caused by deficiencies in information systems, internal processes, and personnel performance or disruptions caused by external events which result in the reduction, deterioration or breakdown of services provided by a CSD, CSDs should identify all risks and monitor their evolution, irrespective of their origin that may include, for instance, their users, providers of services to CSDs and other market infrastructures, including other CSDs. Operational risks should be managed in accordance to a well-documented and robust framework with clearly assigned roles and responsibilities. That framework should include operational targets, tracing features, assessment mechanisms and it should be integrated in the risk management system of the CSD. In this context, a CSD chief risk officer should be responsible for the operational risk management framework. CSDs should manage their risk internally. Where internal controls are insufficient or where eliminating certain risks is not a reasonably feasible option, a CSD should be able to take a financial coverage of those risks through insurance.

(46) CSDs should not enter into investments that may affect their risk profile. CSDs should only enter into derivatives contracts if they are required to hedge a risk that they cannot reduce otherwise. The hedging should be subject to certain strict conditions that ensure that the derivatives are not used for purposes other than for covering risks and are not used for a realisation of profits.

(47) The assets of CSDs should be held safely, be easily accessible and able to be liquidated promptly. A CSD should therefore ensure that its policies and procedures concerning prompt access to its own assets are based at least on the nature, size, quality, maturity and location of the assets. A CSD should also ensure that prompt access to its assets is not negatively affected by the outsourcing of custody or investment functions to a third party entity.

(48) To manage its liquidity needs, a CSD should be able to access its cash assets immediately and also be able to access any securities that it holds under its own name on the same business day when a decision to liquidate the assets is taken.

(49) To ensure a greater degree of protection of the assets of a CSD from the default of the intermediary, a CSD that accesses another CSD through a CSD link should maintain those assets in a segregated account at the linked CSD. This level of segregation should ensure that the assets of a CSD are segregated from those of other entities and protected appropriately. It is however necessary to allow the establishment of links with third-country CSDs even where individually segregated accounts are not available at the third-country CSD provided that assets of the requesting CSD are in any case adequately protected and competent authorities are informed of the risks resulting from the unavailability of individually segregated accounts and the adequate mitigation of such risks.

(50) In order to ensure that a CSD invests its financial resources in highly liquid instruments with minimal market and credit risks and for these investments to be liquidated rapidly with minimal price effect, it should diversify its portfolio and establish appropriate concentration limits with respect to the issuers of the instruments in which it invests its resources.

(51) In order to ensure the safety and efficiency of the link arrangement of a CSD with another CSD, a CSD should identify, monitor, and manage all potential sources of risk arising from the link arrangement. A CSD link should have a well-founded legal basis, in all relevant jurisdictions, that supports its design and provides adequate protection

to the CSDs involved in the link. Linked CSDs should measure, monitor, and manage the credit and liquidity risks arising from each other.

(52) A requesting CSD that uses an indirect CSD link or an intermediary to operate a CSD link with a receiving CSD should measure, monitor, and manage the additional risks, including custody, credit, legal, and operational risks, arising from the use of the intermediary in order to ensure the safety and the efficiency of the link arrangement.

(53) In order to ensure the integrity of the issue, where securities are maintained in several CSDs through CSD links, CSDs should apply specific reconciliation measures and coordinate their actions.

(54) CSDs should provide fair and open access to their services with due regard to the risks to financial stability and the orderliness of the market. They should control the risks arising from their participants and other users by setting risk-related criteria for the provision of their services. CSDs should ensure that their users, such as participants, any other CSDs, central counterparties (CCPs), trading venues or issuers that are granted access to their services meet the criteria and have the required operational capacity, financial resources, legal powers, and risk-management expertise in order to prevent the occurrence of risks for CSDs and other users.

(55) In order to ensure the safety and efficiency of its securities settlement system, a CSD should monitor compliance with its access requirements on an ongoing basis and have clearly defined and publicly disclosed procedures for facilitating the suspension and orderly exit of a requesting party that breaches, or no longer meets, the access requirements.

(56) For the purpose of the authorisation to provide banking-type ancillary services, a CSD should submit an application to the competent authority including all necessary elements to ensure that the provision of the banking-type ancillary services do not affect the smooth provision of core services of a CSD. Entities already authorised as CSDs should not be required to submit again any elements that were already submitted in the course of the process of application for being authorised as a CSD under Regulation (EU) 909/2014.

(57) With a view to ensuring legal certainty and a consistent application of the law, certain requirements provided for in this Regulation concerning settlement discipline measures should start to apply from the date of entry into force of those measures.

(58) This Regulation is based on the draft regulatory technical standards submitted by ESMA to the Commission.

(59) In drawing up the technical standards contained in this Regulation, ESMA has worked in close cooperation with the members of the European System of Central Banks and the European Banking Authority.

(60) ESMA has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the opinion of the Securities and Markets Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1095/2010 of the European Parliament and of the Council[5],

[5] Regulation (EU) No 1095/2010 of 24 November 2010 of the European Parliament and of the Council establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC (OJ L 331, 15.12.2010, p. 84).

HAS ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Definitions

For the purposes of this Regulation, the following definitions apply:

(a) 'review period' means the period under review beginning on the day following the end of the previous review and evaluation period;

(b) 'settlement instruction' means a transfer order as defined in point (i) of Article 2 of Directive 98/26/EC of the European Parliament and of the Council[6];

(c) 'settlement restriction' means the blocking, reservation or earmarking of securities that make them unavailable for settlement, or the blocking or reservation of cash that make it unavailable for settlement;

(d) 'exchange-traded fund' (ETF) means a fund as defined in point (46) of Article 4(1) of Directive 2014/65/EU[7];

(e) 'issuer CSD' means a CSD which provides the core service referred to in point 1 or 2 of Section A of the Annex to Regulation (EU) No 909/2014 in relation to a securities issue;

(f) 'investor CSD' means a CSD that either is a participant in the securities settlement system operated by another CSD or that uses a third party or an intermediary that is a participant in the securities settlement system operated by another CSD in relation to a securities issue;

(g) 'durable medium' means any instrument which enables the storage of information in a way that is accessible for future reference for a period of time adequate for the purposes of the information, and allows the unchanged reproduction of the information stored.

CHAPTER II

DETERMINATION OF THE MOST RELEVANT CURRENCIES AND PRACTICAL ARRANGEMENTS FOR THE CONSULTATION OF THE RELEVANT COMPETENT AUTHORITIES

(Article 12(1)(b) and (c) of Regulation (EU) No 909/2014)

[6] Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems (OJ L 166, 11.06.1998, p. 45).

[7] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

Article 2

Determination of most relevant currencies

1. The most relevant currencies referred to in point (b) of Article 12(1) of Regulation (EU) No 909/2014 shall be identified according to either of the following calculations:

   (a) the relative share of each Union currency in the total value of the settlement by a CSD of settlement instructions against payment, calculated over a period of one year, provided that each individual share exceeds 1%;

   (b) the relative share of settlement instructions against payment settled by a CSD in a Union currency compared to the total value of settlement instructions against payment settled in that currency across all CSDs in the Union, calculated over a period of one year, provided that each individual share exceeds 10%.

2. The calculations referred to in paragraph 1 shall be done on an annual basis by the competent authority of each CSD.

Article 3

Practical arrangements for the consultation of the relevant authorities referred to in Article 12(1)(b) and (c) of Regulation (EU) No 909/2014

1. Where one of the most relevant currencies determined in accordance with Article 2 of this Regulation is issued by more than one central bank, those central banks shall determine a single representative as the relevant authority for that currency referred to in point (b) of Article 12(1) of Regulation (EU) No 909/2014.

2. Where the cash leg of securities transactions is settled in accordance with Article 40(1) of Regulation (EU) No 909/2014 through accounts opened with several central banks that issue the same currency, those central banks shall determine a single representative as a relevant authority referred to in point (c) of Article 12(1) of that Regulation.

CHAPTER III

AUTHORISATION OF CSDs

(Article 17 of Regulation No 909/2014)

SECTION 1

General information on applicant CSDs

Article 4

Identification and legal status of applicant CSDs

1. An application for authorisation shall clearly identify the applicant CSD and the activities and services that it intends to carry out.

2. The application for authorisation shall include the following information:

   (a) contact details of the person responsible for the application;

(b) contact details of the person or persons in charge of the applicant CSD's compliance and internal control function;

(c) the corporate name of the applicant CSD, its Legal Entity Identifier (LEI) and registered address in the Union;

(d) the memorandum and articles of association or other constitutional and statutory documentation of the applicant CSD;

(e) an excerpt from the relevant commercial or court register, or other forms of certified evidence of the registered address and business activity of the applicant CSD that is valid at the date of the application;

(f) the identification of the securities settlement systems that the applicant CSD operates or intends to operate;

(g) a copy of the decision of the management body regarding the application and the minutes of the meeting in which the management body approved the application file and its submission;

(h) a chart showing the ownership links between the parent undertaking, subsidiaries and any other associated entities or branches, wherein the entities shown in the chart are identified by their full corporate name, legal status, registered address, and tax numbers or company registration numbers;

(i) a description of the business activities of the applicant CSD's subsidiaries and other legal persons in which the applicant CSD holds a participation, including information on the level of participation;

(j) a list including:

  (i) the name of each person or entity who, directly or indirectly, holds 5 % or more of the applicant CSD's capital or voting rights;

  (ii) the name of each person or entity that could exercise a significant influence over the applicant CSD's management due to its holding in the applicant CSD's capital;

(k) a list including:

  (i) the name of each entity in which the applicant CSD holds 5 % or more of the entity's capital and voting rights;

  (ii) the name of each entity over whose management the applicant CSD exercises significant influence;

(l) a list of core services listed in Section A of the Annex to Regulation (EU) No 909/2014 that the applicant CSD is providing or intends to provide;

(m) a list of ancillary services explicitly specified in Section B of the Annex to Regulation (EU) No 909/2014 that the applicant CSD is providing or intends to provide;

(n) a list of any other ancillary services permitted under, but not explicitly specified under Section B of the Annex to Regulation (EU) No 909/2014 that the applicant CSD is providing or intends to provide;

(o) a list of the investment services subject to Directive 2014/65/EU of the European Parliament and of the Council referred to in point (n);

(p) a list of services and activities that the applicant CSD outsources or intends to outsource to a third party in accordance with Article 30 of Regulation (EU) No 909/2014;

(q) the currency or currencies that the applicant CSD processes, or intends to process in connection with services that the applicant CSD provides, irrespective of whether cash is settled on a central bank account, a CSD account, or an account at a designated credit institution;

(r) information on any pending and final judicial, administrative, arbitration or any other legal proceedings to which the applicant CSD is a party and which may cause it financial or other costs.

3. Where the applicant CSD intends to provide core services or to set up a branch in accordance with Article 23(2) of Regulation (EU) No 909/2014, the application for authorisation shall also include the following information:

(a) the Member State or Member States in which the applicant CSD intends to operate;

(b) a programme of operations stating in particular the services which the applicant CSD provides or intends to provide in the host Member State;

(c) the currency or currencies that the applicant CSD processes or intends to process in the host Member State;

(d) where the services are provided or intended to be provided through a branch, the organisational structure of the branch and the names of the persons responsible for its management;

(e) where relevant, an assessment of the measures that the applicant CSD intends to take to allow its users to comply with the national laws referred to in Article 49(1) of Regulation (EU) No 909/2014.

Article 5

General information concerning policies and procedures

1. An application for authorisation shall specify the following information on the policies and procedures of the applicant CSD referred to in this Chapter:

(a) the job titles of the persons responsible for the approval and implementation of the policies and procedures;

(b) a description of the measures implementing and monitoring the compliance with the policies and procedures.

2. An application for authorisation shall include a description of the procedures put in place by the applicant CSD pursuant to Article 65(3) of Regulation (EU) No 909/2014.

Article 6

Information concerning services and activities of the CSD

The applicant CSD shall include the following in the application for authorisation:

(a) a detailed description of the services referred to in points (l) to (p) of Article 4(2);

(b) the procedures to be applied in the provision of the services referred to in point (a).

Article 7

Information concerning groups

1. Where the applicant CSD is part of a group of undertakings that includes other CSDs or credit institutions referred to in point (b) of Article 54(2) of Regulation (EU) No 909/2014, the application for authorisation shall include the following:

   (a) the policies and procedures referred to in Article 26(7) of Regulation (EU) No 909/2014;

   (b) information on the composition of the senior management, the management body, and the shareholders structure of the parent undertaking and of the other undertakings in the group;

   (c) the services and key individuals other than senior management that the applicant CSD shares with other undertakings in the group.

2. Where the applicant CSD has a parent undertaking, the application for authorisation shall provide the following information:

   (a) the registered address of the parent undertaking of the applicant CSD;

   (b) where the parent undertaking is an entity authorised or registered and subject to supervision under Union or third country legislation, any relevant authorisation or registration number and the name of the authority or authorities competent for the supervision of the parent undertaking.

3. Where the applicant CSD has outsourced services or activities to an undertaking within the group in accordance with Article 30 of Regulation (EU) No 909/2014, the application shall include a summary and a copy of the outsourcing agreement.

SECTION 2

Financial resources for the provision of services by the applicant CSD

Article 8

Financial reports, business plan, and recovery plan

1. An application for authorisation shall include the following financial and business information to enable the competent authority to assess compliance of the applicant CSD with Articles 44, 46 and 47 of Regulation (EU) No 909/2014:

   (a) financial reports including a complete set of financial statements for the preceding three years, and the statutory audit report on the annual and consolidated financial statements within the meaning of Directive 2006/43/EC of the European Parliament and of the Council[8], for the preceding three years;

[8] Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87).

(b) where the applicant CSD is audited by an external auditor, the name and the national registration number of the external auditor;

(c) a business plan, including a financial plan and an estimated budget that foresees various business scenarios for the services provided by the applicant CSD, over a reference period of at least three years;

(d) any plan for the establishment of subsidiaries and branches and their location;

(e) a description of the business activities that the applicant CSD plans to carry out, including the business activities of any subsidiaries or branches of the applicant CSD.

2. Where historical financial information referred to in point (a) of paragraph 1 is not available, an application for authorisation shall include the following information about the applicant CSD:

(a) evidence that demonstrates sufficient financial resources during six months after the granting of an authorisation;

(b) an interim financial report;

(c) statements concerning the financial situation of the applicant CSD, including a balance sheet, income statement, changes in equity and in cash flows and a summary of accounting policies and other relevant explanatory notes;

(d) audited annual financial statements of any parent undertaking for the three financial years preceding the date of the application.

3. The application shall include a description of an adequate recovery plan to ensure continuity of the applicant CSD's critical operations referred to in Article 22(2) of Regulation (EC) No 909/2014 including:

(a) a summary that provides an overview of the plan and its implementation;

(b) the identification of the critical operations of the applicant CSD, stress scenarios and events triggering recovery, and a description of recovery tools to be used by the applicant CSD;

(c) an assessment of any impact of the recovery plan on stakeholders that are likely to be affected by its implementation;

(d) an assessment of the legal enforceability of the recovery plan that takes account of any legal constraints imposed by Union, national or third country legislation.

SECTION 3

Organisational requirements

Article 9

Organisational chart

An application for authorisation shall include an organisational chart that describes the organisational structure of the applicant CSD. The chart shall include the following:

(a) the identity and tasks of the persons responsible for the following positions:

(i) senior management;

(ii) managers in charge of the operational functions referred to in Article 47(3);

(iii) managers in charge of the activities of any branches of the applicant CSD;

(iv) other significant roles in the operations of the applicant CSD;

(b) the number of staff members in each division and operational unit.

Article 10

Staffing policies and procedures

An application for authorisation shall include the following information on the applicant CSD's policies and procedures related to staff:

(a) a description of the remuneration policy including information about the fixed and variable elements of the remuneration of the senior management, the members of the management body and the staff employed in the risk management, compliance and internal control, internal audit and technology functions of the applicant CSD;

(b) the measures put in place by the applicant CSD to mitigate the risk of over-reliance on the responsibilities entrusted to any individual person.

Article 11

Risk monitoring tools and governance arrangements

1. An application for authorisation shall include the following information on the governance arrangements and risk monitoring tools of the applicant CSD:

(a) a description of the governance arrangements of the applicant CSD established in accordance with paragraph 2 of Article 47;

(b) the policies, procedures and systems established in accordance with paragraph 1 of Article 47;

(c) a description of the composition, role and responsibilities of the members of the management body and senior management and the committees established in accordance with Article 48.

2. The information referred to in paragraph 1 shall include a description of the processes concerning the selection, appointment, performance evaluation and removal of senior management and members of the management body.

3. The applicant CSD shall describe its procedure to make its governance arrangements and the rules governing its activity available to the public.

4. Where the applicant CSD adheres to a recognised corporate governance code of conduct, the application shall identify any code, include a copy of that code and justify any situations where the applicant CSD deviates from the code.

Article 12

Compliance, internal control and internal audit functions

1. An application for authorisation shall include a description of the procedures for the applicant CSD's internal reporting of infringements referred to in Article 26(5) of Regulation (EU) No 909/2014.

2. An application for authorisation shall include information regarding an applicant CSD's internal audit policies and procedures referred to in Article 51, including:

   (a) a description of the monitoring and evaluation tools for the adequacy and effectiveness of the applicant CSD's internal audit systems;

   (b) a description of the control and safeguard tools for the applicant CSD's information processing systems;

   (c) a description of the development and application of the applicant CSD's internal audit methodology;

   (d) a work plan of the internal audit function for three years following the date of application;

   (e) a description of the roles and qualifications of each individual who is responsible for internal audit referred to in Article 47(3)(d) under the oversight of the audit committee referred to in Article 48(1)(b).

3. An application for authorisation shall include the following information concerning the compliance and internal control function of the applicant CSD's referred to in Article 47(3)(c):

   (a) a description of the roles and qualifications of individuals who are responsible for the compliance and internal control function and of any other staff involved in the assessments of compliance, including a description of the means to ensure the independence of the compliance and internal control function from the rest of the business units;

   (b) the policies and procedures of the compliance and internal control function, including a description of the compliance role of the management body and senior management;

   (c) where available, the most recent internal report prepared by the persons responsible for the compliance and internal control function or by any other staff involved in the assessments of compliance within the applicant CSD.

Article 13

Senior management, management body and shareholders

1. An application for authorisation shall include, for each member of the senior management and each member of the management body of the applicant CSD, the following information to enable the competent authority to assess compliance of the applicant CSD with Article 27(1) and (4) of Regulation (EU) No 909/2014:

   (a) a copy of a curriculum vitae which sets out the experience and knowledge of each member;

   (b) details regarding any criminal and administrative sanctions imposed on a member in connection with the provision of financial or data services or in relation to acts of fraud or misappropriation of funds, in the form of an appropriate official certificate where available in the relevant Member State;

(c) a self-declaration of good repute in relation to the provision of financial or data services, where all members of the senior management and management body shall state whether they have been subject to any of the following:

(i) they have been convicted of any criminal or administrative offence in connection with the provision of financial or data services or in relation to acts of fraud or misappropriation of funds;

(ii) they have been subject to an adverse decision in any proceedings of a disciplinary nature brought by a regulatory authority, a government body or agency or they are subject to any ongoing proceedings;

(iii) they have been subject to an adverse judicial finding in civil proceedings before a court in connection with the provision of financial or data services, or fraud in the management of a business;

(iv) they have been members of the management body or senior management of an undertaking whose registration or authorisation was withdrawn by a regulatory body while connected to the undertaking at least one year before the date of withdrawal of authorisation or registration;

(v) they have been refused the right to carry on any type of activities which require registration or authorisation by a regulatory body;

(vi) they have been members of the management body or of senior management of an undertaking against whom insolvency proceedings have been opened at least one year before proceedings have been opened;

(vii) they have been members of the management body or the senior management of an undertaking that was subject to a sanction by a regulatory body while they were connected to the undertaking at least one year before such a sanction was imposed;

(viii) they have been otherwise fined, suspended, disqualified or subject to any other sanction in connection with the provision of financial or data services by a government, regulatory or professional body;

(ix) they have been disqualified from acting as a director or in any other managerial capacity, dismissed from employment or other appointment in an undertaking as a result of misconduct or malpractice.

For the purposes of point (c)(i) of this paragraph, the self-declaration shall not be required where an official certificate is submitted under point (b) of this paragraph.

2. The application for authorisation shall include the following information regarding the management body of the applicant CSD:

(a) evidence of compliance with Article 27(2) of Regulation (EU) No 909/2014;

(b) a description of the roles and responsibilities of the members of the management body;

(c) the target for the representation of the underrepresented gender in the management body, the relevant policy on how to meet that target and the method used by the applicant CSD to make public the target, policy and its implementation.

3. The application for authorisation shall include the following information concerning the ownership structure and shareholders of the applicant CSD:

(a) a description of the ownership structure of the applicant CSD referred to in point (i) of Article 4(2), including a description of the identity and size of interests of any entity in a position to exercise control over the operation of the applicant CSD;

(b) a list of the shareholders and persons who are in a position to exercise, directly or indirectly, control over the management of the applicant CSD.

Article 14

Management of conflicts of interest

1. An application for authorisation shall include the following information on the policies and procedures put in place to identify and manage potential conflicts of interest by the applicant CSD in accordance with Article 50:

(a) a description of the policies and procedures concerning the identification, management and disclosure to the competent authority of potential conflicts of interest and of the process used to ensure that the staff of the applicant CSD is informed of those policies and procedures;

(b) a description of the controls and measures put in place to ensure that the requirements referred to in point (a) on the management of conflicts of interest are met;

(c) a description of the following elements:

(i) the roles and responsibilities of key personnel, especially where they also have responsibilities in other entities;

(ii) arrangements ensuring that individuals who have a permanent conflict of interest are excluded from the decision making process and from the receipt of any relevant information concerning the matters affected by the permanent conflict of interest;

(iii) an up-to-date register of existing conflicts of interest at the time of the application and a description of how those conflicts of interest are managed.

2. Where the applicant CSD is part of a group, the register referred to in point (c)(iii) of paragraph 1 shall include a description of the conflicts of interest arising from other undertakings within the group in relation to any service provided by the applicant CSD, and the arrangements put in place to manage those conflicts of interest.

Article 15

Confidentiality

1. An application for authorisation shall include the applicant CSD's policies and procedures put in place for preventing the unauthorised use or disclosure of confidential information. Confidential information shall include the following information:

(a) information relating to participants, clients, issuers or other users of the applicant CSD services;

(b) other information held by the applicant CSD as a result of its business activity not permitted to be used for commercial purposes.

2. An application for authorisation shall include the following information concerning the access of staff to information held by the applicant CSD:

(a) the internal procedures concerning permissions of access to information that ensure secured access to data;

(b) a description of any restrictions on the use of data for reasons of confidentiality.

Article 16

User committee

An application for authorisation shall include the following information on each user committee:

(a) the mandate of the user committee;

(b) the governance arrangements of the user committee;

(c) the operating procedures of the user committee;

(d) the admission criteria and the election mechanism for the members of the user committee;

(e) a list of the proposed members of the user committee and the indication of interests that they represent.

Article 17

Record keeping

1. An application for authorisation shall include a description of the record-keeping systems, policies and procedures of the applicant CSD, established and maintained in accordance with Chapter VIII of this Regulation.

2. Where an applicant CSD applies for authorisation before the date of application of Article 54, the application for authorisation shall contain the following information:

(a) an analysis of the extent to which the applicant CSD's existing record-keeping systems, policies and procedures are compliant with the requirements under Article 54;

(b) an implementation plan detailing how the applicant CSD will comply with the requirements referred to in Article 54 by the date on which it becomes applicable.

SECTION 4

Conduct of business rules

Article 18

Goals and objectives

An application for authorisation shall include a description of the goals and objectives of the applicant CSD referred to in Article 32(1) of Regulation (EU) No 909/2014.

Article 19

Handling of complaints

An application for authorisation shall include the procedures the applicant CSD has established for the handling of complaints.

Article 20

Requirements for participation

An application for authorisation shall include all necessary information concerning the participation in the securities settlement systems operated by the applicant CSD in accordance with Article 33 of Regulation (EU) No 909/2014 and Articles 88-90 of this Regulation. That information shall include the following:

(a) the criteria for participation that allow fair and open access for all legal persons that intend to become participants in the securities settlement systems operated by the applicant CSD;

(b) the procedures for the application of disciplinary measures against existing participants that do not comply with the criteria for participation.

Article 21

Transparency

1. An application for authorisation shall include the documents and information on the pricing policy of the applicant CSD concerning services referred to in Article 34 of Regulation (EU) No 909/2014. That information shall include in particular the prices and fees for each core service provided by the applicant CSD and any existing discounts and rebates, as well as the conditions for the reductions.

2. The applicant CSD shall provide the competent authority with a description of methods used to disclose the relevant information in accordance with paragraphs (1), (2), (4) and (5) of Article 34 of Regulation (EU) No 909/2014.

3. An application for authorisation shall include information allowing the competent authority to assess how the applicant CSD intends to comply with the requirements to account separately for costs and revenues in accordance with Article 34(6) and (7) of Regulation (EU) No 909/2014.

Article 22

Communication procedures with participants and other market infrastructures

An application for authorisation shall include the relevant information concerning the use by the applicant CSD of international open communication procedures and standards for messaging and reference data in its communication procedures with participants and other market infrastructures.

SECTION 5

Requirements for services provided by CSDs

Article 23

Book-entry form

An application for authorisation shall include information on the processes concerning book entries that ensure the compliance of the applicant CSD with Article 3 of Regulation (EU) No 909/2014.

Article 24

Intended settlement dates and measures for preventing and addressing settlement fails

1. An application for authorisation shall include the following information in respect of the applicant CSD:

   (a) the procedures and measures to prevent settlement fails in accordance with Article 6 of Regulation (EU) No 909/2014;

   (b) the measures to address settlement fails in accordance with Articles 7 of Regulation (EU) No 909/2014.

2. Where an applicant CSD applies for authorisation before Articles 6 and 7 of Regulation (EU) No 909/2014 are applicable in accordance with paragraphs (4) and (5) of Article 76 of that Regulation, the application for authorisation shall contain an implementation plan detailing how the applicant CSD will comply with the requirements under Articles 6 and 7 of Regulation (EU) No 909/2014.

   Institutions referred to in Article 69(1) of Regulation (EU) No 909/2014 shall include in the implementation plan referred to in the first subparagraph an analysis of the extent to which their existing rules, procedures, mechanisms and measures comply with the requirements under Articles 6 and 7 of Regulation (EU) No 909/2014.

Article 25

Integrity of the issue

An application for authorisation shall include information concerning the applicant CSD's rules and procedures for ensuring the integrity of securities issues referred to in Article 37 of Regulation (EU) No 909/2014 and Chapter IX of this Regulation.

Article 26

Protection of participants' and their clients' securities

An application for authorisation shall include the following information concerning the measures put in place to protect the securities of the applicant CSD's participants and those of their clients in accordance with Article 38 of Regulation (EU) No 909/2014:

   (a) the rules and procedures to reduce and manage the risks associated with the safekeeping of securities;

   (b) a detailed description of the different levels of segregation offered by the applicant CSD, a description of the costs associated with each level, the commercial terms on which they are offered, their main legal implications and the applicable insolvency law;

   (c) the rules and procedures for obtaining the consents referred to in Article 38(7) of Regulation (EU) No 909/2014.

Article 27

Settlement finality

An application for authorisation shall contain information concerning the rules on settlement finality put in place by the applicant CSD in accordance with Article 39 of Regulation (EU) No 909/2014.

Article 28

Cash settlement

1. An application for authorisation shall include the procedures for the settlement of the cash payments for each securities settlement system that the applicant CSD operates in accordance with Article 40 of Regulation (EU) No 909/2014.

2. The applicant CSD shall provide information about whether the settlement of the cash payments is provided in accordance with Article 40(1) or (2) of Regulation (EU) No 909/2015.

If the settlement of the cash payments is intended to take place in accordance with Article 40(2) of Regulation (EU) No 909/2014, the applicant CSD shall explain why settlement in accordance with Article 40(1) of Regulation (EU) No 909/2014 is not practical and available.

Article 29

Participant default rules and procedures

An application for authorisation shall include the rules and procedures put in place by the applicant CSD to manage the default of a participant.

Article 30

Transfer of participants and clients' assets in case of a withdrawal of authorisation

An application for authorisation shall include information concerning the procedures put in place by the applicant CSD to ensure the timely and orderly settlement and transfer of the assets of clients and participants to another CSD in the event of a withdrawal of its authorisation.

SECTION 6

Prudential requirements

Article 31

Legal risks

1. An application for authorisation shall include all information necessary to enable the competent authority to assess that the rules, procedures, and contracts of the applicant CSD are clear, understandable and enforceable in all relevant jurisdictions in accordance with Article 43(1) and (2) of Regulation (EU) No 909/2014.

2. Where the applicant CSD intends to conduct business in different jurisdictions, the applicant CSD shall provide the competent authority with information concerning the measures put in place to identify and mitigate the risks arising from potential conflicts of laws across jurisdictions in accordance with Article 43(3) of Regulation (EU) No 909/2014. That information shall include any legal assessment on which those measures are based.

Article 32

General business risks

1. The applicant CSD shall provide the competent authority with a description of the risk management and control systems as well as the IT tools put in place by the applicant CSD to manage business risks in accordance with Article 44 of Regulation (EU) No 909/2014.

2. Where the applicant CSD has obtained a risk rating from a third party, it shall provide it to the competent authority including any relevant information supporting that risk rating.

Article 33

Operational risks

1. An application for authorisation shall include information that demonstrates the applicant CSD is compliant with the requirements for the management of operational risks in accordance with Article 45 of Regulation (EU) No 909/2014 and Chapter X of this Regulation.

2. An application for authorisation shall also contain the following information concerning the list of services referred to in point (p) of Article 4(2) of this Regulation:

   (a) a copy of the outsourcing agreements;

   (b) the methods used to monitor the service level of the outsourced services and activities.

Article 34

Investment policy

An application for authorisation shall include evidence demonstrating that:

   (a) the applicant CSD holds its financial assets in accordance with Article 46(1), (2) and (5) of Regulation (EU) No 909/2014 and Chapter XI of this Regulation.

   (b) the investments of the applicant CSD are compliant with Article 46(3) of Regulation (EU) No 909/2014 and Chapter XI of this Regulation.

Article 35

Capital requirements

An application for authorisation shall include the following information concerning the capital requirements:

(a) information demonstrating that the capital of the applicant CSD, including retained earnings and reserves of the applicant CSD, meets the requirements of Article 47 of Regulation (EU) No 909/2014 ;

(b) the plan referred to in Article 47(2) of Regulation (EU) No 909/2014 and any updates to that plan, and evidence of its approval by the management body or an appropriate committee of the management body of the applicant CSD.

SECTION 7

Article 36

CSD links

Where the applicant CSD has established or intends to establish CSD links, the application for authorisation shall contain the following information:

(a) a description of the CSD links accompanied by assessments of potential sources of risks arising from those link arrangements by the applicant CSD;

(b) the expected or actual settlement volumes and values of the settlement performed within the CSD links;

(c) the procedures concerning the identification, assessment, monitoring and management of all potential sources of risk for the applicant CSD and for its participants arising from the link arrangement and the appropriate measures put in place to mitigate them;

(d) an assessment of the applicability of insolvency laws applicable to the operation of a CSD link and their implications for the applicant CSD;

(e) other relevant information requested by the competent authority for assessing the compliance of CSD links with the requirements provided in Article 48 of Regulation (EU) No 909/2014 and Chapter XII of this Regulation.

SECTION 8

Access to CSDs

Article 37

Access rules

An application for authorisation shall include a description of the procedures for dealing with the following requests for access:

(a) from legal persons intending to become participants in accordance with Article 33 of Regulation (EU) No 909/2014 and Chapter XIII of this Regulation;

(b) from issuers in accordance with Article 49 of Regulation (EU) No 909/2014 and Chapter XIII of this Regulation;

(c) from other CSDs in accordance with Article 52 of Regulation (EU) No 909/2014 and Chapter XIII of this Regulation;

(d) from other market infrastructures in accordance with Article 53 of Regulation (EU) No 909/2014 and Chapter XIII of this Regulation.

SECTION 9

Additional information

Article 38

Request for additional information

The competent authority may request from the applicant CSD any additional information necessary for assessing whether, at the time of granting the authorisation, the applicant CSD complies with the requirements of Regulation (EU) No 909/2014.

CHAPTER IV

PARTICIPATIONS OF CSDs IN CERTAIN ENTITIES

(Article 18(3) of Regulation No 909/2014)

Article 39

Criteria for participations of a CSD

In granting the approval for a CSD's participation in a legal person which does not provide the services set out in Sections A and B of the Annex to Regulation (EU) No 909/2014, the competent authority shall take into account the following criteria:

(a) the extent of the financial liabilities assumed by the CSD as a result of that participation;

(b) whether the CSD holds sufficient financial resources that fulfil the criteria referred to in Article 46 of Regulation (EU) No 909/2014 to cover the risks resulting from the following:

  (i) the guarantees given by the CSD to that legal person;

  (ii) any contingent obligations undertaken by the CSD in favour of that legal person;

  (iii) any loss sharing agreements or recovery mechanism of that legal person;

(c) whether the legal person in which the CSD holds a participation provides services that are complementary to the core services offered by the CSD, as referred to in Article 18(4) of Regulation (EU) No 909/2014, such as:

  (i) a CCP authorised or recognised under Regulation (EU) No 648/2012 of the European Parliament and of the Council; or

  (ii) a trading venue as defined in point (42) of Article 2(1) of Regulation (EU) No 909/2014;

(d) whether the participation of the CSD results in the control by the CSD over the legal person as defined in point (21) of Article 2(1) of Regulation (EU) No 909/2014;

(e) the CSD's analysis of the risks arising from that participation, including any analysis approved by an internal or external auditor, demonstrating that all risks resulting from the participation are adequately managed. Competent authorities shall take into account, in particular, the following aspects of the CSD's analysis:

(i) the strategic justification for the participation, which takes into account the interests of the users of the CSD, including issuers, participants and their clients;

(ii) the financial risks and liabilities resulting from a participation of the CSD.

CHAPTER V

REVIEW AND EVALUATION

(Article 22 of Regulation No 909/2014)

Article 40

Information to be provided to the competent authority

1. For the purposes of this Chapter, a 'review period' as defined in point (a) of Article 1 shall include the period between the first authorisation granted to a CSD in accordance with Article 17(1) of Regulation (EU) No 909/2014 and the first review and evaluation referred to in Article 22(1) of that Regulation

2. For the purposes of the review and evaluation referred to in Article 22(1) of Regulation (EU) No 909/2014, a CSD shall provide the following information to its competent authority:

(a) the information referred to in Articles 41 and 42;

(b) a report on the CSD's activities and the substantive changes referred to in Article 16(4) of Regulation (EU) No 909/2014 made during the review period and all related documents;

(c) any additional information requested by the competent authority that is necessary for assessing the compliance of the CSD and its activities with Regulation (EU) No 909/2014 during the review period.

3. The report referred to under point (b) of paragraph 2 shall include a declaration by a CSD of an overall compliance with the provisions of Regulation (EU) No 909/2014 during the review period.

Article 41

Periodic information relevant for the reviews

For each review period, the CSD shall provide the competent authority with the following information:

(a) a complete set of the latest audited financial statements of the CSD, including those consolidated at group level;

(b) a summarised version of the most recent interim financial statements of the CSD;

(c) any decisions of the management body following the advice of the user committee, as well as any decisions where the management body has decided not to follow the advice of the user committee;

(d) information on any pending civil, administrative or any other judicial or extrajudicial proceedings involving the CSD, in particular in relation to matters concerning tax and insolvency, or matters that may cause financial or reputational costs for the CSD;

(e) information on any pending civil, administrative or any other judicial or extrajudicial, proceedings involving a member of the management body or a member of the senior management that may have an negative impact on the CSD;

(f) any final decisions resulting from the proceedings referred to in points (d) and (e);

(g) a copy of the results of business continuity stress tests or similar exercises performed during the review period;

(h) a report on the operational incidents that occurred during the review period and affected the smooth provision of any core services, the measures taken to address them and the results thereof;

(i) a report on the performance of the securities settlement system, including an assessment of the system's availability during the review period, measured on a daily basis as the percentage of time the system is operational and functioning according to the agreed parameters;

(j) a summary of the types of manual intervention performed by the CSD;

(k) information concerning the identification of the CSD's critical operations, any substantive changes to its recovery plan, the results of stress scenarios, the recovery triggers and the recovery tools of the CSD;

(l) information on any formal complaints received by the CSD during the review period including information on the following elements:

  (i) the nature of the complaint;

  (ii) how the complaint was handled, including the outcome of the complaint;

  (iii) the date when the treatment of the complaint ended;

(m) information concerning the cases where the CSD denied access to its services to any existing or potential participant, any issuer, another CSD or another market infrastructure in accordance with Articles 33(3), 49(3), 52(2) and 53(3) of Regulation (EU) No 909/2014;

(n) a report on changes affecting any CSD links established by the CSD, including changes to the mechanisms and procedures used for the settlement in those CSD links;

(o) information concerning all cases of identified conflicts of interests that materialised during the review period, including the description of how they were managed;

(p) information concerning internal controls and audits performed by the CSD during the review period;

(q) information concerning any identified infringement of Regulation (EU) No 909/2014, including those identified through the reporting channel referred to in Article 26(5) of Regulation (EU) No 909/2014;

(r) detailed information concerning any disciplinary actions taken by the CSD, including any cases of suspension of participants in accordance with Article 7(9) of Regulation No 909/2014 with a specification of the period of suspension and the reason for suspension;

(s) the general business strategy of the CSD covering a period of at least three years after the last review and evaluation and a detailed business plan for the services provided by the CSD covering at least a period of one year after the last review and evaluation.

Article 42

Statistical data to be delivered for each review and evaluation

1. For each review period, the CSD shall provide the competent authority with the following statistical data:

(a) a list of the participants of each securities settlement system operated by the CSD, specifying their country of incorporation;

(b) a list of issuers and a list of securities issues recorded in securities accounts centrally and not centrally maintained in each securities settlement system operated by the CSD, specifying the country of incorporation of the issuers and the identification of the issuers to whom the CSD provides the services referred to in points (1) and (2) of Section A of the Annex to Regulation (EU) No 909/2014;

(c) the total market value and nominal value of the securities recorded in securities accounts centrally and not centrally maintained in each securities settlement system operated by the CSD;

(d) the nominal and market value of the securities referred to in point (c) specified as follows:

(i) by each of the following types of financial instruments:

- transferable securities referred to in point (a) of Article 4(1)(44) of Directive 2014/65/EU;

- sovereign debt referred to in Article 4(1)(61) of Directive 2014/65/EU;

- transferable securities referred to in point (b) of Article 4(1)(44) of Directive 2014/65/EU, other than sovereign debt referred to in Article 4(1)(61) of Directive 2014/65/EU;
- transferable securities referred to in point (c) of Article 4(1)(44) of Directive 2014/65/EU;
- exchange-traded funds as defined in point (46) of Article 4(1) of Directive 2014/65/UE (ETF);
- units in collective investment undertakings, other than ETFs;
- money-market instruments, other than sovereign debt referred to in Article 4(1)(61) of Directive 2014/65/EU;
- emission allowances;
- other financial instruments;

(ii) by country of incorporation of the participant;

(iii) by country of incorporation of the issuer;

(e) the nominal and market value of the securities initially recorded in each securities settlement system operated by the CSD;

(f) the nominal and market value of the securities referred to in point (e) specified as follows:

(i) by types of financial instruments referred to in point (d)(i);

(ii) by country of incorporation of the participant;

(iii) by country of incorporation of the issuer.

(g) the total number and the values of the settlement instructions against payment and the total number and the values of the free of payment (FOP) settlement instructions settled in each securities settlement system operated by the CSD;

(h) the total number and the values of the settlement instructions categorised as follows:

(i) by types of financial instruments referred to in point (d)(i);

(ii) by country of the incorporation of the participant;

(iii) by country of incorporation of the issuer;

(iv) by settlement currency;

(v) by type of settlement instructions, as follows:

- a free of payment (FOP) settlement instructions that consist of deliver free of payment (DFP) and receive free of payment (RFP) settlement instructions;
- delivery versus payment (DVP) and receive versus payment (RVP) settlement instructions;
- delivery with payment (DWP) and receive with payment (RWP) settlement instructions;
- payment free of delivery (PFOD) settlement instructions.

(vi) for settlement instructions against payment, by whether the cash leg is settled in accordance with Article 40(1) of Regulation (EU) No 909/2014 or in accordance with Article 40(2) of Regulation (EU) No 909/2014;

(i) the number and value of buy-in transactions referred to in Article 7(3) of Regulation (EU) No 909/2014;

(j) the number and amount of penalties referred to in Article 7(2) of Regulation (EU) No 909/2014 per participant;

(k) the total value of securities borrowing and lending operations processed by the CSD acting as an agent or as principal for each type of financial instruments referred to in point (d)(i);

(l) the total value of settlement instructions settled via each CSD link, specifying whether the CSD is the requesting CSD or the receiving CSD;

(m) the value of guarantees and commitments received or provided by the CSD related to securities borrowing and lending operations;

(n) the value of treasury activities involving foreign exchange and transferable securities related to managing participants' long balances including categories of institutions whose long balances are managed by the CSD;

(o) the number of reconciliation processes revealing undue creations or deletions of securities as referred to in Article 65(2) where those processes concern securities issues recorded in securities accounts centrally and not centrally maintained by the CSD;

(p) the mean, median, and mode for the length of time taken to remedy the error identified according to Article 65(2).

The values referred to in points (g), (h) and (l) of subparagraph 1 shall be calculated as follows:

(a) in the case of settlement instructions against payment, the settlement amount of the cash leg;

(b) in the case of FOP settlement instructions, the market value of the financial instruments or, where not available, the nominal value of the financial instruments.

2. The market value referred to in paragraph 1 shall be calculated on the last day of the review period as follows:

(a) for financial instruments referred to in Article 3(1) of Regulation (EU) No 600/2014 of the European Parliament and of the Council[9] admitted to trading on a trading venue within the Union, the market value shall be the closing price of the most relevant market in terms of liquidity referred to in Article 4(6)(b) of that Regulation;

(b) for financial instruments admitted to trading on a trading venue within the Union other than those referred to in point (a), the market value shall be the closing price derived from the trading venue within the Union with the highest turnover;

[9] Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (OJ L 173, 12.6.2014, p. 84).

(c) for financial instruments other than those referred to in points (a) and (b) the market value shall be determined on the basis of a price calculated using a pre-determined methodology that refers to criteria related to market data, such as market prices available across trading venues or investment firms.

3. The CSD shall provide the values referred to in paragraph 1 in the currency in which the securities are denominated, settled or in which credit is extended. The competent authority may request the CSD to provide these values in the currency of the home Member State of the CSD or in Euro.

4. For the purposes of statistical reporting by a CSD, the competent authority may determine algorithms or principles for data aggregation.

Article 43

Other information

Documents provided by the CSD to the competent authority pursuant to Article 41 shall indicate the following:

(a) whether a document is provided for the first time or is a document that has already been provided and has been updated during the review period;

(b) the unique reference number of the document assigned by the CSD;

(c) the title of the document;

(d) the chapter, section or page of the document where changes have been introduced during the review period and any additional explanation in relation to the changes introduced during the review period.

Article 44

Information to be supplied to the authorities referred to in Article 22(7) of Regulation (EU) No 909/2014

For each review period, the competent authority shall supply the following information to the authorities referred to in Article 22(7) of Regulation (EU) No 909/2014:

(a) a report on the evaluation by the competent authority of the risks to which the CSD is or might be exposed or which it creates for the smooth functioning of securities markets;

(b) any envisaged or final remedial actions or penalties against the CSD as a result of the review and evaluation.

Where applicable, the report referred to in point (a) shall include the results of the competent authority's analysis of how the CSD complies with the requirements referred to in Article 24(2), and the relevant documents and information referred to in Article 24(2) submitted by the CSD.

Article 45

Exchange of information between the competent authorities referred to in Article 22(8) of Regulation (EU) No 909/2014

1. During the review and evaluation, the competent authority shall send to the competent authorities referred to in Article 22(8) of Regulation (EU) No 909/2014 any relevant information provided by the CSD in connection to staff, key individuals, functions, services or systems shared between that CSD and other CSDs with which it maintains the types of relations referred to in points (a), (b) and (c) of Article 17(6) of Regulation (EU) No 909/2014 within 10 working days from the receipt of that information.

2. After performing the review and evaluation, the competent authority shall send the following information to the competent authorities referred to in Article 22(8) of Regulation (EU) No 909/2014:

   (a) a report on the evaluation by the competent authority of the risks to which the CSD is or might be exposed or which it creates for the smooth functioning of securities markets;

   (b) any envisaged or final remedial actions or penalties against the CSD as a result of the review and evaluation.

CHAPTER VI

RECOGNITION OF A THIRD-COUNTRY CSD

(Article 25(6) of Regulation (EU) No 909/2014)

Article 46

Content of the application

1. An application for recognition shall include the information set out in Annex I.

2. An application for recognition shall:

   (a) be provided in a durable medium;

   (b) be submitted in both paper form and electronic form, the latter using open source formats that may be read easily;

   (c) be submitted in a language customary in the sphere of international finance, including translations therein where the original documents are not drawn up in a language customary in the sphere of international finance;

   (d) be provided with a unique reference number for each document included.

3. The applicant CSD shall provide evidence certifying the information included in Annex I.

CHAPTER VII

RISK MONITORING TOOLS

(Article 26(1) to (7) of Regulation (EU) No 909/2014)

Article 47

Risk monitoring tools of CSDs

1. A CSD shall establish, as part of its governance arrangements, 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, CCPs, trading venues, payment systems, settlement banks, liquidity providers and investors.

   The CSD shall structure the policies, procedures and systems referred to in the first subparagraph so as to ensure that users and, where relevant, their clients properly manage and address the risks they pose to the CSD.

2. For the purposes of paragraph 1, the governance arrangements of the CSD shall include the following:

   (a) the composition, role, responsibilities, procedures for appointment, performance assessment and accountability of the management body and of its risk monitoring committees;

   (b) the structure, role, responsibilities, procedures for appointment and performance assessment of the senior management;

   (c) the reporting lines between the senior management and the management body;

   The governance arrangements referred to in the first subparagraph shall be clearly specified and well documented.

3. A CSD shall establish and specify the tasks of the following functions:

   (a) a risk management function;

   (b) a technology function;

   (c) a compliance and internal control function;

   (d) an internal audit function.

   Each function shall have a well-documented description of its tasks, the necessary authority, resources, expertise and access to all relevant information to carry out those tasks.

   Each function shall operate independently from the other functions of the CSD.

Article 48

Risk monitoring committees

1. A CSD shall establish the following committees:

   (a) a risk committee responsible for advising the management body on the CSD's overall current and future risk tolerance and strategy;

   (b) an audit committee responsible for advising the management body on the performance of the CSD's internal audit function, which it shall oversee;

   (c) a remuneration committee responsible for advising the management body on the CSD's remuneration policy, which it shall oversee.

2. Each committee shall be chaired by a person who has appropriate experience in the field of competence of that committee and is independent from the CSD's executive members of the management body.

The majority of members of each committee shall not be executive members of the management board.

The CSD shall establish a clear and publicly available mandate and procedures for each committee, and shall ensure their access to external expert advice where necessary.

Article 49

Responsibilities of key personnel in respect to the risks

1. A CSD shall have adequate staff to meet its obligations. A CSD shall not share staff with other group entities, unless it does so under the terms of a written outsourcing arrangement in accordance with Article 30 of Regulation (EU) No 909/2014.

2. The management body shall assume at least the following responsibilities:

(a) establish well-documented policies, procedures and processes by which the management body, senior management and committees shall operate;

(b) establish clear objectives and strategies for the CSD;

(c) effectively monitor senior management;

(d) establish adequate remuneration policies;

(e) ensure the surveillance of the risk management function and take the decisions related to risk management;

(f) ensure the independence and adequate resources of the functions referred to in Article 47(3);

(g) monitor outsourcing arrangements;

(h) monitor and ensure compliance with all relevant regulatory and supervisory requirements;

(i) be accountable to shareholders or other owners, employees, users and other relevant stakeholders;

(j) approve internal audit planning and review;

(k) review and update regularly the governance arrangements of the CSD.

Where the management body or its members delegate tasks, they shall retain the responsibility for decisions that may affect the smooth provision of services by the CSD.

The CSD's management body shall hold the final responsibility for managing the CSD's risks. The management body shall define, determine and document an appropriate level of risk tolerance and risk bearing capacity for the CSD and for all the services that the CSD provides. The management body and senior management shall ensure that the CSD's policies, procedures and controls are consistent with the CSD's risk tolerance and risk bearing capacity and that these policies, procedures and controls address how the CSD identifies, reports, monitors and manages risks.

3. The senior management shall have at least the following responsibilities:

(a) ensure consistency of the activities of the CSD with the objectives and strategy of the CSD as determined by the management body;

(b) design and establish risk management, technology, compliance and internal control procedures that promote the objectives of the CSD;

(c) subject the risk management, technology, compliance and internal control procedures to regular review and testing;

(d) ensure that sufficient resources are devoted to risk management, technology, compliance and internal control, and internal audit.

4. A CSD shall establish lines of responsibility that are clear, consistent and well-documented. A CSD shall have clear and direct reporting lines between the members of its management body and the senior management in order to ensure that the senior management is accountable for its performance. The reporting lines for the risk management function, compliance and internal control function and internal audit function shall be clear and separate from those for the operations of the CSD.

5. A CSD shall have a chief risk officer who shall implement the risk management framework including the policies and procedures established by the management body.

6. A CSD shall have a chief technology officer who shall implement the technology framework including the policies and procedures established by the management body.

7. A CSD shall have a chief compliance officer who shall implement the compliance and internal control framework including the policies and procedures established by the management body.

8. A CSD shall ensure that the functions of the chief risk officer, chief compliance officer and chief technology officer are carried out by different individuals, who shall be employees of the CSD or of an entity from the same group as the CSD. A single individual shall have the responsibility for each of these functions.

9. The CSD shall establish procedures ensuring that the chief risk officer, the chief technology officer and the chief compliance officer have direct access to the management body.

10. Persons appointed as chief risk officer, chief compliance officer or chief technology officer may undertake other duties within the CSD provided that specific procedures are put in place in the governance arrangements to identify and manage any conflict of interest that may arise from those duties.

Article 50

Conflicts of interest

1. A CSD shall put in place a policy in relation to conflicts of interest arising or affecting the CSD or its activities, including with respect to outsourcing arrangements.

2. Where a CSD is part of a group of undertakings, its organisational administrative arrangements shall take into account any circumstances, of which the CSD is or should be aware, which may give rise to a conflict of interest arising as a result of the structure and business activities of other undertakings of the same group.

3. Where a CSD shares the functions of chief risk officer, chief compliance officer, chief technology officer, or internal audit with other entities of the group, the governance arrangements shall ensure that related conflicts of interest at group level are appropriately managed.

4. The organisational and administrative arrangements referred to in Article 26(3) of Regulation (EU) No 909/2014 shall include a description of the circumstances which may give rise to a conflict of interest entailing a material risk of damage to the interests of one or more users of the CSD, or their clients, as well as the procedures to be followed and the measures to be adopted in order to manage those conflicts of interest.

5. The description of circumstances referred to in paragraph 4 shall take into account whether a member of the management body, senior management or staff of the CSD, or any person directly or indirectly linked to those individuals or to the CSD:

   (a) has a personal interest in the use of the services, materials and equipment of the CSD for the purposes of another commercial activity;

   (b) holds a personal or financial interest in another entity that enters into contracts with the CSD;

   (c) holds a participation or a personal interest in another entity that provides services used by the CSD, including any entity to which the CSD outsources services or activities;

   (d) has a personal interest in an entity that uses the service of the CSD;

   (e) is related to any legal or natural person that has influence on the operations of any entity that provides the services used by the CSD or uses the services provided by the CSD;

   (f) is member of the management body or any other bodies or committees of any entity that provides the services which are used by the CSD or uses the services provided for the CSD.

   For the purposes of this paragraph, a direct or indirect link to a natural person shall comprise the spouse or legal partner, family members in direct ascending or descending line up to the second degree and their spouses or legal partners, the siblings and their spouse or legal partners, and any person having the same domicile or habitual residence as the employees, managers or members of the management body.

6. A CSD shall take all reasonable steps to prevent any misuse of the information held in its systems and shall prevent the use of that information for other business activities. A natural person who has access to information recorded in a CSD or a legal person that belongs to the same group as the CSD shall not use information recorded in that CSD for any commercial purposes without prior written consent of the person to whom the information refers.

Article 51

Audit methods

1. The internal audit function of a CSD shall ensure the following:

   (a) establish, implement and maintain an all-encompassing audit plan to examine and evaluate the adequacy and effectiveness of the CSD’s systems, risk

management processes, internal control mechanisms, remuneration policies, governance arrangements, activities and operations, including outsourced activities;

(b) review and report the audit plan to the competent authority at least annually;

(c) establish a comprehensive risk-based audit;

(d) issue recommendations based on the result of work carried out in accordance with point (a) and verify compliance with those recommendations;

(e) report internal audit matters to the management body;

(f) be independent from the senior management and report directly to the management body;

(g) ensure that special audits may be performed at short notice on an event-driven basis.

2. Where the CSD belongs to a group, the internal audit function may be carried out at group level provided that the following requirements are complied with:

(a) it is separate and independent from other functions and activities of the group;

(b) it has a direct reporting line to the management body of the CSD;

(c) the arrangement concerning the operation of the internal audit function does not prevent the exercise of supervisory and oversight functions, including on-site access to acquire any relevant information needed to fulfil those functions.

3. The CSD shall assess the internal audit function.

Internal audit assessments shall include an on-going monitoring of the performance of the internal audit activity and periodic reviews performed through self-assessment carried out by the audit committee or by other persons within the CSD or the group with sufficient knowledge of internal audit practices.

An external assessment of the internal audit function shall be conducted by a qualified and independent assessor from outside the CSD and its group structure at least once every five years.

4. A CSD's operations, risk management processes, internal control mechanisms and records shall be subject to regular internal or external audits.

The frequency of the audits shall be determined on the basis of a documented risk assessment. Audits referred to in the first subparagraph shall be carried out at least every two years.

5. A CSD's financial statement shall be prepared on an annual basis and be audited by statutory auditors or audit firms approved in accordance with Directive 2006/43/EC.

Article 52

Sharing audit findings with the user committee

1. A CSD shall share audit findings with the user committee in any of the following cases:

(a) where the findings relate to the criteria for accepting issuers or users to their respective securities settlement systems operated by the CSDs;

(b) where the findings relate to any other aspect of the user committee's mandate;

(c) where the findings may impact the level of provision of services by a CSD, including ensuring business continuity.

2. Members of the user committee shall not be provided with information that may place those members at a competitive advantage.

CHAPTER VIII

RECORD-KEEPING

(Article 29(3) of Regulation (EU) No 909/2014)

Article 53

General Requirements

1. A CSD shall maintain full and accurate records of all its activities as specified in this Regulation at all times, including during disruption events when the business continuity policy and disaster recovery plans are activated. Those records shall be readily accessible.

2. The records kept by a CSD shall cover separately each individual service provided by the CSD in accordance with Regulation (EU) No 909/2014.

3. A CSD shall keep records in a durable medium that allows information to be provided to the authorities referred to in Article 29(2) of Regulation (EU) No 909/2014. The record keeping system shall ensure that all of the following conditions are met:

   (a) each key stage of the processing of records by the CSD may be reconstituted;

   (b) the original content of a record before any corrections or other amendments may be recorded, traced and retrieved;

   (c) measures are put in place to prevent unauthorised alteration of records;

   (d) measures are put in place to ensure the security and confidentiality of the data recorded;

   (e) a mechanism for identifying and correcting errors is incorporated in the record keeping system;

   (f) the timely recovery of the records in the case of a system failure is ensured within the record keeping system.

Article 54

Transaction/Settlement Instruction (Flow) Records

1. A CSD shall maintain records of all transactions, settlement instructions and orders concerning settlement restrictions that it processes and it shall ensure that its records include all necessary information to accurately identify them.

2. In relation to every settlement instruction and order concerning settlement restrictions received, a CSD shall, immediately upon receiving the relevant information, make and keep updated a record of the following details, depending on

whether the settlement instruction or settlement restrictions covers securities or cash only, or both securities and cash:

(a) type of settlement instruction as referred to in point (h)(v) of Article 42(1);

(b) type of transaction, as follows:

  (i) purchase or sale of securities;

  (ii) collateral management operations;

  (iii) securities lending/borrowing operations;

  (iv) repurchase transactions;

  (v) others;

(c) unique instruction reference of the participant;

(d) trade date;

(e) intended settlement date;

(f) settlement timestamp;

(g) timestamp of the moment of entry of the settlement instruction into the securities settlement system;

(h) timestamp of the moment of irrevocability of the settlement instruction;

(i) matching timestamp in case of matched settlement instructions;

(j) securities account identifier;

(k) cash account identifier;

(l) settlement bank identifier;

(m) identifier of the instructing participant;

(n) identifier of the instructing participant's counterpart;

(o) identifier of the instructing participant's client, where known to the CSD;

(p) identifier of the client of the instructing participant's counterpart, where known to the CSD;

(q) securities identifier;

(r) settlement currency;

(s) settlement cash amount;

(t) quantity or nominal amount of securities;

(u) status of the settlement instruction covering:

  (i) pending instructions which can still settle on the intended settlement date ;

  (ii) failed settlement instructions which cannot settle anymore on the intended settlement date ;

  (iii) fully settled settlement instructions;

  (iv) partially settled settlement instructions, including the settled part and the missing part of either financial instruments or cash;

(v) cancelled settlement instructions, including information whether it is cancelled by the system or by the participant.

For each of the categories of settlement instructions referred to in the first subparagraph, the following information shall be recorded:

(a) whether an instruction is matched or not matched;

(b) whether an instruction can settle partially;

(c) whether an instruction is on hold;

(d) where relevant, what the reasons are for instruction being pending or failing

(e) place of trading;

(f) if applicable, place of clearing;

where a buy-in process is initiated in accordance with Article 7(3) of Regulation (EU) No 909/2014, details regarding:

(i) the final results of the buy-in process on the last business day of the deferral period at the latest, including the number and value of the financial instruments where the buy-in is partially or fully successful;

(ii) the payment of cash compensation, including the amount of the cash compensation, where the buy-in is not possible, fails or is partially successful;

(iii) the cancellation of the initial settlement instruction;

(iv) for each settlement fail, the amount of the penalties referred to in Article 7(2) of Regulation (EU) No 909/2014.

Article 55

Position (Stock) Records

1. A CSD shall keep records of positions corresponding to all securities accounts that it maintains. Separate records shall be held for each account kept in accordance with Article 38 of Regulation (EU) No 909/2014.

2. A CSD shall keep records of the following information:

(a) identifier of each issuer for which the CSD provides the core service referred to in point 1 or 2 of Section A of the Annex to Regulation (EU) No 909/2014;

(b) identifier of each securities issue for which the CSD provides the core services referred to in point 1 or 2 of Section A of the Annex to of Regulation (EU) No 909/2014, the law under which the securities recorded by the CSD are constituted and the country of incorporation of the issuers of each securities issue;

(c) identifier of each securities issue recorded in securities accounts not centrally maintained by the CSD, the law under which the securities recorded by the CSD are constituted and the country of incorporation of the issuers of each securities issue;

(d) identifier of the issuer CSD or of the relevant third country entity performing similar functions to an issuer CSD for each securities issue referred to in point (c);

(e) issuers' securities accounts identifiers, in the case of issuer CSDs;

(f) issuers' cash accounts identifiers, in the case of issuer CSDs;

(g) identifiers of settlement banks used by each issuer, in the case of issuer CSDs;

(h) participants' identifiers;

(i) participants' country of incorporation;

(j) participants' securities accounts identifiers;

(k) participants' cash accounts identifiers;

(l) identifiers of settlement banks used by each participant;

(m) country of incorporation of settlement banks used by each participant.

3. At the end of each business day, a CSD shall record for each position the following details to the extent that they are relevant for the position:

(a) identifiers of participants and of other account holders;

(b) type of securities accounts according to whether a securities account belongs to a participant ('participant's own account'), to one of its clients ('individual client segregation') or to several of its clients ('omnibus client segregation');

(c) for each securities issue identifier (ISIN), end of day balances of securities accounts covering the number of securities;

(d) for each securities account and ISIN under point (c), the number of securities subject to settlement restrictions, type of the restrictions and the identity of the beneficiary of restrictions at the end of day.

4. A CSD shall keep records of settlement fails and the measures adopted by the CSD and its participants to prevent and address settlement fails in accordance with Articles 6 and 7of Regulation (EU) No 909/2014.

Article 56

Ancillary Services Records

1. A CSD shall keep the types of records specified in Annex II to this Regulation for each of the ancillary services provided by a CSD in accordance with Sections B and C of the Annex to Regulation (EU) No 909/2014, including the end of day balances of the cash accounts provided by the CSD or the designated credit institution for each currency.

2. Where a CSD provides ancillary services other than those explicitly mentioned in Sections B or C of the Annex to Regulation (EU) No 909/2014, it shall keep adequate records of those services.

Article 57

Business Records

1. A CSD shall maintain adequate and orderly records of activities related to its business and internal organisation.

2. The records referred to in paragraph 1 shall reflect any substantive changes in the documents held by the CSD and shall include the following:

(a) the organisational charts for the management body, senior management, relevant committees, operational units and all other units or divisions of the CSD;

(b) the identities of the shareholders, whether natural or legal persons, that exercise direct or indirect control over the management of the CSD or that have participations in the capital of the CSD and the amounts of those holdings;

(c) participations of the CSD in the capital of other legal entities;

(d) the documents attesting the policies, procedures and processes required under the CSD's organisational requirements and in relation to the services provided by the CSD;

(e) the minutes of management body meetings and of meetings of senior management committees and other committees;

(f) the minutes of meetings of the user committees;

(g) the minutes of consultation groups with participants and clients, if any;

(h) internal and external audit reports, risk management reports, internal control and compliance reports, including responses from the senior management to the reports;

(i) all outsourcing contracts;

(j) business continuity policy and disaster recovery plan;

(k) records reflecting all assets, liabilities and capital accounts of the CSD;

(l) records reflecting all costs and revenues, including costs and revenues which are accounted separately in accordance with Article 34(6) of Regulation (EU) No 909/2014;

(m) formal complaints received, including information on the complainant's name and address; the date when the complaint was received; the name of all persons identified in the complaint; a description of the nature and content of the complaint; and the date when the complaint was resolved;

(n) records of any interruption of services or dysfunction, including a detailed report on the timing, effects and remedial actions of that interruption or dysfunction;

(o) records of the results of the back and stress tests performed by the CSDs providing banking-type ancillary services;

(p) written communications with the competent authority, ESMA and relevant authorities;

(q) legal opinions received in accordance with the relevant provisions on organisational requirements in accordance with Chapter VII of this Regulation;

(r) documentation regarding link arrangements in accordance with Chapter XII of this Regulation;

(s) tariffs and fees applied to the different services, including any discount or rebate.

Article 58

Additional records

A CSD shall keep the additional records requested by the competent authority for the purpose of enabling the competent authority to monitor compliance of the CSD with Regulation (EU) 909/2014.

CHAPTER IX

RECONCILIATION MEASURES

(Article 37 (4) of Regulation No 909/2014)

Article 59

General reconciliation measures

1. A CSD shall perform the reconciliation measures referred to in Article 37(1) of Regulation (EU) No 909/2014 for each securities issue recorded in securities accounts centrally and not centrally maintained by the CSD.

   The CSD shall compare the previous end-of-day balance with all the settlements processed during the day and the current end-of-day balance for each securities issue and securities account centrally or not centrally maintained by the CSD.

   A CSD shall use double-entry accounting, according to which for each credit entry made on a securities account maintained by the CSD, centrally or not centrally, there is a corresponding debit entry on another securities account maintained by the same CSD.

2. The audits referred to in Article 26(6) of Regulation No 909/2014 shall ensure that the records of a CSD related to securities issues are accurate, and that its reconciliation measures referred to in Article 37(1) of Regulation (EU) No 909/2014 and the measures concerning cooperation and exchanges of information with third parties related to reconciliation referred to in Article 37(2) of Regulation (EU) No 909/2014 are adequate.

3. Where the reconciliation process concerns securities subject to immobilisation, a CSD shall put in place adequate measures to protect the physical securities from theft, fraud, and destruction. Those measures shall at least include the use of vaults whose design and location ensure a high level of protection against floods, earthquakes, fire and other disasters.

4. Audits referred to in Article 26(6) of Regulation No 909/2014 with respect to the vaults, including physical inspections, shall be performed at least annually. The CSD shall share the results of those audit controls with the competent authority.

Article 60

Reconciliation measures for corporate actions

1. A CSD shall not determine the entitlements to the proceeds of a corporate action on stock that would change the balance of securities accounts maintained by the CSD

until the reconciliation measures specified in Article 59 and in Articles 61, 62 and 63 are completed.

2. When a corporate action has been processed, a CSD shall ensure that all securities accounts maintained by the CSD, centrally or not centrally, are updated.

Article 61

Reconciliation measures for the registrar model

Where a registrar, issuance agent, or other similar entity is involved in the reconciliation process for a certain securities issue in accordance with Article 37(2) of Regulation (EU) No 909/2014, and maintains records of securities which are also recorded in the CSD, the measures to be taken by the CSD and that entity to ensure the overall integrity of the issue shall include a daily reconciliation of the total balance recorded on the securities accounts maintained by the CSD with the corresponding records of securities maintained by that entity. The CSD and that entity shall also conduct:

(a) where the securities have been transferred during a given business day, an end of day reconciliation of the balance of each securities account maintained by the CSD with the balance of the corresponding record of securities maintained by that entity;

(b) at least once every two weeks, a full reconciliation of all balances in a securities issue with all balances on the corresponding record of securities maintained by that entity.

Article 62

Reconciliation measures for the transfer agent model

Where a fund manager, transfer agent or other similar entity is responsible for the reconciliation process for an account that maintains a part of a securities issue recorded in a CSD, the measures to be taken by the CSD and that entity to ensure the integrity of this part of the issue shall include a daily reconciliation of the total balance of the securities accounts maintained by the CSD with that entity’s records of securities maintained by the CSD, including the aggregated opening and closing balances.

Where the CSD maintains its accounts in that entity's register through a third party which is not a CSD, the CSD shall require the third party to inform that entity that it is acting on behalf of the CSD and to set up equivalent cooperation and information exchange measures with that entity to ensure that the requirements under this Article are met.

Article 63

Reconciliation measures for the common depository model

Where CSDs that have established an interoperable link use a common depository or any other similar entity, each CSD shall reconcile on a daily basis the total balance per securities issue recorded on the securities accounts it maintains, other than for other CSDs in the interoperable link, with the corresponding records of securities that the common depository or the other similar entity maintains for that CSD.

Where a common depository or any other similar entity is responsible for the overall integrity of a certain securities issue, the common depository or the other similar entity shall conduct a daily comparison of the total balance per securities issue against the balances in the securities accounts it maintains for each CSD.

Where the reconciliation process concerns securities subject to immobilisation, the CSDs shall ensure that the common depository or the other entity meets the requirements set out in Article 59(3).

Article 64

Additional measures where other entities are involved in the reconciliation process

1. A CSD shall review at least annually its cooperation and information exchange measures with other entities referred to in Articles 61, 62 and 63. This review may be conducted in parallel with a review of the CSD link arrangements. When required by the competent authority, the CSD shall implement other cooperation and information exchange measures in addition to those specified in this Regulation.

2. When a CSD establishes links, they shall comply with the additional requirements provided in Article 86.

3. A CSD shall require its participants to reconcile their records with the information received from that CSD on a daily basis.

4. For the purposes of paragraph 3, the CSD shall provide participants on a daily basis the following information specified for each securities account and for each securities issue:

   (a) the aggregated balance of a securities account at the beginning of the respective business day;

   (b) the individual transfers of securities in or from a securities account during the respective business day;

   (c) the aggregated balance of a securities account at the end of the respective business day.

   The CSD shall provide the information referred to in the first subparagraph at the request of other holders of securities accounts maintained by the CSD, centrally or not centrally, where that information is necessary for the reconciliation of those holders' records with the records of the CSD.

5. A CSD shall ensure that, upon its request, its participants, other holders of accounts in the CSD and the account operators provide the CSD with the information that the CSD deems necessary to ensure the integrity of the issue, in particular to solve any reconciliation problems.

   For the purposes of this paragraph, ‘account operator’ shall mean an entity that is contracted by a CSD to record book entries into its securities accounts.

Article 65

Problems related to reconciliation

1. A CSD shall analyse any mismatches and inconsistencies resulting from the reconciliation process and endeavour to solve them before the beginning of settlement on the following business day.

2. Where the reconciliation process reveals an undue creation or deletion of securities, and the CSD fails to solve this problem by the end of the following business day, the CSD shall suspend the securities issue for settlement until the undue creation or deletion of securities has been remedied.

3. In the event of suspension of the settlement, the CSD shall inform without undue delay its participants, competent authority, relevant authorities and all other entities involved in the reconciliation process referred to in Articles 61, 62 and 63.

4. The CSD shall take without undue delay all the necessary measures to remedy the undue creation or deletion of securities and shall inform its competent authority and relevant authorities with regard to the measures taken.

5. The CSD shall inform without undue delay its participants, competent authority, relevant authorities and the other entities involved in the reconciliation process that are referred to in Articles 61, 62 and 63, when the undue creation or deletion of securities has been remedied.

6. Where a securities issue is suspended from settlement, the settlement discipline measures set out in Article 7 of Regulation (EU) No 909/2014 shall not apply in relation to that securities issue for the period of suspension.

7. The CSD shall resume settlement as soon as the undue creation or deletion of securities has been remedied.

8. Where the number of instances of undue creation or deletion of securities referred to in paragraph 2 is higher than five per month, the CSD shall send within one month the competent authority and the relevant authorities a proposed plan of measures for mitigating the occurrence of similar instances. The CSD shall update the plan and shall provide a report on its implementation to the competent authority and the relevant authorities on a monthly basis, until the number of instances referred to in paragraph 2 falls below five per month.

CHAPTER X

OPERATIONAL RISKS

(Article 45(1) to (6) of Regulation 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 on-going 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 sub-contract 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.

SECTION 4

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;

(e) 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 backup 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.

CHAPTER XI

INVESTMENT POLICY

(Article 46(2), (3) and (5) of Regulation No 909/2014)

Article 81

Highly liquid instruments with minimal market and credit risk

1. Financial instruments shall be considered highly liquid with minimal credit and market risk where they are debt instruments meeting the following conditions:

   (a) they are issued or guaranteed by:

      (i) a government;

      (ii) a central bank;

      (iii) a multilateral development bank as listed under Article 117 of Regulation (EU) No 575/2013 of the European Parliament and of the Council[10];

      (iv) the European Financial Stability Facility or the European Stability Mechanism;

   (b) the CSD can demonstrate to the competent authority that the financial instruments have low credit and market risk based upon an internal assessment by the CSD;

   (c) they are denominated in any of the following currencies:

      (i) a currency in which transactions are settled in the securities settlement system operated by the CSD;

      (ii) any other currency the risks of which the CSD is able to manage.

   (d) they are freely transferable and without any regulatory constraint or third party claims that impair liquidation;

[10] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

(e) they have an active outright sale or repurchase market, with a diverse group of buyers and sellers, including in stressed conditions, and to which the CSD has reliable access;

(f) reliable price data on these instruments are publicly available on a regular basis;

For the purposes of point (b), in performing the assessment the CSD shall employ a defined and objective methodology that shall not exclusively rely on external opinions and that takes into consideration the risk arising from the establishment of the issuer in a particular country

2. By way of derogation to paragraph 1, derivative contracts shall be considered highly liquid financial instruments with minimal credit and market risk where the following conditions are met:

(a) they are entered into for the purpose of hedging currency risk arising from the settlement in more than one currency in the securities settlement system operated by the CSD or interest rate risk that may affect CSD assets and, in both cases, qualify as a hedging contract pursuant to International Financial Reporting Standards (IFRS) adopted in accordance with Article 3 of Regulation (EC) No 1606/2002 of the European Parliament and of the Council[11];

(b) reliable price data is published on a regular basis for those derivative contracts;

(c) they are concluded for the specific period of time necessary to reduce the currency or interest rate risk to which the CSD is exposed.

Article 82

Appropriate timeframe for access to assets

1. A CSD shall have immediate and unconditional access to cash assets.

2. A CSD shall have access to financial instruments on the same business day when a decision to liquidate the financial instruments is taken.

3. For the purposes of paragraph 1 and 2, the CSD shall put in place procedures ensuring that the CSD is able to access cash and financial instruments within the timeframes set out therein. The CSD shall inform the competent authority of any change to those procedures in accordance with Article 16(4) of Regulation (EU) No 909/2014 and shall obtain its validation before implementing that change.

Article 83

Concentration limits to individual entities

1. For the purposes of Article 46(5) of Regulation (EU) No 909/2014, a CSD shall hold its financial assets in diversified authorised credit institutions or authorised CSDs in order to remain within acceptable concentration limits.

2. For the purposes of Article 46(5) of Regulation (EU) No 909/2014, acceptable concentration limits shall be determined based on the following:

[11] Regulation (EC) No 1606/2002 of the European Parliament and of the Council of 19 July 2002 on the application of international accounting standards (OJ L 243, 11.9.2002, p. 1).

(a) the geographic distribution of the entities with which the CSD holds its financial assets;

(b) the interdependency relationships that the entity holding the financial assets or entities of its group may have with the CSD;

(c) the level of credit risk of the entity holding the financial assets.

CHAPTER XII

(Article 48(3), (5), (6) and (7) of Regulation (EU) No 909/2014)

CSD LINKS

Article 84

Conditions for the adequate protection of linked CSDs and of their participants

1. A CSD link shall be established and maintained under the following conditions:

(a) the requesting CSD shall meet the requirements of the receiving CSD's participation rules;

(b) the requesting CSD shall conduct an analysis of the receiving third-country CSD's financial soundness, governance arrangements, processing capacity, operational reliability and any reliance on a third party critical service provider;

(c) the requesting CSD shall take all necessary measures to monitor and manage the risks that are identified following the analysis referred to in point (b);

(d) the requesting CSD shall make the legal and operational terms and conditions of the link arrangement available to its participants allowing them to assess and manage the risks involved;

(e) before the establishment of a CSD link with a third-country CSD, the requesting CSD shall perform an assessment of the local legislation applicable to the receiving CSD;

(f) the linked CSDs shall ensure the confidentiality of information in connection to the operation of the link. The ability to ensure confidentiality shall be evidenced by the information provided by the CSDs, including any relevant legal opinions or arrangements;

(g) the linked CSDs shall agree on aligned standards and procedures concerning operational issues and communication in accordance with Article 35 of Regulation (EU) No 909/2014;

(h) before the link becomes operational, the requesting and receiving CSDs shall:

(i) conduct end-to-end tests;

(ii) establish an emergency plan, as part of the business continuity plans of the respective CSDs, identifying the situations where the securities settlement systems of the two CSDs malfunction or break down, and provide for the remedial actions planned if those situations occur;

(i) all link arrangements shall be reviewed at least annually by the receiving CSD and the requesting CSD taking into account all relevant developments, including market and IT developments, as well as any developments in local legislation referred to in point (e);

(j) for CSD links that do not provide for DVP settlement, the annual review referred to in point (i) shall also include an assessment of any developments that may allow supporting DVP settlement.

For the purposes of point (e), in performing the assessment, the CSD shall ensure that the securities maintained in the securities settlement system operated by the receiving CSD benefit from a level of asset protection comparable to the one ensured by the rules applicable to the securities settlement system operated by the requesting CSD. The requesting CSD shall require from the third-country CSD a legal assessment addressing the following issues:

(i) the entitlement of the requesting CSD to the securities, including the law applicable to proprietary aspects, the nature of the rights of the requesting CSD on the securities, the possibility of encumbering the securities;

(ii) the impact of insolvency proceedings opened against the receiving third-country CSD on the requesting CSD regarding the segregation requirements, settlement finality, procedures and time-limits to claim the securities in the relevant third country.

2. In addition to the conditions referred to in paragraph 1, a CSD link providing for DVP settlement shall be established and maintained under the following conditions:

(a) the requesting CSD shall assess and mitigate the additional risks resulting from the settlement of cash;

(b) a CSD that is not authorised to provide banking-type ancillary services in accordance with Article 54 of Regulation (EU) No 909/2014, and which is involved in the execution of cash settlement on behalf of its participants, shall not receive credit and shall use prefunding mechanisms covered by its participants in relation to the DVP settlements to be processed through the link;

(c) a CSD that uses an intermediary for the cash settlement shall ensure that the intermediary performs that settlement efficiently. The CSD shall conduct yearly reviews of the arrangements with that intermediary.

3. In addition to the conditions referred to in paragraphs 1 and 2, an interoperable link shall be established and maintained under the following conditions:

(a) the linked CSDs shall agree on equivalent standards concerning reconciliation, opening hours for the processing of the settlement and of corporate actions and cut-off times;

(b) the linked CSDs shall establish equivalent procedures and mechanisms for transmission of settlement instructions to ensure a proper, secure and straight through processing of settlement instructions;

(c) where an interoperable link supports DVP settlement, the linked CSDs shall reflect at least daily and without undue delay the results of the settlement in their books;

(d) the linked CSDs shall agree on equivalent risk management models;

(e) the linked CSDs shall agree on equivalent contingency and default rules and procedures referred to in Article 41 of Regulation (EU) No 909/2014.

Article 85

Monitoring and management of additional risks resulting from the use of indirect links or intermediaries to operate CSD links

1. In addition to complying with the requirements under Article 84, where a requesting CSD uses an indirect link or an intermediary to operate a CSD link, it shall ensure that:

(a) the intermediary is one of the following:

(i) a credit institution as defined in point (1) of Article 4(1) of Regulation (EU) No 575/2013 that complies with the following requirements:

- it complies with Article 38(5) and (6) of Regulation (EU) No 909/2014 or with segregation and disclosure requirements at least equivalent to those laid down in Article 38(5) and (6) of Regulation (EU) No 909/2014 where the link is established with a third-country CSD;
- it ensures prompt access by the requesting CSD to the securities of the requesting CSD when required;
- it has low credit risk, which shall be established in an internal assessment by the requesting CSD by employing a defined and objective methodology that does not exclusively rely on external opinions;

(ii) a third-country financial institution that complies with the following requirements:

- it is subject to and complies with prudential rules at least equivalent to those laid down in Regulation (EU) No 575/2013;
- it has robust accounting practices, safekeeping procedures, and internal controls;
- it complies with Article 38(5) and (6) of Regulation (EU) No 909/2014 or with segregation and disclosure requirements at least equivalent to those laid down in Article 38(5) and (6) of Regulation (EU) No 909/2014 where the link is established with a third-country CSD;
- it ensures prompt access by the requesting CSD to the securities of the requesting CSD when required;
- it has low credit risk, based upon an internal assessment by the requesting CSD by employing a defined and objective methodology that does not exclusively rely on external opinions;

(b) the intermediary complies with the rules and requirements of the requesting CSD, as evidenced by the information provided by that intermediary, including any relevant legal opinions or arrangements;

(c) the intermediary ensures the confidentiality of information concerning the operation of the CSD link, as evidenced by the information provided by that intermediary, including any relevant legal opinions or arrangements;

(d) the intermediary has the operational capacity and systems for:

(i) handling the services provided to the requesting CSD;

(ii) sending the CSD any information relevant to the services provided in relation to the CSD link in a timely manner;

(iii) complying with the reconciliation measures in accordance with Article 86 and Chapter IX;

(e) the intermediary adheres to and complies with the risk management policies and procedures of the requesting CSD and it has an appropriate risk management expertise;

(f) the intermediary has put in place measures that include business continuity policies and associated business continuity and disaster recovery plans, to ensure the continuity of its services, the timely recovery of its operations and the fulfilment of its obligations in events that pose a significant risk of disrupting its operations;

(g) the intermediary holds sufficient financial resources to fulfil its obligations towards the requesting CSD and to cover any losses for which it may be held liable;

(h) an individually segregated account at the receiving CSD is used for the operations of the CSD link;

(i) the condition referred to in point (e) of Article 84(1) is fulfilled;

(j) the requesting CSD is informed of the continuity arrangements between the intermediary and the receiving CSD;

(k) the proceeds from settlement are promptly transferred to the requesting CSD.

For the purposes of the first indent in point (a)(i), the third indent in point (a)(ii) and point (h), the requesting CSD shall ensure that it can have access to the securities held in the individually segregated account at any point in time. Where an individually segregated account at the receiving CSD is however not available for the operations of a CSD link established with a third-country CSD, the requesting CSD shall inform its competent authority about the reasons justifying the unavailability of individually segregated accounts and shall provide it with the details on the risks resulting from the unavailability of individually segregated accounts. The requesting CSD shall in any case ensure an adequate level of protection of its assets held with the third-country CSD.

2. In addition to complying with the requirements under paragraph 1, when a requesting CSD uses an intermediary to operate a CSD link and that intermediary operates the securities accounts of the requesting CSD on its behalf in the books of the receiving CSD, the requesting CSD shall ensure that:

(a) the intermediary does not have any entitlement to the securities held;

(b) the account in the books of the receiving CSD is opened in the name of the requesting CSD and the liabilities and obligations as regards the registration, transfer and custody of securities are only enforceable between both CSDs;

(c) the requesting CSD is able to immediately access the securities held with the receiving CSD, including in the event of a change or insolvency of the intermediary.

3. Requesting CSDs referred to in paragraphs 1 and 2 shall perform a yearly due diligence to ensure that the conditions referred to therein are fulfilled.

Article 86

Reconciliation procedures for linked CSDs

1. The reconciliation procedures referred to in Article 48(6) of Regulation (EU) No 909/2014 shall include the following measures:

(a) the receiving CSD shall transmit to the requesting CSD daily statements with information specifying the following, per securities account and per securities issue:

(i) the aggregated opening balance;

(ii) the individual movements during the day;

(iii) the aggregated closing balance;

(b) the requesting CSD shall conduct a daily comparison of the opening balance and the closing balance communicated to it by the receiving CSD or by the intermediary with the records maintained by the requesting CSD itself.

In the case of an indirect link, the daily statements referred to in point (a) of the first subparagraph shall be transmitted through the intermediary referred to point (a) of Article 85(1).

2. Where a CSD suspends a securities issue for settlement in accordance with Article 65(2), all CSDs that are participants of or have an indirect link with that CSD, including in the case of interoperable links, shall subsequently suspend the securities issue for settlement.

Where intermediaries are involved in the operation of CSD links, those intermediaries shall establish appropriate contractual arrangements with the CSDs concerned in order to ensure compliance with the first subparagraph.

3. In the event of a corporate action that reduces the balances of securities accounts held by an investor CSD with another CSD, settlement instructions in the relevant securities issues shall not be processed by the investor CSD until the corporate action has been fully processed by the other CSD.

In the event of a corporate action that reduces the balances of securities accounts held by an investor CSD with another CSD, the investor CSD shall not update the securities accounts that it maintains to reflect the corporate action until the corporate action has been fully processed by the other CSD.

An issuer CSD shall ensure the timely transmission to all its participants, including investor CSDs, of information on the processing of corporate actions for a specific securities issue. The investor CSDs shall in turn transmit the information to their participants. That transmission shall include all necessary information for investor CSDs to adequately reflect the outcome of those corporate actions in the securities accounts they maintain.

Article 87

DVP Settlement through CSD links

Delivery versus Payment (DVP) settlement shall be regarded as practical and feasible where:

(a) there is a market demand for DVP settlement evidenced through a request from any of the user committees of one of the linked CSDs;

(b) the linked CSDs may charge a reasonable commercial fee for the provision of DVP settlement, on a cost-plus basis, unless otherwise agreed by the linked CSDs;

(c) there is a safe and efficient access to cash in the currencies used by the receiving CSD for settlement of securities transactions of the requesting CSD and its participants.

CHAPTER XIII

ACCESS TO A CSD

(Articles 33(5), 49(5), 52(3) and 53(4) of Regulation (EU) No 909/2014)

Article 88

Receiving and requesting parties

1. For the purposes of this Chapter, a receiving party shall include one of the following entities:

(a) a receiving CSD as defined in point (5) of Article 2(1) of Regulation (EU) No 909/2014, in respect of paragraphs 1, 4, 9, 13 and 14 of Article 89 and Article 90 of this Regulation;

(b) a CSD which receives a request from a participant, an issuer, a central counterparty (CCP) or a trading venue to have access to its services in accordance with Articles 33(2), 49(2) and 53(1) of Regulation (EU) No 909/2014 in respect of paragraphs 1 to 3, 5 to 8 and 10 to 14 of Article 89 and Article 90 of this Regulation;

(c) a CCP which receives a request from a CSD to have access to its transaction feeds in accordance with Article 53(1) of Regulation (EU) No 909/2014 in respect of Article 90 of this Regulation;

(d) a trading venue which receives a request from a CSD to have access to its transaction feeds in accordance with Article 53(1) of Regulation (EU) No 909/2014 in respect of Article 90 of this Regulation.

2. For the purposes of this Chapter, a requesting party shall include one of the following entities:

(a) a requesting CSD as defined in point (6) of Article 2(1) of Regulation (EU) No 909/2014 in respect of paragraphs 1, 4, 9 and 13 of Article 89 and Article 90 of this Regulation;

(b) a participant, an issuer, a CCP or a trading venue which requests access to the securities settlement system operated by a CSD or to other services provided by a CSD in accordance with Articles 33(2), 49(2) and 53(1) of Regulation (EU) No 909/2014 in respect of paragraphs 1 to 3, 5 to 8 and 10 to 14 of Article 89 and Article 90 of this Regulation;

(c) a CSD which requests access to the transaction feeds of a CCP in accordance with Article 53(1) of Regulation (EU) No 909/2014 in respect of Article 90 of this Regulation;

(d) a CSD which requests access to the transaction feeds of a trading venue in accordance with Article 53(1) of Regulation (EU) No 909/2014 in respect of Article 90 of this Regulation.

SECTION 1

Criteria justifying refusal of access

(Articles 33(3), 49(3), 52(2) and 53(3) of Regulation (EU) No 909/2014)

Article 89

Risks to be taken into account by CSDs and competent authorities

1. Where, in accordance with Articles 33(3), 49(3), 52(2) or 53(3) of Regulation (EU) No 909/2014, a CSD carries out a comprehensive risk assessment following a request for access by a requesting participant, an issuer, a requesting CSD, a CCP or a trading venue, as well as where a competent authority assesses the reasons for refusal by the CSD to provide services, they shall take into account the following risks resulting from access to the services of the CSD:

   (a) legal risks;

   (b) financial risks;

   (c) operational risks.

2. When assessing legal risks following a request for access by a requesting participant, a CSD and its competent authority shall take into account the following criteria:

   (a) the requesting participant is not able to comply with the legal requirements for participation in the securities settlement system operated by the CSD, or does not provide the CSD with the information necessary for the CSD to assess the compliance, including any required legal opinions or legal arrangements;

   (b) the requesting participant is not able to ensure, in accordance with the rules applicable in the home Member State of the CSD, the confidentiality of the information provided through the securities settlement system, or does not provide the CSD with the information necessary for the CSD to assess its ability to comply with those rules on confidentiality, including any required legal opinions or legal arrangements;

   (c) where a requesting participant is established in a third country, either of the following:

      (i) the requesting participant is not subject to a regulatory and supervisory framework comparable to the regulatory and supervisory framework that

would be applicable to the requesting participant if it were established in the Union:

(ii) the rules of the CSD concerning settlement finality referred to in Article 39 of Regulation (EU) No 909/2014 are not enforceable in the jurisdiction of the requesting participant.

3. When assessing legal risks following an issuer's request for recording its securities in the CSD in accordance with Article 49(1) of Regulation (EU) No 909/2014, the CSD and its competent authority shall take into account the following criteria:

(a) the issuer is not able to comply with the legal requirements for the provision of services by the CSD;

(b) the issuer is not able to guarantee that the securities have been issued in a manner that enables the CSD to ensure the integrity of the issue in accordance with Article 37 of Regulation (EU) No 909/2014.

4. When assessing legal risks following a request for access by a requesting CSD, the receiving CSD and its competent authority shall take into account the criteria set out in points (a), (b) and (c) of paragraph 2.

5. When assessing legal risks following a request for access by a CCP, a CSD and its competent authority shall take into account the criteria set out in points (a), (b) and (c) of paragraph 2.

6. When assessing legal risks following a request for access by a trading venue, a CSD and its competent authority shall take into account the following criteria:

(a) the criteria set out in point (b) of paragraph 2;

(b) where a trading venue is established in a third country, the requesting trading venue is not subject to a regulatory and supervisory framework comparable to the regulatory and supervisory framework applicable to a trading venue in the Union;

7. When assessing financial risks following a request for access by a requesting participant, a CSD and its competent authority shall take into account whether the requesting participant holds sufficient financial resources to fulfil its contractual obligations towards the CSD.

8. When assessing financial risks following an issuer's request for recording its securities in the CSD in accordance with Article 49(1) of Regulation (EU) No 909/2014, a CSD and its competent authority shall take into account the criterion set out in paragraph 7.

9. When assessing financial risks following a request for access by a requesting CSD, the receiving CSD and its competent authority shall take into account the criterion set out in paragraph 7.

10. When assessing financial risks following a request for access by a CCP or a trading venue, a CSD and its competent authority shall take into account the criterion set out in paragraph 7.

11. When assessing operational risks following a request for access by a requesting participant, a CSD and its competent authority shall take into account the following criteria:

(a) the requesting participant does not have the operational capacity to participate in the CSD;

(b) the requesting participant does not comply with the risk management rules of the receiving CSD, or it lacks the necessary expertise in that regard;

(c) the requesting participant has not put in place business continuity policies or disaster recovery plans;

(d) the granting of access requires the receiving CSD to undertake significant changes of its operations affecting its risk management procedures and endangering the smooth functioning of the securities settlement system operated by the receiving CSD, including the implementation of ongoing manual processing by the CSD.

12. When assessing operational risks following an issuer's request for recording its securities in the CSD in accordance with Article 49(1) of Regulation (EU) No 909/2014, a CSD and its competent authority shall take into account the following criteria:

(a) the criterion set out in point (d) of paragraph 11;

(b) the securities settlement system operated by the CSD cannot process the currencies requested by the issuer.

13. When assessing operational risks following a request for access by a requesting CSD, or a CCP, the receiving CSD and its competent authority shall take into account the criteria set out in paragraph 11.

14. When assessing the operational risks following a request for access by a trading venue, the receiving CSD and its competent authority shall take into account at least the criteria set out in point (d) of paragraph 11.

SECTION 2

Procedure for refusal of access

(Articles 33(3), 49(4), 52(2) and 53(3) of Regulation (EU) No 909/2014)

Article 90

Procedure

1. In the event of a refusal of access, the requesting party shall have the right to complain within one month from the receipt of the refusal to the competent authority of the receiving CSD, CCP or trading venue that has refused access to it in accordance with Articles 33(3), 49(4), 52(2) or 53(3) of Regulation (EU) No 909/2014.

2. The competent authority referred to in paragraph 1 may request additional information concerning the refusal of access from the requesting and receiving parties.

The responses to the request for information referred to in the first subparagraph shall be sent to the competent authority within two weeks from the date of the receipt of the request.

In accordance with Article 53(3) of Regulation (EU) No 909/2014, within two business days from the date of the receipt of the complaint referred to in paragraph 1, the competent authority of the receiving party shall transmit the complaint to the relevant authority referred to in point (a) of Article 12(1) of Regulation (EU) No 909/2014 from the Member State of the place of establishment of the receiving party.

3. The competent authority referred to in paragraph 1 shall consult the following authorities on its initial assessment of the complaint within two months from the date of the receipt of the complaint, as appropriate:

   (a) the competent authority of the place of establishment of the requesting participant in accordance with Article 33(3) of Regulation (EU) No 909/2014;

   (b) the competent authority of the place of establishment of the requesting issuer in accordance with Article 49(4) of Regulation (EU) No 909/2014;

   (c) the competent authority of the requesting CSD and the relevant authority referred to in point (a) of Article 12 of Regulation (EU) No 909/2012 responsible for the oversight of the securities settlement system operated by the requesting CSD in accordance with Articles 52(2) and 53(3) of Regulation (EU) No 909/2014;

   (d) the competent authority of the requesting CCP or trading venue in accordance with Article 53(3) of Regulation (EU) No 909/2014 and the relevant authority referred to in point (a) of Article 12(1) of Regulation (EU) No 909/2014 responsible for the oversight of the securities settlement systems in the Member State where the requesting CCP and trading venues are established in accordance with Article 53(3) of Regulation (EU) No 909/2014.

4. The authorities referred to in points (a) to (d) of paragraph 3 shall respond within one month from the date of the request for consultation specified in paragraph 3. Where an authority referred to in points (a) to (d) of paragraph 3 does not provide its opinion within that time-limit, it shall be deemed to have a positive opinion on the assessment provided by the competent authority referred to in paragraph 3.

5. The competent authority referred to in paragraph 1 shall inform the authorities referred to in points (a) to (d) of paragraph 3 of its final assessment of the complaint within two weeks from the time-limit provided in paragraph 4.

6. Where one of the authorities referred to in points (a) to (d) of paragraph 3 disagrees with the assessment provided by the competent authority referred to in paragraph 1, any of them may refer the matter to ESMA within two weeks from the date when the competent authority referred to in paragraph 1 provides the information concerning its final assessment of the complaint in accordance with paragraph 5.

7. When the matter has not been referred to ESMA, the competent authority referred to in paragraph 1 shall send a reasoned reply to the requesting party within two working days from the time-limit provided in paragraph 6.

   The competent authority referred to in paragraph 1 shall also inform the receiving party and the authorities referred to in points (a) to (d) of paragraph 3 of the reasoned reply referred to in the first subparagraph of this paragraph within two working days from the date where it sends the reasoned reply to the requesting party.

8. In the event of a referral to ESMA referred to in paragraph 6, the competent authority referred to in paragraph 1 shall inform the requesting party and the receiving party of the referral within two working days from the date where the referral has been made.

9. Where the refusal by the receiving party to grant access to the requesting party is deemed to be unjustified following the procedure provided for in paragraphs 1 to 7, the competent authority referred to in paragraph 1 shall, within two weeks from the time-limit specified in paragraph 7, issue an order requiring that receiving party to grant access to the requesting party within three months from the date when the order enters into force.

The time-limit referred to in the first subparagraph shall be extended to eight months in case of customised links that require significant development of IT tools, unless otherwise agreed by the requesting and receiving CSDs.

The order shall include the reasons why the competent authority referred to in paragraph 1 concluded that the refusal by the receiving party to grant access was unjustified.

The order shall be sent to ESMA, the authorities referred to in points (a) to (d) of paragraph 3, the requesting party and the receiving party within two working days after the date when it enters into force.

10. The procedure referred to in paragraphs 1 to 9 shall also apply when the receiving party intends to withdraw access to a requesting party to whom it already provides its services.

CHAPTER XIV

AUTHORISATION TO PROVIDE BANKING TYPE OF ANCILLARY SERVICES

(Article 55(1) and (2) of Regulation (EU) No 909/2014)

Article 91

CSDs offering banking-type ancillary services themselves

An application for authorisation in accordance to point (a) of Article 54(2) of Regulation (EU) No 909/2014 shall include the following information:

(a) a copy of the decision of the management body of the applicant CSD to apply for authorisation and the minutes from the meeting where the management body approved the content of the application file and its submission;

(b) the contact details of the person responsible for the application for authorisation, where that person is not the one submitting the application for authorisation referred to under Article 17 of Regulation (EU) 909/2014;

(c) evidence that proves the existence of an authorisation referred to in point (a) of Article 54(3) of Regulation (EU) No 909/2014;

(d) evidence that the applicant CSD meets the prudential requirements referred to in Article 59(1), (3) and (4) of Regulation (EU) No 909/2014 and the supervisory requirements referred to in Article 60 of that Regulation;

(e) evidence, containing any relevant documents including articles of incorporation, financial statements, audit reports, reports from risk committees, which proves that the applicant CSD complies with point (d) of Article 54(3) of Regulation (EU) No 909/2014;

(f) details concerning the recovery plan referred to in point (f) of Article 54(3) of Regulation (EU) No 909/2014;

(g) a programme of operations that fulfils the following conditions:

(i) it includes a list of the banking-type ancillary services referred to in Section C of the Annex to Regulation (EU) No 909/2014 that the CSD intends to provide;

(ii) it includes an explanation of how the banking-type ancillary services referred to in Section C of the Annex to Regulation (EU) No 909/2014 are directly related to any core or ancillary services referred to in Sections A and B of the Annex to Regulation (EU) No 909/2014 that the CSD is authorised to provide;

(iii) it is structured following the list of banking-type ancillary services referred to in Section C of the Annex to Regulation (EU) No 909/2014;

(h) evidence supporting the reasons for not settling the cash payments of the CSD's securities settlement system through accounts opened with a central bank of issue of the currency of the country where the settlement takes place;

(i) detailed information on the arrangements which ensure that the provision of banking-type ancillary services intended to be provided does not affect the smooth provision of the core CSD services referred to in Section A of the Annex to Regulation (EU) No 909/2014, including:

(i) the IT platform used for the settlement of the cash leg of securities transactions, including an overview of the IT organisation and an analysis of the related risks and how they are mitigated;

(ii) the operation and legal arrangements of the DVP process and, in particular, the procedures used to address the credit risk resulting from the settlement of the cash-leg of securities transactions;

(iii) the selection, monitoring, legal documentation and management of interconnections with any other third parties involved in the process of cash transfers, in particular the relevant arrangements with third parties involved in the process of cash transfers;

(iv) the detailed analysis contained in the recovery plan of the applicant CSD of regarding any impact of the provision of banking-type ancillary services on the provision of core CSD services;

(v) the disclosure of possible conflicts of interests in the governance arrangements resulting from the provision of banking-type ancillary services, and the measures taken to address them.

Article 92

CSDs offering banking-type ancillary services through a designated credit institution

An application for authorisation in accordance with point (b) of Article 54(2) of Regulation (EU) No 909/2014 shall contain the following information:

(a) a copy of the decision of the management body of the applicant CSD to apply for authorisation and the minutes from the meeting where the management body approved the content of the application file and its submission;

(b) the contact details of the person responsible for the application for authorisation, where the person is not the same person as the one submitting the application for authorisation referred to in Article 17 of Regulation (EU) No 909/2014;

(c) the corporate name of the credit institution to be designated in accordance with point (b) of Article 54(2) of Regulation (EU) No 909/2014, its legal status and registered address in the Union;

(d) evidence that the credit institution referred to in point (c) has obtained an authorisation referred to in point (a) of Article 54(4) of Regulation (EU) No 909/2014;

(e) the articles of incorporation and other relevant statutory documentation of the designated credit institution;

(f) the ownership structure of the designated credit institution, including the identity of its shareholders;

(g) the identification of any common shareholders of the applicant CSD and the designated credit institution and any participations between the applicant CSD and the designated credit institution;

(h) evidence that the designated credit institution meets the prudential requirements referred to in Article 59(1), (3) and (4) of Regulation (EU) No 909/2014 and the supervisory requirements referred to in Article 60 of that Regulation;

(i) evidence, including a memorandum of association, financial statements, audit reports, reports from risk committees, or other documents, which proves that the designated credit institution complies with point (e) of Article 54(4) of Regulation (EU) No 909/2014;

(j) the details of the recovery plan referred to in point (g) of Article 54(4) of Regulation (EU) No 909/2014;

(k) a programme of operations that fulfils the following conditions:

  (i) it includes a list of the banking-type ancillary services referred to in Section C of the Annex to Regulation (EU) No 909/2014 that the designated credit institution intends to provide;

  (ii) it includes an explanation of how the banking-type ancillary services referred to in Section C of the Annex to Regulation (EU) No 909/2014 are directly related to any core or ancillary services referred to in Sections A and B of the Annex to Regulation (EU) No 909/2014 that the applicant CSD is authorised to provide;

  (iii) it is structured following the list of banking-type ancillary services referred to in Section C of the Annex to Regulation (EU) No 909/2014;

(l) evidence supporting the reasons for not settling the cash payments of the CSD's securities settlement system through accounts opened with a central bank of issue of the currency of the country where the settlement takes place;

(m) detailed information concerning the following aspects of the relation between the CSD and the designated credit institution:

(i) the IT platform used for the settlement of the cash leg of securities transactions, including an overview of the IT organisation and an analysis of the related risks and how they are mitigated;

(ii) the applicable rules and procedures that ensure compliance with the requirements concerning settlement finality referred to in Article 39 of Regulation (EU) No 909/2014;

(iii) the operation and the legal arrangements of the DVP process, including the procedures used to address the credit risk resulting from the cash-leg of a securities transaction;

(iv) the selection, monitoring and management of the interconnections with any other third parties involved in the process of cash transfers, in particular the relevant arrangements with third parties involved in the process of cash transfers;

(v) the service level agreement establishing the details of functions to be outsourced by the CSD to the designated credit institution or from the designated credit institution to the CSD and any evidence that demonstrates compliance with the outsourcing requirements set out in Article 30 of Regulation (EU) No 909/2014;

(vi) the detailed analysis contained in the recovery plan of the applicant CSD about any impact of the provision of banking-type ancillary services on the provision of core CSD services;

(vii) the disclosure of possible conflicts of interests in the governance arrangements resulting from the banking-type ancillary services, and the measures taken to address them;

(viii) evidence that demonstrates that the credit institution has the necessary contractual and operational ability to have prompt access to the securities collateral located in the CSD and related to the provision of intraday credit and, as the case may be, short term credit.

Article 93

Specific requirements

1. Where the CSD applies for authorisation to designate more than one credit institution to provide banking-type ancillary services, its application shall include the following information:

(a) the information referred to Article 91 for each of the designated credit institution;

(b) a description of the role of each designated credit institution and the relations between them.

2. Where the application to be authorised in accordance with point (a) or (b) of Article 54(2) of Regulation (EU) No 909/2014 is submitted after the authorisation referred to in Article 17 of that Regulation has been obtained, the applicant CSD shall identify and inform the competent authority of substantive changes referred to in Article 16(4) of Regulation (EU) No 909/2014 unless it has already provided the

information in the process of review and evaluation referred to in Article 22 of that Regulation.

Article 94

Standard forms and templates for the application

1. An applicant CSD shall provide an application for the authorisations referred to in points (a) and (b) of Article 54(2) of Regulation (EU) No 909/2014 in the format provided in Annex III to this Regulation.
2. An applicant CSD shall submit the application referred to in paragraph 1 in a durable medium.
3. An applicant CSD shall provide a unique reference number for each document that it submits in the application referred to in paragraph 1.
4. An applicant CSD shall ensure that the information submitted in the application referred to in paragraph 1 clearly identifies to which specific requirement of this Chapter that information refers to and in which document that information is provided.
5. An applicant CSD shall provide its competent authority with a list of all the documents provided in the application referred to in paragraph 1 accompanied by their reference number.
6. All information shall be submitted in the language indicated by the competent authority. The competent authority may ask the CSD to submit the same information in a language customary in the sphere of international finance.

CHAPTER XV

FINAL PROVISIONS

Article 95

Transitional provisions

1. Information referred to in Article 17(2) of this Regulation, shall be provided to the competent authority at the latest six months before the date referred to in Article 96(2).
2. Information referred to in Article 24(2) of this Regulation shall be provided to the competent authority at the latest six months before the date referred to in Article 96(2).
3. Information referred to in points (j) and (r) of Article 41 and in points (d), (f), (h), (i), and (j) of Article 42(1) of this Regulation shall be provided from the date referred to in Article 96(2).

Article 96

Entry into force and application

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. Article 54 shall apply from the date of entry into force of the delegated acts adopted by the Commission pursuant to Articles 6(5) and 7(15) of Regulation (EU) No 909/2014, whichever is the later.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 11.11.2016

For the Commission
The President
Jean-Claude JUNCKER