



Disclosure Framework

CPI IOSCO 2020

Self- Assessment Euroclear Sweden AB – June 2021

Reference information

Document owner	Head of Legal & Corporate Affairs
Key contact(s)	Legal & Corporate Affairs
Version	V 2.0
CSDR reference	B3002-3
Approved by and date of approval	ES CEO 1 st June 2021
Next revision	2022-12-31
Applicable from	2021-01-01
Applicable to	N/A

Euroclear Sweden Disclosure

Responding institution: Euroclear Sweden AB ("Euroclear Sweden" or "ES")

Jurisdiction(s) in which the financial market infrastructure ("FMI") operates: Sweden

Authorities regulating, supervising or overseeing the FMI: The Swedish Financial Supervisory Authority (SFSA) and the Swedish Riksbank.

The date of this disclosure is 31/12/2020

This disclosure can also be found at www.euroclear.com/sweden

For further information, please contact: esw.legal@euroclear.com

Table of contents

Reference information	2
I. EXECUTIVE SUMMARY	4
II. SUMMARY OF MAJOR CHANGES SINCE THE LAST UPDATE OF THE DISCLOSURE.....	4
III. GENERAL BACKGROUND ON THE FMI.....	5
General description of the FMI and the markets it serves	5
The clearing and settlement landscape	5
Legal and regulatory framework	7
General organisation of the FMI.....	7
IV. PRINCIPLE-BY-PRINCIPLE SUMMARY NARRATIVE DISCLOSURE	10
Principle 1: Legal basis.....	11
Principle 2: Governance	17
Principle 3: Framework for the comprehensive management of risks	30
Principle 4: Credit risk.....	40
Principle 7: Liquidity risk	41
Principle 8: Settlement finality.....	44
Principle 9: Money Settlements	47
Principle 11: Central securities depositories.....	49
Principle 12: Exchange-of-value settlement systems	52
Principle 13: Participant-default rules and procedures.....	53
Principle 15: General business risk.....	55
Principle 16: Custody and investment risks	61
Principle 17: Operational risk.....	65
Principle 18: Access and participation requirements	81
Principle 19: Tiered participation arrangements	85
Principle 20: FMI links.....	88
Principle 21: Efficiency and effectiveness.....	91
Principle 22: Communication procedures and standards.....	93
Principle 23: Disclosure of rules, key procedures, and market data.....	95
V. LIST OF PUBLICLY AVAILABLE RESOURCES.....	99

I. EXECUTIVE SUMMARY

This document, produced during the second quarter of 2021, contains the disclosures relating to the CPMI-IOSCO self-assessment of Euroclear Sweden AB ("**ES**" or "Euroclear **Sweden**") and its activities as of 31 December 2020.

ES is licensed to operate as a central securities depository according to the CSD Regulation (EU no 909/2014)¹ ("**CSDR**").

ES operates the VPC system, a settlement system approved by the Swedish Financial Supervisory Authority ("**SFSA**"), and offers initial recording of securities in a book-entry system to issuers and provides and maintain securities accounts at the top tier level.

Services include clearing and settlement of securities, corporate action processing, account and asset management, funds order routing and issuer services such as shareholder meeting services. Additionally, ES provides shareholder information services and information on securities and corporate actions to the market. ES serves approximately 40 participants and close to 1 850 issuers.

The main risk type for ES is operational risk. The framework in place allows ES to track its full range of risks and to present a consolidated view of the risks to management, CEO, risk committee and to the Board.

The Disclosure Framework shows that ES adheres to international standards and market practice and is sufficiently efficient and effective in meeting the requirements of its participants and the markets it serves.

ES has appropriate clear and transparent rules and procedures in place to run its operations, support the stability of the broader financial system and to monitor, manage and minimize the risks involved. A clear business continuity management exists and ES has a profound set of policies, procedures, and controls to support its operations.

II. SUMMARY OF MAJOR CHANGES SINCE THE LAST UPDATE OF THE DISCLOSURE

Since the last update of this document, ES has launched both the changes needed to be compliant with CSDR, and the adaptation needed to handle issuance, payments and settlement in the Danish Krona for Exchange traded products, according to plan (2019). ES is currently adapting the system to comply with the last phase of the CSDR framework, i.e. the Settlement Discipline Regime² ("**SDR**"), which covers penalties and buy ins, and which will enter into force in February 2022. ES is also in the process of adapting the system regarding how payments (dividend etc) are distributed and the plan is to launch the new process during Q3 2022.

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 Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012

² Commission Delegated Regulation (EU) 2018/1229 of 25 May 2018 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on settlement discipline

III. GENERAL BACKGROUND ON THE FMI

General description of the FMI and the markets it serves

Euroclear Sweden has been the Swedish central securities depository ("CSD") since 1971. Euroclear Sweden is part of the Euroclear group which also includes Euroclear Bank, Euroclear Belgium, Euroclear Finland, Euroclear France, Euroclear Nederland and Euroclear UK & Ireland.

As the Swedish central securities depository and clearing organisation, Euroclear Sweden provides post-trade services to domestic and foreign clients. Services include register services, clearing and settlement of securities, corporate action processing, account and asset management, funds order routing and issuer services such as shareholder meeting services. Additionally, ES provides shareholder information services and information on securities and corporate actions to the market. Euroclear Sweden offers both nominee and owner accounts, allowing direct securities holding in the CSD for both professional and retail investors and their intermediaries. A large portion of the financial instruments existing on the Swedish market are registered and settled in the Euroclear Sweden technical system, the VPC system. Both Swedish and foreign instruments are handled in the VPC system and Euroclear Sweden has passported, according to CSDR (as further described under "Legal and regulatory framework" below), its authorisation to, Germany, Denmark, Finland and France. Euroclear Sweden is also under the United Kingdom ("UK") transitional regime to provide services in the UK and is in the process of applying to the Bank of England for a permanent recognition to provide services in the UK. Moreover, Euroclear Sweden also maintains direct and indirect international links for the settlement of cross-border transactions in foreign securities.

All activities related to securities settlement are based entirely on automatic data processing in the VPC system and communication is carried out by means of encrypted and secure messages between Euroclear Sweden and the various participants via networks approved by Euroclear Sweden.

General statistics by Q4 2020:

- Number of Issuers: approx. 1850
- Number of Participants: approx. 40
- Number of Securities accounts: approx. 700 thousand

The clearing and settlement landscape

Euroclear Sweden provides i) notary services; ii) central maintenance services (direct and nominee accounts); and iii) settlement services, all which are considered core services for a CSD under CSDR. Euroclear Sweden makes a distinction in the settlement process between equity (AM sub-market) and money market (PM sub-market). Settlement is available in financial instruments such as equities, fixed income, exchange traded funds and warrants. Transactions originate from regulated markets, multilateral trading facilities or over the counter trades. Euroclear Sweden operates a Bank for International Settlement (BIS) model 1 system i.e. a system that settles instructions on a gross basis, trade by trade servicing participants, such as Nordic Banks, local broker dealers credit institutions, investment banks, fund managers and CCPs.

Euroclear Sweden's clearing and settlement aims at guaranteeing clearing members³ a final and irrevocable settlement by means of delivery versus payment ("**DvP**"). This means, amongst other things, that no clearing member risks delivering to another clearing member without receiving payment, and vice versa.

For settlement in central bank money in Swedish kronor, the Riksbank has commissioned Euroclear Sweden to administer settlement accounts that are included in the Riksbank's system for the settlement of payment obligations. The Riksbank and Euroclear Sweden have reached an agreement concerning more detailed terms in relation to Euroclear Sweden's administration of the liquidity settlement accounts and the granting of credit in relation to these. The settlement of securities applies to all securities that are registered in the VPC-system pursuant to the Swedish CSD and Financial Instruments Account Act (1998:1479) ("**Financial Instruments Account Act**"). Settlement may currently take place in Swedish kronor ("**SEK**"), Euros ("**EUR**") or Danish kronor ("**DKK**").

For the settlement in EUR or DKK, Euroclear Sweden has opened a client fund account at Bank of Finland (EUR) and Denmark's Nationalbank (DKK) on behalf of the settlement banks. The holdings on those accounts are mirrored on each settlement banks liquidity settlement account ("**LSA**") in Euroclear Sweden. For EUR and DKK, the cash accounts in the VPC-system are to be seen as memorandum accounts.

Settlement figures by year end 2020:

Data for full year 2020	Equity	Fixed Income
Number of transactions	14,404,306	298,174
Settled value – MSEK	14,773,412	86,775,646
Settlement ratio - transactions	95.41%	98.80%
Settlement ratio - value	88.14%	99.72%

³ A clearing member is an undertaking, which has received authorisation from Euroclear Sweden to participate in clearing operations.

Legal and regulatory framework

As a regulated FMI, Euroclear Sweden is supervised by the SFSA and the Riksbank. Euroclear Sweden is currently licensed to operate as a central securities depository pursuant to CSDR.

Moreover, the Financial Instruments Accounts Act contains provisions regarding the registration in Swedish CSD registers and book entry accounts of ownership and special rights to shares and other financial instruments. In accordance with applicable regulatory and legal framework, Euroclear Sweden supervises that the ES General Terms and Conditions Account operations and Clearing ("**ES Account Rules**"), as well as the ES Rules for Issuers and Issuer Agents ("**ES Issuer Rules**") are complied with. ES Account Rules and ES Issuer Rules are together referred to as "ES Rules". In order to fulfil its supervisory obligations, Euroclear Sweden has e.g. the right to obtain information from its participants.

The VPC-system is registered with the European Commission in accordance with the Swedish Act on Systems for the Settlement of Obligations on the Financial Market (SFS 1999:1309). This Act is based on the Settlement Finality Directive (1998/26/EU)). Euroclear Sweden is also under a temporary regime in relation to settlement finality rules in the UK and is under the process of applying to the Bank of England for the VPC system to be regarded as a designated system under the UK rules on settlement finality.

General organisation of the FMI

Euroclear Holding SA/NV, incorporated in Belgium, is the ultimate holding company of the Euroclear group. It owns Euroclear SA/NV ("**ESA**"), a Belgian financial holding company, which is the parent company of the operational group (I)CSD's, including Euroclear Sweden. ESA acts as the Group service company.

The Euroclear group consists of Euroclear France, Euroclear Nederland, Euroclear Sweden, Euroclear UK & Ireland, Euroclear Finland and Euroclear Belgium as well as the International CSD Euroclear Bank.

Euroclear Sweden's governance requirements are set out in CSDR, as well as Swedish company laws and other Swedish legal and regulatory recommendations. In accordance with the Swedish Companies Act (SFS 2005:551), the Board of Directors of Euroclear Sweden is responsible for the organisation of the company and the management of the company's affairs and for the appropriate arrangement of the control of e.g. the company accounts and finances. Moreover, Euroclear Sweden must also comply with the governance requirements stipulated in CSDR regarding independency of board members, board committees etc.

The Chief Executive Officer ("**CEO**") handles the day-to-day management of Euroclear Sweden's affairs in accordance with the Swedish Companies Act and the Board's guidelines and instructions. An Executive Committee consisting of the CEO and the operational managers of the main functions within Euroclear Sweden has been established under the responsibility of the CEO. The organisation includes IT, Business Operations, Commercial, Product Management and Support functions.

The current structure of the Euroclear group is presented on ES web site.

System design and operations - Settlement process

ES offers two types of settlement:

- Gross settlement at certain pre-determined points in time (Designated Time Gross Settlement – “**DTGS**”)
- Gross settlement in real time (Real Time Gross Settlement – “**RTGS**”)

The settlement process covers the four steps which are briefly outlined below;

1. Input of transfer order

The settlement process is initiated when a transfer order is sent to the VPC System.

2. Matching

Once both the purchasing and the selling clearing members have entered their respective transfer orders in the system, a matching of the instructions is normally required for the settlement process to continue.

3. Assuring delivery and payment capacity

For settlement to take place, it is necessary for ES to carry out a pre-settlement check. This is a check to confirm that the clearing members have delivery (seller) or payment (buyer) capacity.

4. Settlement moment

Settlement takes place when the securities are finally credited to the accounts specified by the purchasing clearing member and this is the final stage in the settlement process. At the same time the same amount and type of securities are debited to those accounts specified by the selling clearing member and cash being credited to the seller.

This settlement timetable specifies the times when settlement takes place with delivery versus payment cycles at 08.00 (only PM market), 10.00, 12.00 and 14.00 hours with one last free of payment cycle at 17.00 hours.

Instructions not settled in the first settlement cycle will instead be assessed for ‘ready to settle’ marking and settlement in subsequent cycles. Instructions that have not been possible to settle in any of the settlement cycles will receive the status ‘not settled’ has to be entered once again for settlement on the following day.

Gross settlement (RTGS instructions) with payment may occur at any time between 07.00-17.00 hours, i.e. while the RIX system is open.

Settlement headroom

Settlement headroom constitutes the amount available which can be used as payment capacity in conjunction with a pre-settlement check. Settlement headroom comprises two parts with one part made available before the settlement process starts. For clearing members this part is defined by limits set by the settlement bank whereas for settlement banks this part consists of central bank funds allocated for securities settlement. The second part of the settlement headroom is created within the framework of the settlement process in conjunction with the ‘ready to settle’ marking of

instructions, i.e. the net total of 'ready to settle' instructions.

A settlement day

The gross settlement system supports different technical netting functionalities in order to optimize the process. Upon start of the settlement day one major technical netting is performed with several limited functionalities operating on continuous basis. Four batches are run in the equity sub-market and five batches in the fixed income sub-market. In the batch securities capacity and payment capacity is checked gross in real-time parallel with technical netting processes (simultaneous instruction processing). If securities and payment capacity is in place, the transaction (deliver and receive instructions) are marked 'ready to settle'. When the settlement point in time is reached all the instructions marked 'ready to settle' will be marked as 'settled' and finality is obtained. A transaction is irrevocable from a settlement perspective when the instruction is marked 'ready to settle'. Then it is just a matter of time for the instructions to be final, i.e. an instruction marked 'ready to settle' will always be settled.

Settlement is obtained by debiting or crediting those VPC accounts specified by the clearing member. At the same time, a debit or credit is made on the relevant liquidity settlement accounts and cash memorandum accounts.

IV. PRINCIPLE-BY-PRINCIPLE SUMMARY NARRATIVE DISCLOSURE

Assessment Category	Principle
Observed	1, 2, 4, 7, 8, 9, 11, 12, 13, 15, 16, 17, 18, 20, 21, 22, 23
Broadly Observed	3
Partly Observed	19
Not Observed	
Not Applicable	5, 6, 10, 14, 24

Principle 1: Legal basis

An FMI should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions.

Key consideration 1: The legal basis should provide a high degree of certainty for each material aspect of an FMI's activities in all relevant jurisdictions.

Material aspects

The following material aspects for Euroclear Sweden's activities require a high degree of legal certainty:

- Regulatory framework - the existence of an adequate authorisation and supervision, from a regulatory point of view;
- Asset protection - the protection of the holdings of financial instruments of the clients in the books of Euroclear Sweden;
- Dematerialisation - legal basis for dematerialisation of securities;
- Finality – the settlement finality of securities and cash;
- Contractual framework – the material aspects of the services and activities of Euroclear Sweden
- Default procedures – the rules concerning default situations.

The most relevant legal jurisdiction for all the above material aspects of Euroclear Sweden activities is Sweden, being the location of the securities settlement system operated by Euroclear Sweden. From an asset protection point of view, all jurisdictions where financial instruments are held through links are also relevant. The actual location or place of incorporation of clients is also relevant in case of insolvency or resolution proceedings affecting those clients as well as the governing law of certain agreements.

The relevant contractual framework for Euroclear Sweden's operations are the ES Rules. ES Account Rules govern the rights and obligations of a clearing member or other participant who enters into an accession agreement with ES and set forth detailed rules and procedures with respect to the VPC-system, while the ES Issuer Rules govern the rights and obligations for issuers and issuer agents who enter into an affiliation agreement with ES. The accession agreements and affiliation agreements, respectively, are private law contracts governed by Swedish law. The process through which the ES Rules have been prepared and are continuously revised (as described below) provides a high degree of legal certainty for these rules.

Regulatory framework

CSDR

CSDR has introduced new measures for the authorisation and supervision of EU CSDs and sets out to create a common set of prudential, organisational, and conduct of business standards at a European level, including the introduction of a securities settlement discipline regime. This harmonise operational aspects of securities settlement, including the possibility to settle instructions partially mandatory buy- ins; and cash penalties, to prevent and address settlement fails.

CSDR also stipulates that CSDs should have publicly disclosed, transparent, objective and non-discriminatory criteria for participation in the securities settlement system, which would allow restriction of access by participants only on the basis of the risks involved.

CSDR also stipulates that CSDs need to apply for authorisation from their national competent authorities.

Swedish Act on Systems for the Settlement of Obligations on the Financial Market

The VPC system has been designated in accordance with the Swedish Act on Systems for the Settlement of Obligations on the Financial Market (SFS 1999:1309) which transposes the Settlement Finality Directive (1998/26/EC) and has thus been approved by the SFSA and registered with the European Commission. An administrator of a settlement system shall according to the aforesaid act establish satisfactory joint rules and standardized arrangements to execute transfer orders as well as rules which states that Swedish law is applicable.

The Financial Instruments Account Act

The Financial Instruments Account Act contains provisions regarding the registration in Swedish CSD registers and book entry accounts of ownership and special rights to shares and other financial instruments. The act aims to ensure that ES conducts its operations in such a manner as to ensure that it satisfies stringent requirements of security and efficiency, maintain public confidence in the book-entry system and to ensure that the interests of individuals are not jeopardised. The act also contains rules regarding free access and neutrality.

Euroclear Sweden's supervision

In accordance with applicable regulatory and legal framework, ES supervises that the ES Account Rules are complied with. In order to fulfil its obligations, ES has e.g. the right to acquire information from the participants.

Asset protection

Euroclear Sweden's handling of dematerialised financial instruments is governed by the Financial Instruments Account Act. This Act contains provisions regarding the registration in Swedish CSD registers of ownership and special rights to shares and other financial instruments. The Swedish CSD registers comprise of Swedish CSD book-entry accounts opened for owners of financial instruments which are registered in accordance with said Act. Such accounts are held by financial firms who are authorised by Euroclear Sweden to act as nominees, i.e. on nominee accounts. Such registers and accounts are maintained in dematerialised form with the assistance of automated processing in the

VPC-system. According to the Swedish Financial Instruments Account Act, a person who is listed as the owner or nominee on a Swedish CSD book-entry account shall, subject to the limitations set forth in the account, be deemed to have the right to dispose of the financial instruments. The two types of accounts in the VPC- System – owner and nominee accounts – therefore have a clear basis in Swedish law.

The transfer of securities between accounts is enabled by an account operator who has been granted the right by ES to effect registration measures in the VPC system. These transfers are legally binding in relation to third parties as stipulated in the Financial Instruments Account Act and the Swedish Act on Systems for the Settlement of Obligations on the Financial Market.

Dematerialisation

The handling of dematerialised financial instruments is supported and governed by the Financial Instruments Account Act. Share certificates or comparable documents may not be issued with regard to financial instruments registered pursuant to the Financial Instruments Accounts Act. Where such documents have been issued, such documents shall not constitute evidence of a legal obligation. The process for dematerialisation of securities is further specified in ES Rules for Issuers and Issuer Agents.

However, for financial instruments issued in a country other than Sweden, the Act states that there is an option for the CSD to immobilise the security, if it is lodged for safekeeping before registration in a Swedish CSD book-entry account takes place. The document must be held in such safekeeping for as long as the instrument is registered in a Swedish CSD register.

Finality

ES aims at guaranteeing clearing members a final and irrevocable settlement by means of delivery against payment (DVP). This means, amongst other things, that no clearing member risks delivering to another clearing member without receiving payment, and vice versa. The settlement of payment takes place in central bank money in SEK. For settlement in central bank money in Swedish kronor, the Riksbank has commissioned ES to administer accounts that are included in the Riksbank's system (the RIX-System) for the settlement of payment obligations. Settlement may take place in Swedish kronor, Euros or Danish Kronor. For settlement in EUR/DKK the process is identical but instead of an integrated model, as in SEK, ES holds a cash account for clients at Bank of Finland and at Denmark's Nationalbank via which the settlement banks transfer cash. All cash holdings in EUR in the VPC system, are backed by the holding on this account.

As mentioned above, the VPC system is a designated system under the EU Settlement Finality Directive and the Swedish Act on Systems for the Settlement of Obligations on the Financial Market. In accordance with said act, transfer orders in the VPC-system remain applicable to third parties even if a collective bankruptcy proceeding has been initiated as regards an ES participant. This assumes that such an order has been entered into the system before the announcement of the decision to initiate bankruptcy proceedings. An order may not be revoked by a participant in the VPC System or by a third party after the time stipulated in ES Account Rules.

Participants can generally feel confident that no other participant or external party can hinder the settlement of a transfer order once it has been entered into the VPC-system. Although the fact that

a particular transfer order is protected and irrevocable does not guarantee actual settlement. Settlement remains dependent on a number of factors, including availability of cash and/or securities. It is also important to note that the Swedish Act on Systems for the Settlement of Obligations on the Financial Market does not regulate the validity of the underlying transaction, only circumstances on the system level.

The VPC system is a gross settlement system in which the system processes each transaction separately, but ES has implemented a technical netting function to reduce the liquidity needs of the participants. This is a technical function and cannot legally be considered netting. Four batches are run in the equity sub-market and five batches in the fixed income sub-market. In the batch securities capacity and payment capacity is checked gross in real-time, in parallel with technical netting processes (simultaneous instruction processing). If securities and payment capacity is in place, the transaction (deliver and receive instructions) are marked "ready to settle". When the settlement point in time is reached all the instructions marked 'ready for settlement' will be marked as 'settled' and finality is obtained. A transaction is irrevocable from a settlement perspective when the instruction is marked 'ready to settle'. Then it is just a matter of time for the instructions to be final, i.e. an instruction marked "ready to settle" will always be settled.

Although ES process instructions in "batch" cycles, ES do not use netting per se as ES operates a gross settlement system, both from a securities and a payments perspective, i.e. unwinding can never take place.

As mentioned above, the VPC system is also under a temporary regime to be regarded as a designated system under settlement finality rules in the UK and Euroclear Sweden is under the process of applying to the Bank of England for the VPC system to be regarded as a designated system in the UK.

Default procedures

As noted above, the Swedish Act on Systems for the Settlement of Obligations states that a transfer order must be entered into the settlement system before the announcement of the decision to initiate bankruptcy proceedings. ES Rules clearly defines that ES has the right to determine that participation of a Clearing Member or Settlement Bank shall cease in case bankruptcy or when other proceedings of a comparable nature have been initiated. Any further transfer orders from that participant will be rejected.

Key consideration 2: An FMI should have rules, procedures, and contracts that are clear, understandable, and consistent with relevant laws and regulations.

ES Rules were originally drafted in close consultation with market participants and aspects of ES Rules were subject to legal opinions by external experts in the field of securities law. They have thereafter been updated to reflect e.g. operational and legislative changes and an oversight is carried out on a

regular basis by in-house legal counsels as well as by operational staff who work with ES Rules on a daily basis. When necessary, ES obtains legal opinions from external legal counsel on changes in ES Rules. Each update to ES Rules is preceded by a formalised consultation process, which is further described under Principle 23.

ES has standard agreements for affiliation of participants and issuers, respectively. The standard accession agreements for participants are included in ES Account Rules and are therefore updated following the procedure for updating the ES Account Rules. The standard agreements for issuers are reviewed regularly by in-house counsel and changes to the documents are made when needed. ES Account Rules form part of the accession agreements with participants and ES Issuer Rules form part of the affiliation agreements with issuers, as well as issuer agents.

Key consideration 3: An FMI should be able to articulate the legal basis for its activities to relevant authorities, participants, and, where relevant, participant’s customers, in a clear and understandable way.

Euroclear Sweden has a clear and understandable legal framework that is publicly available via the Euroclear website. The legal basis for the activity of Euroclear Sweden is essentially articulated in the following documents:

- ES Account Rules, which are published on Euroclear Sweden’s website.
- Various explanatory documentation, which is also available on Euroclear Sweden’s website.
- This Disclosure framework in a public version, available on Euroclear Sweden’s website.

Key consideration 4: An FMI should have rules, procedures, and contracts that are enforceable in all relevant jurisdictions. There should be a high degree of certainty that actions taken by the FMI under such rules and procedures will not be voided, reversed, or subject to stays.

Enforceability of rules, procedures and contracts

In order to achieve legal certainty on that the rules, procedures and contracts related to ES operations are enforceable in all relevant jurisdictions, all participants and issuers with a domicile other than Sweden are required to provide a legal opinion as part of the affiliation process. The legal opinion must be drawn up by a legal expert independent of the applicant and must confirm the validity and enforceability of the applicable set of rules in the applicant’s country of domicile, as well as the possibility of enforcing a Swedish court decision or a Swedish arbitration decision in the applicant’s country of domicile.

According to the ES Account Rules the participants of Euroclear Sweden shall notify Euroclear Sweden without delay of any material information of which they become aware and which may affect their right to act as an account operator, nominee, clearing member or settlement bank. In the case of foreign companies (participants or issuers), these must immediately notify Euroclear Sweden of any amendments in legislation or other statutes or any decisions by court or other governmental

authorities which affect the application of the ES Rules or applicable Swedish law in the company's home country. Similar provisions apply in the ES Issuer Rules. According to the ES Rules, ES has the right to determine that the contract shall cease where, inter alia, the counterparty contravenes the provisions set forth in the ES Rules.

Degree of certainty for rules and procedures

The process by which the ES Rules are created give a high degree of certainty that ES Rules, procedures and contracts will not be voided, reversed or subject to stays. For participants in foreign jurisdiction the above mentioned legal opinions provide a similar degree of certainty.

Further assurance for ES Rules and the procedures of Euroclear Sweden is provided by the legal regime for settlement finality, i.e. the Settlement Finality Directive and their national implementations. However, these rules leave unaffected general rules of national bankruptcy law in relation to the voidance of transactions entered into during a prescribed period prior to, and defined by reference to, the commencement of bankruptcy proceedings, for instance in case of fraud to the rights of the creditors of the ailing debtor.

Key consideration 5: An FMI conducting business in multiple jurisdictions should identify and mitigate the risks arising from any potential conflict of laws across jurisdictions.

Euroclear Sweden mainly conducts its business in Sweden, which is the country of incorporation of Euroclear Sweden and also the jurisdiction where the securities settlement system operated by Euroclear Sweden is located. Euroclear Sweden also acts as an issuer CSD for securities which are governed by the laws of the United Kingdom, Germany, Denmark, Finland and France. Euroclear Sweden passports its authorisation under CSDR to Germany, Denmark, Finland and France and is currently under the process of applying to the Bank of England for a recognition to provide services in the UK.

Euroclear Sweden also handles a smaller number of cross-border transactions via its CSD links. Euroclear Sweden has cross-border links, either directly with other CSDs or indirectly via custodial banks, to facilitate the transfer of certain foreign securities. For the accounts held with these foreign financial firms, local law normally applies.

Principle 2: Governance

An FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.

Key consideration 1: An FMI should have objectives that place a high priority on the safety and efficiency of the FMI and explicitly support financial stability and other relevant public interest considerations.

The main strategic objective of the Euroclear Group and Euroclear Sweden is to be one of the leading providers of post-trade services through reliability, innovation and leadership by

- Building long-term partnerships with clients and
- Supporting the stability and developments of the markets, locally or globally.

The Board of ES set the objectives for ES and ES benefits from the pooling of investment within a larger group, the ability to develop new services and cover new products leveraging the expertise of the Group with the objective of meeting the needs of the market where they operate.

The Group's shares are largely owned by users of its services and its boards are essentially composed of members drawn from a cross-section of firms that use the Euroclear services allowing users' interests and sensitivities to influence the decision-making process of Euroclear. In addition, independent directors, not affiliated with firms using the Group's services have been appointed to each of the Boards of the group including ES in order to allow for the interests of stakeholders other than users to be represented. Users can also influence the decision-making bodies through the User Committee, which is established by ES.

Key consideration 2: An FMI should have documented governance arrangements that provide clear and direct lines of responsibility and accountability. These arrangements should be disclosed to owners, relevant authorities, participants, and, at a more general level, the public.

Governance arrangements

Euroclear Sweden is one of the CSD of the Euroclear Group and is incorporated under Swedish law. ES is a wholly-owned subsidiary of ESA, a Belgian financial holding company regulated by the National Bank of Belgium.

ES governance requirements are set out in CSDR, Swedish company law and other Swedish legal and regulatory requirements. In accordance with the Swedish Companies Act, the Board of Directors of ES is responsible for the organisation of the company and the management of the company's affairs and for the appropriate arrangement of the control of e.g. the company accounts and finances.

Disclosure of governance arrangements

Euroclear makes public relevant governance information to its stakeholders via different channels:

- Publications with relevant authorities (e.g. Swedish regulators, etc.);
- Publications on the ES website (e.g. Board composition, Board Terms of Reference, Annual report, etc.).

Key consideration 3: The roles and responsibilities of an FMI's board of directors (or equivalent) should be clearly specified, and there should be documented procedures for its functioning, including procedures to identify, address, and manage member conflicts of interest. The board should review both its overall performance and the performance of its individual board members regularly.

Roles and responsibilities of the board

In accordance with the Swedish Companies Act, the Board of Directors of Euroclear Sweden is responsible for the organisation of the company and the management of the company's affairs. The Board of Directors of ES is also responsible for the appropriate arrangement of the control of e.g. the company accounts and finances. Furthermore, according to the Board Terms of Reference adopted by the ES Board, the ES Board shall address matters of principle nature and of material financial importance for the company. The Board Terms of Reference is published on the ES website.

In carrying out this role, each Board member acts in good faith in the way she/he considers would be most likely to promote the success of ES for the benefit of its shareholders as a whole while having due regard to the interests of other stakeholders (such as customers, employees and suppliers).

In order to perform its responsibilities more efficiently, the Board has established the following advisory committees: the Audit Committee ("**AC**"), the Risk Committee ("**RC**") and the Remuneration, Nomination and Governance Committee ("**RNGC**").

The AC assists the Board in fulfilling its oversight responsibilities for ES. The committee reviews and makes recommendations in relation to ES financial results, the financial reporting process and its integrity, and the financial soundness. The AC also assists the Board in fulfilling its oversight responsibilities by monitoring and reviewing the effectiveness of ES internal audits. Furthermore, the AC oversees the relationship with the Internal Auditor and External Auditor considering relevant professional and regulatory requirements.

The RC assists the Board in fulfilling its risk oversight responsibilities for ES. The committee reviews and advises the Board in Risk capacity, appetite and profile and in Risk exposure. The committee also oversees, review and advise on ES Risk Management framework and critical risk policies and effectiveness and independence of ES Risk Management department. The RC also assists the Board in fulfilling its oversight responsibilities by monitoring and reviewing the effectiveness of ES internal controls, the effectiveness and independence of the Compliance function and review and recommendation on technology framework. Furthermore, the RC reviews ES business continuity arrangements.

The RNGC advises the Board in all matters in relation to the nomination and remuneration of Board members and CEO, Board and Committee composition, succession planning as well as corporate governance matters as they apply to the Company.

The CEO of ES is responsible for the day-to-day management of the company, in accordance with the Swedish Companies Act and instructions issued by the ES Board of Directors and the operational management of ES. Please also see the reply under Key Consideration 5. The ES Executive Committee ("**ExCom**") has been set up in order to advise the CEO.

The ExCom supports the CEO in carrying out ES day-to-day operations in a coordinated manner and advises the CEO in his decision making. The responsibilities of the ExCom is described and regulated by the ES Terms of Reference Internal Governance.

ES management model is based on a decentralized model with delegated responsibility, within certain limits, to each function's operational managers.

Procedures for the Board's functioning and Conflicts of Interest

The ES Board meets regularly (at least five times a year, as required by the Board Terms of Reference). The Board is composed of suitable members of sufficiently good repute with an appropriate mix of skills, experience and knowledge of the Company and of the market. Additional information on the functioning of the Board is included in the Board Terms of Reference, which are reviewed annually.

ES has adopted comprehensive policies that Board members, the CEO, ExCom and other staff (including contractors), must follow in order to identify, notify, assess, properly manage and control potential and actual Conflicts of Interest ('**CoI**') including:

- Board Code of Ethics, Policy on Conflicts of interest for Board Members and Policy on External Mandates for Board and CEO;
 - Conflict of Interest Policy Handbook;
 - Guidelines for categorisation, assessment and determination of management measures and controls for Conflict of Interest.

Those policies cover both personal and corporate conflicts, with due consideration of potential intra-group conflicts resulting from the group structure and its operating model entailing multiple outsourcing arrangements. CoI Policy documents require all board, CEO and staff and contractors not only to consider and disclose the conflicts of interest they may have both personally (including via persons directly or indirectly linked to them) and when they act upon a mandate, but also to take reasonable steps to avoid engagement in activities which could create a perception of impropriety or jeopardise Euroclear's integrity or reputation.

The Guidelines detail how to:

- categorise and assess the materiality of conflicts of interest identified or disclosed under the CoI Board Policy or the CoI Policy Handbook;
- assess the effectiveness of available management measures and controls in respect of any conflicts of interest;
- implement effective management measures and controls for identified and disclosed CoI.

ES seeks to limit the occurrence of material CoI situations. ES Board and Board Committee composition policy form integral part of this objective.

In case of an actual permanent conflict of interest, ES will automatically apply the measures foreseen in relevant regulation (i.e. involved individuals will be excluded from the decision-making process and from the receipt of any relevant information concerning the matters affected by the permanent Conflict of Interest).

All potential or actual conflicts identified or disclosed in line with the CoI Board Policy and the CoI Policy Handbook are recorded either in the Conflicts of Interest Inventory or Register along with the outcome of the categorisation and materiality and manageability assessments which are required by the Guidelines.

Review of performance

On an annual basis, the board of ES shall perform a self-assessment of its own performance and effectiveness. This self-assessment endeavours to ensure that the Board has the necessary framework in place within which to make decisions, focusing on the optimum mix of skills and knowledge amongst the Directors, clarity of goals and processes, a culture of frankness that encourages constructive evaluation, full disclosure of procedures and an effective relationship with CEO. This annual review is carried out by completion of a detailed questionnaire by each Board member. The Board can also decide to request an independent external assessment.

The consolidated responses of the self-assessment are reviewed by the Corporate Secretariat function with the support of the Compliance & Ethics function, and the results are reported to the Board for discussion. Where concerns are raised in the responses, they are the object of any follow-up actions. The outcome of the Board discussion are documented in the Board minutes and are used as basis for the creation of the Board training plan for the coming year.

In addition, the RNGC reviews at least annually the balance of skills, experience and participation on the Board (both individually and collectively) to ensure sufficient collective expertise and make recommendations to the Board in this regard.

Key consideration 4: The board should contain suitable members with the appropriate skills and incentives to fulfil its multiple roles. This typically requires the inclusion of non-executive board member(s).

The Board of Directors of Euroclear Sweden consists of eight ordinary members, of whom one is the CEO of ES, two are non-executive Directors, three are independent of the Euroclear Group, and two are employee representatives. In addition, the Board also has two deputy members which are deputies to the employee representatives. The SFSA conducts a suitability assessment of the members of the Board of Directors. The suitability assessment also encompasses the CEO.

The majority of the Board members are non-executive Directors. One of the non-executive directors on the ES Board is also a member of the Group management. This promotes coherence in strategy and policies as between Group entities and ensures the sensitivities of ES are well understood by ESA and vice versa. All non-executive directors have a fiduciary duty to act objectively and independently in that function to ensure that the corporate interests of ES and the general interests of the infrastructure are preserved. As stated above the Board also includes three independent Board members which ensure input from an external perspective on the operations of ES.

The RNGC review and make recommendations in respect of nominations of the Board members of ES with due regard to such person's professional background, expertise and seniority, willingness to be actively involved in the business of the Board and independence requirements. In each case with a view to ensuring that the Board or committee have the correct knowledge base and skills among its members and that all members of the Board or committee have the adequate personal attributes in order for each of the Board or committee to fulfil its role efficiently.

Only non-executive board members receive remuneration for their mandate, the remuneration is determined taking into account their level of responsibility and time required of them in fulfilment of their Board role. It comprises an annual gross fee and is not linked to the performance of Euroclear. No Board member receives incentive compensation (short or long-term) or stock options or employment benefits (other than reimbursement of expenses). This is also in line with market practice.

Key consideration 5: The roles and responsibilities of management should be clearly specified. An FMI's management should have the appropriate experience, a mix of skills, and the integrity necessary to discharge their responsibilities for the operation and risk management of the FMI.

Roles and responsibilities of management

The responsibilities of the CEO are set out in the Swedish Companies Act. Furthermore, it also includes in which situations a CEO cannot participate in a matter (conflict of interests).

The Board of Directors of ES has approved Instructions for the CEO where the role, responsibilities and duties are stated in more detail.

According to ES 's CEO Instructions, the CEO of ES may assign its duties to his/her reports but shall be responsible for directing and overseeing the activities of the management. The ExCom comprises of persons responsible for the ES 's key business functions and report directly to the CEO. Decisions made by the CEO and advised by the ExCom are documented in the minutes of the ExCom meetings, which are held regularly.

The Terms of Reference Internal Governance describes the internal governance structure within ES, including the duties of e.g. the ExCom (please see Key Consideration 3 above), CEO and Heads of Department. It provides clarity, autonomy and delegated authority.

In the CEO Instructions, it is stated that the CEO shall, in particular, see to it that the strategy and objectives concerning development and profitability are maintained.

The specific objectives of the management are reviewed and updated on a yearly basis by the CEO who assesses performance of all heads of department in accordance with the Group wide performance management process (PMP).

Experience, skills and integrity

The CEO is appointed by the Board based on merit and on the basis of the knowledge, experience and skills of the candidate, regardless of his/her gender or ethnic background.

Experienced HR personnel are in charge of the recruitment of management persons in close cooperation with the CEO and other concerned parties. When necessary, ES HR personnel also cooperate with external HR experts. Personal testing of the candidates is carried out together with reference taking. This ensures that the management positions are filled by staff with the required skills necessary for their positions. ExCom members receive induction training, where relevant and can request training, as needed.

Key consideration 6: The Board should establish a clear documented risk-management framework that includes the FMI's risk-tolerance policy, assigns responsibilities and accountability for risk decisions, and addresses decision making in crisis and emergencies. Governance arrangements should ensure that the risk management and internal control functions have sufficient authority, independence, resources and access to the board.

Enterprise Risk management framework

The Management of ES actively support the development and maintenance of a strong internal control system (ICS). ES operates a robust and documented framework for the identification, measurement, monitoring, management and reporting of all types of risks relevant for ES.

In line with best market practice, ES operate a three lines of defence model. The allocation of responsibilities within the three lines of defence model is:

First line of defence:

The first line (management) is responsible for taking acceptable risks as per our risk appetite to meet the key business objectives/key goals. In this context, the first line becomes the primary source of (non-independent) assurance to the Board. Management uses the ERM framework to identify, assess and manage risks that might impact the achievement of the key goals or are outside of the risk appetite.

The first line:

- Provides the Board with information on our risk profile, as well as our key and emerging risks;
- Demonstrates to the Board that risk controls are both adequate and effective; and
- Advises whether key goals are likely to be achieved.

Second line of defence:

The second line, Risk Management and Compliance & Ethics function ("**C&E**"), provides robust independent oversight of management's risk-taking activities.

For Risk Management through:

- establishing, maintaining, facilitating and assessing the effective operation of our ERM framework
- challenging management and advising the Board around identification, assessment, risk-response and reporting of risks, including compliance risks
- providing the Board with an independent view of our:
 - risk capacity, appetite (including risk appetite framework) and risk profile
 - key and emerging risks, both at the Group and entity level
 - achievement of business goals
- acting as an independent risk 'sounding board' (providing advice) for executive management and the Board.

The Compliance & Ethics function ensures there is a robust independent oversight of the management of compliance risks through:

- Designing, implementing and overseeing the Compliance Risk Management Framework;
- Monitoring compliance with legal and regulatory requirements;
- Providing objective and independent advice, guidance and challenge on the first line's identification, assessment and management of Compliance Risks;
- Assisting CEO in educating and enhancing the awareness of staff members on compliance matters and promoting a culture of compliance throughout the company;

- Providing assurance to CEO, Boards and regulators on the effective management of Compliance Risks.

Compliance and ethics risks are a subset of the risk categories within ES Enterprise Risk Management Framework. Specifically:

- Conduct & Culture risk
- Compliance risk
- and, within Operational risk:
- Internal and External Fraud risks

The Compliance & Ethics Charter (the Charter) sets out the role, objectives, accountabilities and authority of C&E, its organisation, its activities within the three lines of defence and how it ensures its independence. The Charter has been prepared on the basis of good practice guidance and known current or up-coming regulatory requirements.

The ES Chief Compliance Officer ("**CCO**") has a direct access and reports line to the Chair of ES Risk Committee to ensure that C&E is fully independent, free from interference by any element of the organization.

The ES CCO also has a reporting line to ES CEO, to

- ensure adequate positioning, resourcing and organisation of C&E within the CSD;
- ensure unrestricted access to records, personnel and physical properties relevant to the delivery of the C&E mission.

The Risk Management Charter and the Compliance & Ethics Charter clarifies how the second line functions will achieve their mission and objectives through the authority, remit and responsibilities provided to them. Other support functions as Finance or Human Resources monitor specific controls and escalate to management in case of control defects.

Third line of defence:

The third line (Internal Audit) provides the Board with independent assurance and insight on governance, risk management and internal controls, to support Euroclear Sweden in achieving its objectives. Internal Audit's Charter governing the internal audit functions' mission, authority, remit and responsibilities are approved by the Board, upon Audit Committee recommendations.

The Risk Management, Compliance and Internal Audit Departments are independent from the business lines they monitor. The Risk Officer and the Compliance Officer have a direct reporting line to the CEO. The Risk Officer, the Compliance Officer and the Head of Audit have direct access to the chairman of the relevant Board committees.

The ERM Framework is documented through a comprehensive set of Board policies, handbooks and procedures and the risk management framework is described in more detail under principle 3.

Our Corporate Risk Board Policy sets out the Board's role in relation to risk management and communicates the Board's risk management expectations to the business. In so doing, the Board has

articulated our desired risk culture and overall risk appetite, which details how much and what types of risk we are willing to accept in order to achieve our key goals.

The Board in line with Euroclear's mission and corporate strategy has set its risk appetite (tolerance). In relation to our risk appetite the Board regularly discusses the actual risk profile. The risk appetite is defined by the Board considering ES available capital and liquidity capacity. A key pillar of our ERM Framework is the risk culture. The risk appetite and tolerance levels are used in daily risk management processes in order to assess risks and prioritise the actions to mitigate them. Euroclear has a risk adverse culture, emphasised by management through its actions. The importance of having the risk culture appropriately embedded is demonstrated also by the importance it plays in the Balanced Scorecard and the risk and control assertions signed by senior managers.

Euroclear is continuously improving its ERM Framework. In this context we are further enhancing our risk appetite framework.

Euroclear has established a risk strategy, a risk appetite, a risk Register, High Level Control Objectives (HLCOs) and more detailed Control Objectives to mitigate the risks identified, describing how and by whom the risks are to be managed. These control objectives are supported by detailed controls and control processes describing how the risks impacting business activities are to be mitigated. These control objectives are the foundation of the group's internal control system and are documented in the Positive Assurance Reports/RCSA material (PAR). The PAR is deployed at departmental level. They link business objectives with the control objectives, control activities, and forms of evidences. The PARs allow first line management to timely identify and report on the adequacy and effectiveness of the control environment.

In addition to the Corporate Risk Board policy a number of other key policies and handbooks guide the organisation on the way risks are managed in Euroclear. The most important ones amongst others are the Remuneration Policy, Operational Risk Management Board Policy, Board Code of Ethics, Policy on Conflicts of Interest for Board Members & Policy on External Mandates for board and CEO, the Compliance Risk Board policy and the Legal Risk Board policy.

The accountability for risk decisions is distributed at all levels of the group. Strong crisis procedures are also in place allowing quick escalation at entity or group level depending on the nature and the severity of the crisis. Those crisis procedures are regularly tested.

Authority, independence and resources of Risk Management and audit functions and access to the board

ES has in place independent Risk Management, Compliance & Ethics and Internal Audit functions, according to the highest applicable standards in ensuring a robust and transparent management structure and control environment.

The Risk Management, Compliance & Ethics and Internal Audit departments are independent control functions, each with a dedicated Board-approved Charter.

There are a number of mechanisms set up to safeguard their independence:

- decisions on appointment and removal of the heads of the internal control functions are made

by the Board with input from the relevant Board Risk/Audit Committees;

- the Chief Risk Officer, the Chief Compliance Office and the Head of Audit have a direct reporting line to the Chairman of the relevant ES Board Risk/Audit committee;
- the heads of the control functions each regularly attend closed sessions of the relevant Board Risk/Audit Committee (i.e. without executive directors present). Additionally, they each have unmediated access to the Chairman of the ES Board, the Board itself and members of the relevant ES Board Risk/Audit Committee.

Risk Management

Mission

The Risk Management department's mission is to support Euroclear in achieving its goals and delivering its strategy through providing robust, independent oversight of risk taking activities. Risk Management implements an approach which enables the identification and understanding of all material current and emerging risks and the management of appropriate responses.

This is done by providing a coherent effective framework, suitable training, appropriate tools, expert impartial advice, timely risk assessments, escalation of material risk issues, informed relevant reporting, all of which enable risks to be managed within our risk appetite.

More specifically, the Risk Management department:

- establishes, maintains, facilitates and assesses the effective operation of ES ERM framework including the risk appetite framework
- constructively challenges management and advises the board(s) on the identification, assessment, mitigation and reporting of risks
- provides the Board and Management with an independent view of:
 - risk capacity, appetite (including risk appetite framework) and risk profile;
 - key current and emerging risks, both at Euroclear group and ES; and
 - likely achievement of strategic business objectives
 - Acts as an independent risk 'sounding board' (advising) for executive management and the ESA and entity boards (through the relevant board Risk Committee).
 - Leads and shares risk thinking within the organisation and wider financial market infrastructure sector.

Organisation and authority

Risk Management acts independently of other functions and reports directly to the CEO. It is headed by a Chief Risk Officer (CRO) who is also a permanent invitee (observer) to the management Committee of ES.

The Risk Committee of the ES Board will review and approve as appropriate decisions regarding appointment, or removal of the RO, as well as consider the CRO's performance annually. The Risk Committee will be consulted as appropriate on decisions regarding appointment or removal of entity CROs and on performance. The CRO has unrestricted direct access to the Chairman of the ES Board and to its Audit and Risk Committee.

The Risk management department is assigned to address the risks of ES and can leverage on resources and skills available at Euroclear Group for specific FMI skills covering a range of topics from systemic risk to capital modelling.

The mission, authority, operating model of Risk Management department is laid down in the Risk Management Charter.

Internal Audit

Mission

The mission of Internal Audit (IA) is set out in the IA Charter approved by the Board upon Audit Committee recommendation, as providing independent assurance and insight on governance, risk management and internal control, on the adequacy and effectiveness of the internal control systems to support the Board and CEO in reaching their objectives.

Organisation

The Internal Audit Charter describes IA's purpose, authority and responsibility. The Charter stipulates that the Head of Internal Audit reports to a level within the organisation that allows IA to fulfil its responsibilities, with proper independence in determining the Audit Universe, Audit Plan and scope of audit reviews, performing work (through an unrestricted access right to all records and data of the company), and communicating results. The single, primary and functional reporting line of the Head of Internal Audit is with the Chair of the Audit Committee (AC).

IA is organisationally independent from any operational or business activity. The Head of Internal Audit has direct access to the Chair and members of the AC, the Chair of the Board of directors, and the accredited statutory auditors.

Functioning

In order to carry out its mission, Internal Audit has set up a comprehensive audit universe including all processes, whether directly operated or outsourced. The Audit Plan covers the full audit universe and is presented annually for approval by the Board upon recommendation by the AC, and after

consultation of the Executive Committee. The Audit Plan is the result of:

- a risk and control based approach: each line of the audit universe is assessed, which drives the depth and scope of audits
- a cyclical approach: even though the results of the risk and control assessments would not lead to a full scope audit, audit work is anyway performed every three years.

In a rolling manner, the Audit Plan focuses on the next twelve months but has a three-year time horizon.

Such frequency and comprehensiveness ensures that the Audit Plan remains commensurate to the risk profile of the company and focuses on the areas presenting the highest risks or being heavily control dependent.

Issues identified by Internal Audit are entered into the risk database used at group level. In line with the Institute of Internal Auditors standards, Internal Audit performs the follow-up and verification of the issues it raises.

Reporting

ES CEO and management and the Audit Committee are informed periodically of the adequacy and effectiveness of the internal control system through the regular IA activity report, which covers:

- the progress on the internal audit plan
- the results of audit work (including concerns regarding the effectiveness or timeliness of management's actions to address audit issues)
- resourcing

In addition to this, IA sends any communication, audit reports it deems necessary, directly to management members; the follow-up of the Internal Audit issues is made regularly to highlight significant control issues as well as progress in mitigating them.

IA also has meetings with external auditors. Audit reports are communicated to these stakeholders upon request.

Crisis management

ES Risk management framework also includes crisis management and incident escalation, to ensure that when a significant incident/crisis occurs, it is escalated rapidly to the appropriate governance bodies and appropriate measures are taken at the right level. ES's Business Continuity Management framework describes roles and responsibilities, and the adopted approach.

The Risk Appetite Framework lays down roles and responsibilities and escalation mechanisms in case of breaches.

For incidents, ES uses different levels of escalation depending on the severity of the incident (crisis). Each significant incident is assessed in terms of its (potential) impact on ES activities or the wider market (systemic risk).

Moreover, in accordance with legal requirements, ES's Business Continuity Management framework describes roles and responsibilities, and the adopted approach. It also includes objectives supporting the business targets for the timely resumption of critical operations.

Key consideration 7: The board should ensure that the FMI's design, rules, overall strategy, and major decisions reflect appropriately the legitimate interests of its direct and indirect participants and other relevant stakeholders. Major decisions should be clearly disclosed to relevant stakeholders and, where there is a broad market impact, the public.

Identification and consideration of stakeholder interests

The user governance framework of ES ensures that the interests of participants and other stakeholders are taken into account in Euroclear Sweden's rules, strategy and major decisions.

The users can influence the ES's decision-making bodies through the User Committee ("UC"). The purpose of the UC is to provide advice (which is independent from any direct influence by the CEO of ES) to the Board of the CSD on key arrangements that impact ES's participants. The UC is the main channel for ES to communicate with the Swedish market participants. The members of the UC are appointed by the Board of Euroclear, who makes sure that the members represent all the different interests in the local market. The chairman of the UC reports to/is invited to the Euroclear Sweden Board at least annually.

Member Meetings: The Member Meetings are for ES participants; i.e. clients that are involved in settlement, clearing, account operations and corporate actions processing. The purpose of the meetings is to inform clients about on-going matters such as an update of current initiatives within the post-trade area as well as operational issues related to settlement, corporate actions and account operations. Clients are encouraged to put forward their views and request desired areas to be added to the agenda. In general, the information is on a relatively high level without going into detail. When there is a need to discuss and investigate specific matters in detail, bi-lateral meetings are set-up between ES and client/clients.

Market Implementation Group ("MIG"): A market wide group, consisting of participants, exchanges, CSDs, Issuers and CCPs, appointed to monitor the implementation of market standards ("Market Standards for Corporate Action Processing" and "Market Standards for General Meetings"). The mandate for the group is to first analyse existing gaps between current processes and those described in the standards and secondly to conclude on actions in order to fill the gaps. Furthermore, the process of filling the gaps is continuously monitored by the Swedish MIG and status updates are reported to the Broad Stakeholder Group ("BSG") via the E-MIG twice a year. ES has one representative in the Swedish MIG.

According to ES Account Rules, account operators, nominees or clearing members may personally, or through interest organisations or other representatives, propose amendments to the rules. Furthermore, according to ES Account Rules, ES is obliged to circulate proposed amendments to the rules to all account operators, nominees, clearing members and settlement banks, which shall be afforded the opportunity, within a specified period of time, to submit comments regarding the amendments.

As explained above the user framework and the interaction with the UC ensures that the views of (direct) participants and other stakeholders are taken into consideration. Users and other

stakeholders can also influence ES's decisions by participating in ad hoc working groups and committees and international groups or through ad hoc consultations.

Conflicts of interest

The SFSA has issued General Guidelines (FFFS 2005:1) on governance and control of financial institutions stating that a financial institution shall handle the responsibilities and the tasks internally so that the risk of conflicts of interest is avoided.

Conflicts of interest matters are governed by applicable company policies such as the Board level Conflicts of Interest Policy and the Policy on Ethical Conduct, Legal and Compliance Risk. All staff members, CEO and Board members are made aware of the importance of identifying and handling conflicts of interest, i.e. through the Company's on-boarding process conducted by HR, and by annual assessments on the topic. ES ensures fair treatment to all clients and shareholders by disclosure or otherwise minimizing any unfair impact of such conflicts.

Disclosure

Major decisions are communicated to the SFSA and the Riksbank through bilateral contacts and to the market and the participants of ES via channels contractually defined. In addition, the Commercial relationship managers are at the disposal of clients and prospects for any information needed.

Principle 3: Framework for the comprehensive management of risks

Key consideration 1: An FMI should have risk-management policies, procedures, and systems that enable it to identify, measure, monitor, and manage the range of risks that arise in or are borne by the FMI. Risk-management frameworks should be subject to periodic review.

Enterprise Risk Management framework

ES Enterprise Risk Management (ERM) framework is the methodology designed by the Risk Management department, approved by the ES board and implemented and operated by the CEO that shall ensure that ES manage risks in a structured way. The ERM framework contains policies, handbooks and processes for identification, measurement, response and the monitoring of risks. The ERM framework builds on key pillars including amongst others the risk governance, the risk appetite framework and the Recovery, Restructuring and orderly Wind down arrangements. Other important aspects are interdependencies to external parties i.e. service providers and clients. ES work together with the participants on the Swedish market to facilitate a secure and effective settlement system including measures to be taken to mitigate the effect of widespread scenarios on the Swedish market. The ERM framework including policies and handbooks is reviewed when deemed necessary but at least annually.

ES' strategy, goals and risk appetite are linked with, and central to, our ERM framework. However, it is important to highlight that our culture also has a significant influence on our attitude towards risk and how it is managed. Our positive and collaborative culture, underpinned by our REACH values and willingness to constructively challenge, is critical in supporting risk-aware behaviours and embedding

effective risk management in everyday activities and processes across Euroclear Sweden.

Risk Management policies and handbooks

- The ERM framework starts with the Corporate Risk Management Board Policy, The Risk Appetite Board Policy and the Operational Risk Management Board Policy. These together with ES Enterprise risk management policy handbook provide for a robust and consistent framework for the identification, measurement, monitoring, management and reporting of all types of risks relevant for ES as well as outlining key risk management roles and responsibilities, processes and risk reporting expectations.
- ES' framework has been further strengthened (e.g. ES' Systemic Risk Handbook, ES' Operational Risk framework, New Initiative, Product & Pricing Handbook) in line with new regulatory requirements (CSDR3).
- ES' risk appetite framework (RAF) was developed by Risk Management working in close co-operation with the CEO and the Board. The Board has approved a set of diverse entity -level risk appetite metrics and associated limits based on risk reward analysis and related to our strategic objectives. The metrics have been cascaded down to different departments for regular monitoring.
- ES' systemic risk management framework is being reviewed in depth, to enable ES to better identify, measure, monitor, manage and report on the risks ES may pose to other entities (the focus until now was more on the risks ES was itself facing). ES is also strengthening its operational risk management framework. We elaborate on this aspect under Principle 17.
- The ERM Framework also describes the practical application of ES' risk policies and guidance, represented by the four-step risk cycle (known as 'Risks in execution'), representing how ES goes about identifying, assessing, mitigating and reporting on its risks.
- The three lines of defence model operated by ES facilitate the effective operation of the ERM framework. Each line plays a distinct role providing the ES CEO and ES Board with confidence that ES is likely to achieve its key goals through the effective management of risks

Risks that arise in the Euroclear Sweden

ES describes the risk categories used to facilitate risk identification and analysis in the Enterprise Risk Management (ERM) framework Policy Handbook. The key sources of risk are reviewed continuously and are mapped into the relevant risk category. For each risk category, ES defines a risk strategy that outlines its broad approach to managing and mitigating those risks.

ES uses a risk library to ensure consistent identification of the risks. The key sources of risk (whether direct or indirect) are:

- **Conduct & Culture risk**, arising from ES' corporate and risk culture, governance arrangements, conduct and dealings with its stakeholders, and ES' corporate responsibility as a trusted financial organisation. Stakeholders include participants, shareholders, suppliers, regulators, competitors and other users including other FMIs
- **Operational risk** is the most relevant risk for ES. To ensure robust risk management, the

risk is divided in sub categories aligned with the Basel 2 definition i.e. but it also includes custody risk Model Risk, Fraud and Cyber, Business disruption and system failures

- **Legal & Compliance risk**, is the risk of financial loss or reputational damage arising from failure to comply with legal and regulatory requirements and material contractual obligations necessary to maintain ES's license to operate or protect the Group's rights and interests.
- **Credit risk** arising from the default or failure of a participant or counterparty to meet their financial obligations to ES.
- **Liquidity risk**, arising from being unable to settle a cash or securities obligation when due resulting from inappropriate and/or insufficient liquidity sources **Market risk**, the uncertainty on the value of assets and liabilities (on- or off-balance sheet) and on the future earnings (linked to foreign exchange or interest rate movements). Market risk arises from possible changes in foreign exchange rates, interest rates, equity or commodity prices and is very limited given ES balance sheet and fee models.
- **Strategic & Business risk** are the uncertainties and untapped opportunities embedded in the strategic intent and how well they are executed
- **Change risk**, including considerations on programme and project management capabilities, adaptability to industry and market change
- **Systemic risk**: the risk of disruption to financial services organisations that have the potential to have serious consequences for the financial system and/or the real economy. Systemic risk events can originate in, propagate through, or remain outside of Euroclear Sweden/group

Risk management systems

ES uses a Positive Assurance Reporting (PAR) process which facilitates bottom up risk identification and enables the CEO to evaluate whether key risks are appropriately mitigated through the effective operation of key controls. The PAR process is integrated into the Internal Control System (ICS) processes and allows the Board to take a holistic view on ES' risk and control environment. Further information is provided on ES' PAR process under Principle 15 (General Business Risk) and Principle 17 (Operational Risk).

Risk Issues including control gaps are logged, monitored and aggregated in the I-track database. Operational risk events (incidents) are logged, monitored and managed in the Integrated Risk Management (IRM) tool embedded in 2020. IT events are logged in the IT-events database Efecte..Within the next two years, the IRM tool will replace the I-Track database as ES dedicated risk and issue tracking tool, which allows for effective assessment and follow-up of risks, control gaps and weaknesses that have been identified by the 1st, 2nd or 3rd line of defence. ES promotes and encourages the pro-active identification and logging of risk issues. Each issue is populated with detailed action plans that set out the specific steps needed to be taken in order to mitigate or reduce the risks faced if such risk is unacceptable as such. Risks that cannot be mitigated within set time frames is subjected for approval by different governance levels depending of materiality.

The Integrated Risk Management Tool (IRM) is the dedicated incident repository for logging

operational incidents across ES. All operational incidents must be recorded in the tool, which supports a standardised workflow for the different incident management steps. All ES Departments are required to use Efecte to capture operational risk incidents also incidents that are caused by external parties i.e. service providers and participants. The singular corporate Incident Repository centralises all operational incident information which serves as the operational loss database.

As part of its management of business risk, and specifically the risks related to its P&L, ES uses tools for collaborative planning, budgeting and forecasting as well as for reporting and analysis purposes.

We further elaborate on supporting systems in the KC 3 further down in this chapter.

Aggregation

ES monitors all risks that arise in or are borne by ES, as described above - financial and non-financial. The risk appetite framework as well as the PAR facilitates aggregation of the risks. The aggregated risk view is presented to the Board at least quarterly and to the CEO at least monthly. The report also includes details for relevant areas.

Effectiveness of the risk management policies, procedures and systems

The effectiveness of the ERM framework, constituting ES' risk management policies, procedures and systems, is routinely assessed by each of the three lines of defence.

- **First line:** the first line of defence consists of all but the control functions, whose role is to identify risk, as well as execute actions to manage it. The first line has responsibility for implementing and operating the ERM framework. In so doing, the first line is ideally positioned to identify and escalate concerns in the overall design and operation of the framework. Such concerns can be escalated either through the Chief Risk Officer, the Chief Compliance Officer, or via the CEO.

The first line operates several risk-related processes that support the CEO and board-level governance oversight, enabling the effectiveness of the ERM framework to be considered as appropriate. Examples include the Positive Assurance Report (PAR)⁴ process, the Risk & control self-assessment (RCSA) process⁵, Internal Control System Assurance (ICS) process⁶, Stress tests and scenario analysis.

Additionally, ES has installed first line control units within the Operational and the IT departments respectively. These functions report to management and are tasked with routine oversight and testing of key internal controls within the department. The first line control units are being supplemented by a network of first line risk champions to bolster the effectiveness, monitoring and reporting of risk management activities in the first line.

⁴ PAR: Positive Assurance Report ensures that the key risks and associated controls are identified in all divisions, and effectively monitored to allow timely management of risks and adjustment of the system when necessary

⁵ Performed by all Euroclear entities and divisions, the RCSA process is a twice-yearly management assessment of the adequacy and effectiveness of Euroclear's risk & control framework facilitated by the Risk Management department. The RCSA process also seeks to identify any new or emerging risks that need to be addressed

⁶ ICS is a consolidation and reporting process that seeks to combine and summarise information from the PAR and RCSA processes for review by the CEO and the AC/RC. Both Risk Management and Internal Audit independently review and opine on the adequacy and accuracy of management's risk & control framework assertions

- **Second line – Risk Management:** Risk Management (RM) is responsible for designing, facilitating and assessing the effective operation of the ERM framework. In relation to the latter, RM uses a combination of continuous risk monitoring and analysis combined with a rolling programme of independent risk assessments to assess how effectively the overall ERM framework is operating. Key RM concerns are highlighted when deemed necessary but at least monthly to the CEO and to the ES Board Risk Committee/Board (RC) at least quarterly.
- **Second line – Compliance & Ethics:** supports and challenges the 1st line in its management of Compliance Risks. This includes: monitoring compliance with the applicable legal and regulatory requirements; proactively identifying, assessing and monitoring of the Compliance Risks faced by ES; designing, implementing and overseeing the Compliance Risks Management Framework; providing objective and independent advice, guidance and challenge on ES's identification, assessment and management of Compliance Risks; assisting the CEO in educating and enhancing the awareness of staff members on compliance matters and promoting a culture of compliance throughout the company; and providing assurance to the CEO, Board and regulators on the effective management of Compliance Risks.
- **Third line – Internal Audit:** Internal Audit is responsible for providing independent assurance over the effectiveness of ES' ERM framework. This is achieved through a programme of on-going monitoring and internal audit engagements. Key concerns are highlighted to the CEO, management and the Audit Committee through a regular Audit Committee Report.

Key consideration 2: An FMI should provide incentives to participants and, where relevant, their customers to manage and contain the risks they pose to the FMI.

ES continuously invests to encourage participants to manage and contain the risks they pose to ES, by keeping them informed- through user documentation, monitoring of transactions performed including settlement ratios, training, relationship (via user committee and client facing relationship) and by applying other types of measures (i.e. charges to deter riskier behaviour, thorough admission process).

ES services and system have been specifically designed to enable participants to monitor, manage and reduce the risk they face, including through Delivery versus Payment and extensive real time information (the information contains among others data on participant's transactions, cash and securities positions).

Client admission process

ES operates a securities settlement system (VPC). Access to VPC is subject to admission criteria driven by risk considerations. ES has implemented a robust admission approval process to reduce the risks both for ES and its participants. The admission approval process consists of an initial Know-Your-Client (KYC) exercise to ensure that each participant meets the admission criteria including mandatory training, at the time of its admission which is followed up by regular reviews to ensure the admission criteria are still met.

See principle 17 for more information.

Documentation and Information

ES encourages its participants to use the system in the best way, by providing extensive information on their use and on the products and services available. This helps them to better manage their risks when dealing with ES – and therefore minimise the risk they pose to ES. Information such as Terms and Conditions, Operating Procedures, Newsletters, Product / Service Descriptions are provided both via ES' website and via dedicated trainings. The ES Commercial Department keeps ES' participants informed of changes and evolution. Furthermore, the annual report contains information about ES' risk management strategy, governance and policies.

Finally, ES has established a User Committee that meets regularly throughout the year to exchange information with Participants. The User Committees Terms of References have been reviewed along with new regulatory (CSD Regulation) requirements.

Incentives/Deterrent measures

ES does not provide any credit facility to participants and has no financial exposure with participants (except the payment of invoices). ES encourages its participants to use the ES' system in the best way and provides extensive information regarding the use of the system and the services available.

Beside the information available on the web site ES organizes training for participants.

ES has no contractual relationship with participants' customer. The contractual relationship remains exclusively between ES and its participants.

Key consideration 3: An FMI should regularly review the material risks it bears from and poses to other entities (such as other FMIs, settlement banks, liquidity providers, and service providers) as a result of interdependencies and develop appropriate risk- management tools to address these risks.

Material risks

Euroclear Sweden has a risk framework that has been used for years to manage the risks that it is exposed to, whether material or not.

The Enterprise Risk Management (ERM) framework has been enhanced to also include the risks that ES poses to other entities. This was done through the integration of systemic considerations in the framework, which aims to cover both the risks posed to ES by the financial system (e.g. other actors in the financial system, such as market participants, FMIs, service providers) and the risks ES might cause to such financial system. Existing risk management processes and tools such as stress-testing, risk assessments, the risk library has been reviewed to explicitly include systemic considerations. On top of that, new processes and tools have been developed to further grow the systemic risk management capabilities (e.g. through interdependency maps).

Systemic risk is a residual risk that can arise from several risk areas but typically from operational events. The first line of defence remains therefore responsible for the integration of systemic risk considerations into their day-to-day risk management activities including new products development and information security. The risks that ES bear from and pose to other entities are operational risks. They are identified within the ERM framework as with other risks, e.g. by project or service risk assessments, risk self- assessments or testing of key controls and systems as well as a robust information security control framework.

The risks borne by ES from other entities (such as FMI's, large participants, settlement banks, network providers and data providers) are mainly affecting the efficiency of the system and the level of services offered by the CSDs. Some examples are listed below:

- risk of lower settlement ratio if one or several significant participants make operational errors (for example sends wrong instructions) or cannot deliver their instructions in time
- risk to settlement ratio and completeness if major infrastructure players in the financial sector is down, like the central bank or a Central Counterparty (CCP)
- risk to the general market stability and risk of delays or losses to other participants and investors if a participant default (but not any de facto risk to the CSD)
- weak information security protection that could cause a cyber event

The risks that ES pose to other FMI or stakeholders are similar to those posed to ES. A long system standstill or severe technical or operational error could cause substantial delays, losses or liquidity issue to participants or their customers. To mitigate this, ES has implemented many layers of precaution and protection of its processes and services with business continuity plans regularly tested. For more information on operational risk management in ES, see Principle 17.

The second line of defence uses specific methods and tools, such as the horizon scanning process and regular contacts with other actors on the market, to further enhance the systemic risk framework and to challenge the first line's views on the potential systemic impacts their activities/processes might generate.

Risk management tools

Systemic risk often crystallises in the market in the wake of a credit, a liquidity, a market, or an operational incident but the nature of the risk can change as it propagates. As a consequence, systemic risk considerations are part of the day to day risk management activities (i.e. identification, assessment, response, monitoring, and reporting) and the risk management tools and processes referred to in the section above under Key consideration 1 are also used when assessing the risks posed by other entities. However, specific considerations are given to the following;

- Standard Risk assessments (including the new product approval risk assessments)
- Stress tests such a business continuity tests and default procedure tests
- first line and second line monitoring activities
- Other specific initiatives on specific risks such as the 'Long-term IT outage' analysis and information security control framework
- Incident analysis and availability follow-up

Beside the regular tools and processes, two new processes have been introduced specifically for systemic risk analysis: interdependency maps and horizon scanning. These processes will be further enhanced in the coming years, with further integration of their outcome in existing processes and further involvement of relevant stakeholders.

Interdependency maps are used as a tool by the first line to identify and manage systemic risk arising from our interactions with the market. These maps will be used to identify stress scenarios originating from incidents happening within ES (e.g. the temporary unavailability of one of our services) or externally, e.g. at a critical service provider or another entity in the market. The maps will assist ES in assessing the potential impact of those stress scenarios on the market.

Horizon scanning refers to a series of activities that Risk Management as second line facilitates, aiming at the identification of potential emerging risks impacting ES or the financial system.

The risks that ES bear from and pose to other entities are operational risks. They are identified within the ERM framework as with other risks, e.g. by project or service risk assessments, or by annual risk self-assessments.

Key consideration 4: An FMI should identify scenarios that may potentially prevent it from being able to provide its critical operations and services as a going concern and assess the effectiveness of a full range of options for recovery or orderly wind-down. An FMI should prepare appropriate plans for its recovery or orderly wind-down based on the results of that assessment. Where applicable, an FMI should also provide relevant authorities with the information needed for purposes of resolution planning.

Recovery plans

In accordance with regulatory rules and guidelines, ES prepares recovery, restructuring and orderly wind-down (RRW) plans for the critical operations.

Building on a broader risk framework, ES' RRW plan aims to assist the Board and the CEO in taking timely and appropriate actions should ES face a situation that threatens its financial viability as a going concern and its continued provision of critical services to the market.

In particular, the RRW plan presents the ES Board's conclusions on:

- capabilities and options:
 - alternative approaches to deal with the crystallised impact of a stress situation and their demonstrated capacity to do so effectively
 - operational plans and preparatory measures to enhance the effectiveness of the identified options
- sources of residual risk and recovery scenarios:
 - the sources of risks which, in the extreme, could threaten ES' viability and hence its ability to continue providing its critical services
 - how, using scenario analysis as a tool, residual risk might crystallise and undermine ES' financial position, necessitating activation of the plan
- governance and implementation:
 - the appropriate governance of decision-making in a recovery scenario arrangements for systematic review and testing schedule of ES' RRW plan and ongoing refinement of the plan

The preparation of such recovery, restructuring and orderly wind-down plans is coordinated by Risk Management and Finance, based on input from other departments. The plan owner is the CEO,

whose responsibility is to liaise with the different stakeholders to ensure the plan is valid, complete, properly reviewed, updated and tested.

The RRW plan is reviewed annually or when a significant change occurs that would impact the feasibility or materiality of a recovery option. As required by relevant regulations, those plans are shared with the authorities.

Recovery scenarios

ES' RRW plan describes various scenarios that span the range of risk sources to which ES is exposed. Each scenario comprises an "Extreme but plausible" (ESP) 'base' scenario that could threaten the viability of ES as a going concern if risk reduction or recapitalisation actions were not taken. In each case, sensitivity analysis considers an escalation of stress into the 'Beyond ESP' zone. Various combinations of scenarios are also considered. In contemplating such extreme scenarios, a certain number of control failures and a conjunction of extreme events need to be assumed.

The scenario analysis presented in the RRW plan builds on similar analysis carried out routinely by ES to size and assess the sufficiency of its capital and liquidity resources. The Risk Appetite framework takes recovery risks into account and specific indicators are in place to monitor to signal a deterioration in ES' financial situation, including any depletion of capital and liquidity relative to required levels. Specified triggers in the dashboard ensure timely escalation to decision makers to determine whether ES' financial viability is at risk and hence whether actions should be taken under the RRW plan.

The set of scenarios included in the plan are complementary in terms of scale (idiosyncratic vs. systemic), rapidity of unfolding (slow burning vs. fast moving materialisation) and risks type (credit, liquidity, business, etc.). This ensures their adequacy to test the completeness and robustness of recovery options in the recovery plans. The scenarios cover:

- External fraud (cyber)
- Long term IT outage (cyber)
- Multiple default of participants (Credit risk/liquidity risk)
- Macroeconomic shock

Recovery options

The ES RRW plan describes in detail a large range of recovery, restructuring and wind-down options that could be taken in order to restore financial soundness of the entity after the occurrence of severe but plausible scenarios in a reasonable and appropriate timeframe.

The options considered in the plans may be categorised as follows:

- options to absorb losses and transfer risks. These options are designed directly to absorb the first-impact losses, with a view to preventing further transmission of stress and recourse to further options. Some of these options involve transferring the risk to a third party
- options to address uncovered losses or to recapitalise. These options aim to generate additional loss-absorbing capacity should losses arise beyond the level contemplated in capital-sizing decisions, or to recapitalise to restore capital to the required level
- options to address uncovered liquidity shortfalls. These options aim to support ES' capacity

to continue to meet payment obligations as they fall due in the event that liquidity needs arise beyond the capacity of available liquidity resources

- options to restructure activities. These are options to restructure activities to: reduce risk exposure, avoid further losses, or address structural weaknesses. They may be further categorised as business restructuring – e.g. urgent cost reductions or downsizing – or disposal strategies – e.g. the sale of a business line. These strategies aim to preserve continuity in the provision of critical functions and services to the wider market
- options to wind down activities. These are options directed at achieving an orderly wind-down of activities over a defined period of time (set internally at six months), again ensuring that critical services to the market are preserved uninterrupted

By supporting ES' recovery or restructuring, or by facilitating an orderly sale or transfer, it is ES' assessment that the effective implementation of identified options and strategies would support financial stability in the markets it serves. If successfully implemented in accordance with the plan, it is anticipated that the provision of critical functions and services provision to the market would continue uninterrupted.

Principle 4: Credit risk

An FMI should effectively measure, monitor, and manage its credit exposures to participants and those arising from its payment, clearing, and settlement processes. An FMI should maintain sufficient financial resources to cover its credit exposure to each participant fully with a high degree of confidence. In addition, a CCP that is involved in activities with a more-complex risk profile or that is systemically important in multiple jurisdictions should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the two participants and their affiliates that would potentially cause the largest aggregate credit exposure to the CCP in extreme but plausible market conditions. All other CCPs should maintain additional financial resources sufficient to cover a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would potentially cause the largest aggregate credit exposure to the CCP in extreme but plausible market conditions.

Key considerations

- 1. An FMI should establish a robust framework to manage its credit exposures to its participants and the credit risks arising from its payment, clearing, and settlement processes. Credit exposure may arise from current exposures, potential future exposures, or both.**
- 2. An FMI should identify sources of credit risk, routinely measure and monitor credit exposures, and use appropriate risk-management tools to control these risks.**
- 3. A payment system or SSS should cover its current and, where they exist, potential future exposures to each participant fully with a high degree of confidence using collateral and other equivalent financial resources (see Principle 5 on collateral). In the case of a DNS payment system or DNS SSS in which there is no settlement guarantee but where its participants face credit exposures arising from its payment, clearing, and settlement processes, such an FMI should maintain, at a minimum, sufficient resources to cover the exposures of the two participants and their affiliates that would create the largest aggregate credit exposure in the system.**
- 7. An FMI should establish explicit rules and procedures that address fully any credit losses it may face as a result of any individual or combined default among its participants with respect to any of their obligations to the FMI. These rules and procedures should address how potentially uncovered credit losses would be allocated, including the repayment of any funds an FMI may borrow from liquidity providers. These rules and procedures should also indicate the FMI's process to replenish any financial resources that the FMI may employ during a stress event, so that the FMI can continue to operate in a safe and sound manner.**

Euroclear Sweden is never part in any transaction in the SSS regardless of currency or type of settlement offered.

Euroclear Sweden does not, as a counter party, give intraday- or overnight credit to the participants in the SSS. Therefore Euroclear Sweden has no framework applicable for risks arising from credit exposures as a participant in a SSS.

In the SSS each participant acting as settlement bank ensures a settlement capacity for settling its (and on behalf of its clearing members') obligations in each currency where the participant participates. A credit exposure between a settlement bank at a clearing member is agreed upon and followed up between the two parties. Euroclear Sweden is not a part in that agreement, and can therefore not suffer any losses as a result of such an arrangement.

Principle 7: Liquidity risk

An FMI should effectively measure, monitor, and manage its liquidity risk. An FMI should maintain sufficient liquid resources in all relevant currencies to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate liquidity obligation for the FMI in extreme but plausible market conditions.

Key considerations:

1. An FMI should have a robust framework to manage its liquidity risks from its participants, settlement banks, nostro agents, custodian banks, liquidity providers, and other entities.

ES is never part in a transaction in the SSS therefore ES never need to provide liquidity for settlement in the VPC system (SSS).

2. An FMI should have effective operational and analytical tools to identify, measure, and monitor its settlement and funding flows on an ongoing and timely basis, including its use of intraday liquidity.

Operations Settlement and Asset servicing team monitors all settlement activities including the assurance of funds being transferred to ES account in relevant central bank and also re-transferring of funds to the participants at end of day.

3. A payment system or SSS, including one employing a DNS mechanism, should maintain sufficient liquid resources in all relevant currencies to effect same-day settlement, and where appropriate intraday or multiday settlement, of payment obligations with a high degree of confidence under a wide range of potential stress scenarios that should include, but not be limited to, the default of the participant and its affiliates that would generate the largest aggregate payment obligation in extreme but plausible market conditions.

ES never takes part in a transaction so therefor no liquid resources on behalf of ES are needed for settlement in the SSS. ES offers DTGS settlement and settlement incentives regulating liquidity on all levels (settlement banks/ clearing members).

5. For the purpose of meeting its minimum liquid resource requirement, an FMI's qualifying liquid resources in each currency include cash at the central bank of issue and at creditworthy commercial banks, committed lines of credit, committed foreign exchange swaps, and committed repos, as well as highly marketable collateral held in custody and investments that are readily available and convertible into cash with prearranged and highly reliable funding arrangements, even in extreme but plausible market conditions. If an FMI has access to routine credit at the central bank of issue, the FMI may count such access as part of the minimum requirement to the extent it has collateral that is eligible for pledging to (or for conducting other appropriate forms of transactions with) the relevant central bank. All such resources should be available when needed.

ES has no credit facility in a central bank. Settlement banks in the SSS are to provide liquidity for settlement in each currency. Transactions that are unsettled at end of day are handled according to ES Account rules.

6. An FMI may supplement its qualifying liquid resources with other forms of liquid resources. If the FMI does so, then these liquid resources should be in the form of assets that are likely to be saleable or acceptable as collateral for lines of credit, swaps, or repos on an ad hoc basis following a default, even if this cannot be reliably prearranged or guaranteed in extreme market conditions. Even if an FMI does not have access to routine central bank credit, it should still take account of what collateral is typically accepted by the relevant central bank, as such assets may be more likely to be liquid in stressed circumstances. An FMI should not assume the availability of emergency central bank credit as a part of its liquidity plan.

Not applicable to ES since ES is never part in a transaction in the SSS.

7. An FMI should obtain a high degree of confidence, through rigorous due diligence, that each provider of its minimum required qualifying liquid resources, whether a participant of the FMI or an external party, has sufficient information to understand and to manage its associated liquidity risks, and that it has the capacity to perform as required under its commitment. Where relevant to assessing a liquidity provider's performance reliability with respect to a particular currency, a liquidity provider's potential access to credit from the central bank of issue may be taken into account. An FMI should regularly test its procedures for accessing its liquid resources at a liquidity provider.

There are daily controls of the performance of the participants in the SSS. Yearly due diligence is performed on all participants in the SSS.

8. An FMI with access to central bank accounts, payment services, or securities services should use these services, where practical, to enhance its management of liquidity risk.

9. An FMI should determine the amount and regularly test the sufficiency of its liquid resources through rigorous stress testing. An FMI should have clear procedures to report the results of its stress tests to appropriate decision makers at the FMI and to use these results to evaluate the adequacy of and adjust its liquidity risk-management framework. In conducting stress testing, an FMI should consider a wide range of relevant scenarios. Scenarios should include relevant peak historic price volatilities, shifts in other market factors such as price determinants and yield curves, multiple defaults over various time horizons, simultaneous pressures in funding and asset markets, and a spectrum of forward-looking stress scenarios in a variety of extreme but plausible market conditions. Scenarios should also take into account the design and operation of the FMI, include all entities that might pose material liquidity risks to the FMI (such as settlement banks, nostro agents, custodian banks, liquidity providers, and linked FMIs), and where appropriate, cover a multiday period. In all cases, an FMI should document its supporting rationale for, and should have appropriate governance arrangements relating to, the amount and form of total liquid resources it maintains.

The settlement participants only provide liquidity from accounts in a central bank.

There are daily controls of performance of the participants in the SSS. Yearly due diligence is performed on all participants in the SSS. ES Account rules regulate the calculation of provision of liquidity. here are daily controls of performance of the participants in the SSS. Yearly due diligence is performed on all participants in the SSS. ES Account rules regulate the calculation of provision of liquidity.

10. An FMI should establish explicit rules and procedures that enable the FMI to effect same-day and, where appropriate, intraday and multiday settlement of payment obligations on time following any individual or combined default among its participants. These rules and procedures should address unforeseen and potentially uncovered liquidity shortfalls and should aim to avoid unwinding, revoking, or delaying the same-day settlement of payment obligations. These rules and procedures should also indicate the FMI's process to replenish any liquidity resources it may employ during a stress event, so that it can continue to operate in a safe and sound manner.

ES SSS performs DvP settlement and DTGS 4 times a day.

Principle 8: Settlement finality

An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time.

Key consideration 1: An FMI's rules and procedures should clearly define the point at which settlement is final.

Settlement finality and the VPC-system exchange of cash to securities and vice versa is achieved by ES having standards and functionalities implemented corresponding to the "Swedish Act on Systems for the Settlement of Obligations on the Financial Market (SFS 1999:1309)" and Settlement Finality Directive. ES operates an integrated securities settlement model, in the main currency SEK, with momentarily settlement of securities and cash through accounts commissioned by the Riksbank for ES to administer settlement of payment obligations. These accounts are technically integrated into the same system as the securities, i.e. the VPC-system. Consistency is then ensured as both legs of the transaction, security and cash, are integrated and settle within the same system (the VPC-system).

For settlement in EUR and DKK the processes are identical but instead of an integrated model, as in SEK, ES holds a cash account for clients at Bank of Finland and Denmark's Nationalbank via which the settlement banks transfer cash. All cash holdings in EUR and DKK, mirrored in the VPC system, are backed by the holdings on those accounts. While the exchange of cash and securities in the system being the final stage to settlement finality it is preceded by several steps. For members to have their instructions settled these have to be matched and assessed for 'Ready to settle' prior the VPC-systems settlement cycles. Matched instructions in the VPC-system means that the instruction cannot be unilaterally revoked and that it will be included in the systems assessment of what instructions are to be marked 'Ready to settle' i.e. the establishment whether counterparties hold enough cash and securities to fulfil their obligation for the specific transaction. Information covering settlement finality in the VPC-system is publicly available on ES homepage and included in the ES Account Rules.

The VPC-system guarantees that delivery of securities only takes place if payment is simultaneously done. In regards of settlement finality, all stages of finality have been achieved as the final phase of settlement has been executed. Settlement is final upon execution and generation of records i.e. the simultaneous exchange or transfer of securities and cash (if against payment) are final at such time. Provided that all conditions are fulfilled (instruction is matched and ready to settle), the execution and generation of records occurs either

- At the end of each DTGS cycle (designated time gross settlement)
- In real time for RTGS (real time gross settlement)

Additional information relating the procedures can be found in section C in ES Account Rules with settlement finality more specifically described in section C 2.6.1.

The ES Account Rules are enforceable in case of insolvency of a participant. Transactions registered in the VPC-system prior to insolvency proceeding are subject to ordinary routines⁷.

Participants can generally feel confident that no other participant or external party can hinder the settlement of a transfer order once it has been entered into the VPC-system. Although the fact that a particular transfer order is protected and irrevocable does not guarantee actual settlement. Settlement remains dependent on a number of factors, including availability of cash and/or securities. It is also important to note that the Swedish Act on Systems for the Settlement of Obligations on the Financial Market does not regulate the validity of the underlying transaction, only circumstances on the system level⁸.

The original drafting of ES Account Rules, as well as the process of making changes to ES Account Rules, is further described under Principle 1 and Principle 23.

Key consideration 2: An FMI should complete final settlement no later than the end of the value date, and preferably intraday or in real time, to reduce settlement risk. An LVPS or SSS should consider adopting RTGS or multiple-batch processing during the settlement day.

The VPC-system allows for settlement both through DTGS intraday as per schedule set out in ES Account Rules and through RTGS.

- RTGS functionality is available on both sub markets between 7:00 until 17:00.
- DTGS cycles runs at 08:00, 10:00, 12:00 and 14:00 with the 8:00 cycle reserved for PM sub-market. All the above DTGS cycles are for both DvP and free of payment (FoP) instructions.
- Additionally there is a FoP settlement cycle for both sub-markets at 17:00.⁹

Real time status of an instruction can be found directly in the VPC-system though also available for through subscription for reports through ES different interfaces. ES provides participants with real time updates on aggregated membership level and detailed transaction breakdown level with regard to cash and security holdings.

Intraday, transactions not marked 'Ready to settle' i.e. does not fulfil settlement conditions are moved forward and continuously tried for next settlement cycle as part of the settlement process. Instruction that has not settled on intended settlement day will be re-cycled to the following settlement day.

ES has not experienced deferral of settlement between business days due to system down time or any other reason. The VPC-system had a service availability of 99,9698% during 2020. ES has taken business continuity measures, e.g. back-up data centres, back up sites for staff, mirroring of data, contingency tests etc¹⁰.

Additionally ES participants are required to have back up contingency measures in place with regard

⁷ ES Account Rules C 2.5.2

⁸ Please also view response to principle 1 relating to any legal aspects of settlement finality

⁹ Special resolution CS 2

¹⁰ Please also view response on principle 17

to communication¹¹. If there is no other alternative available the participant can input instructions via proprietary interface at ES premises.

Key consideration 3: An FMI should clearly define the point after which unsettled payments, transfer instructions, or other obligations may not be revoked by a participant.

Section C 2 in the ES Account Rules clearly defines the possibilities for a participant to revoke any instruction. Matched instructions are not allowed to be unilaterally revoked by participants. However if both parties to a matched transaction agree to cancel it, this can be achieved by registering opposite instructions i.e. 'counter book'. Participants cancelling instruction must fulfil the same settlement criteria's as the original instruction i.e. it may be the case that funds and securities have to be in place to cancel the original instruction. Participants are only allowed to cancel matched instructions up until the end of settlement day. Unmatched instructions are allowed to be unilaterally cancelled¹².

All transactions will be processed in accordance with the routines and rules of the settlement process and ES has no mandate or possibility to intervene and prevent any settlement. Nor does ES allow exceptions or extensions to the revocation deadline, but ES has the possibility, in accordance with ES Account Rules, to take extraordinary measures ¹³to avoid serious market disruption this may include (but not exclusively), serious IT disruptions in the market etc.

The above information on revocation of instructions is further described in the ES Account Rules available on ES public website¹⁴. More specifically the information could be found in section C in ES Account Rules.

¹¹ ES Account Rules A 7.4

¹² ES Account Rules C2

¹³ ES Account Rules A 11

¹⁴ www.euroclear.com

Principle 9: Money Settlements

An FMI should conduct its money settlements in central bank money where practical and available. If central bank money is not used, an FMI should minimize and strictly control the credit and liquidity risk arising from the use of commercial bank money.

Key consideration 1: An FMI should conduct its money settlements in central bank money, where practical and available, to avoid credit and liquidity risks.

ES operates securities settlement in SEK and EUR with exchange of securities and cash as per BIS model 1¹⁵. SEK settlement banks are required to be participants to the RIX system. DKK settlement banks are required to be participants in Denmark's Nationalbank. To participate as EUR settlement banks, the institute has to be participant in a payment system at a central bank and thereby have access to deposits in EUR; or by means of an agreement with a participant in such payment system, have access to deposits in euros on terms that are effectively equivalent to those applying to participants in the system. Non settlement bank clearing members have to engage an authorized settlement bank to access the Securities Settlement System ("SSS"). Settlement banks grant the clearing member limits and facilitates the clearing members liquidity needs, which becomes part of the settlement Banks own funding requirement.

SEK Settlement takes place in an integrated¹⁶ model with exchange of cash taking place directly on accounts outsourced by the Riksbank and administered by ES. While the model allows for funding through the RIX system SEK Settlement banks have the option of using the ES auto-collateralization functionality whereby securities held in the VPC- system are used to create central bank money for settlement purposes.

ES as a direct participant to Bank of Finland ("BoF") and Denmark's Nationalbank facilitates EUR/DKK funding for Settlement banks by maintaining a cash account in the Euro area payment system Target 2 through the BoF and a cash account in Denmark's Nationalbank's payment system, Cronos2. To be accepted as EUR Settlement banks must be members at a Central Bank or have an agreement with another Central Bank participant thereby having access to Euro credit. Participant funds are segregated reflected to the settlement bank EUR Liquidity Settlement Account ("**LSA**") in the VPC-system.

Key consideration 2: If central bank money is not used, an FMI should conduct its money settlements using a settlement asset with little or no credit or liquidity risk.

ES settlement in SEK takes place in Central Bank money. For settlement in EUR and DKK ES holds a cash account for clients at Bank of Finland (EUR) and Denmark's Nationalbank (DKK) via which the settlement banks transfer cash. All cash holdings in EUR/DKK on EUR/DKK LSA in the VPC system are backed by the holding on this account.

¹⁵ <http://www.bis.org/publ/cpss06.pdf>

¹⁶ <http://www.ecb.int/pub/pdf/other/useofcbmoneyforssten.pdf>

Key consideration 3: If an FMI settles in commercial bank money, it should monitor, manage, and limit its credit and liquidity risks arising from the commercial settlement banks. In particular, an FMI should establish and monitor adherence to strict criteria for its settlement banks that take account of, among other things, their regulation and supervision, creditworthiness, capitalization, access to liquidity, and operational reliability. An FMI should also monitor and manage the concentration of credit and liquidity exposures to its commercial settlement banks.

Not applicable for ES.

Key consideration 4: If an FMI conducts money settlements on its own books, it should minimize and strictly control its credit and liquidity risks.

Please see answer to key consideration 2 above.

Key consideration 5: An FMI's legal agreements with any settlement banks should state clearly when transfers on the books of individual settlement banks are expected to occur, that transfers are to be final when effected, and that funds received should be transferable as soon as possible, at a minimum by the end of the day and ideally intraday, in order to enable the FMI and its participants to manage credit and liquidity risks.

Settlement finality and the relationship between participants and ES with regard to the exchange of funds and securities are set out in ES Account Rules. Though ES Account Rules form part of all members' bilateral relationship with ES it includes sections only applicable to Settlement Banks. ES operates a settlement model with simultaneous exchange of cash and securities thus included in the ES Account Rules are sections covering the timing of settlement¹⁷, at what stage finality is reached and when finality is achieved. Funds are transferred and made available intraday to settlement banks at times corresponding to the settlement schedule as set out in ES Account Rules. Additionally ES transfers any remaining liquidity out of the VPC-system to the participant entitled to the liquidity by the end of day, i.e. end of day balances is always set to zero in VPC system.

¹⁷ ES Account Rules section C 2.

Principle 11: Central securities depositories

A CSD should have appropriate rules and procedures to help ensure the integrity of securities issues and minimize and manage the risks associated with the safekeeping and transfer of securities. A CSD should maintain securities in an immobilized or dematerialised form for their transfer by book entry.

Key consideration 1: A CSD should have appropriate rules, procedures, and controls, including robust accounting practices, to safeguard the rights of securities issuers and holders, prevent the unauthorized creation or deletion of securities, and conduct periodic and at least daily reconciliation of securities issues it maintains.

To safeguard the rights of securities issuers and holders, ES has two set of rules, ES Account Rules and ES Issuer Rules, as further described under Principle 23.

All account operators have online access to its accounts and can monitor its transactions. Statements are also produced to account holders on any change or update to the account and account holders annually receive compiled information on the account. To support the monitoring and follow-up of authorisation administration, the VPC system produces a daily report for the respective account operators showing all changes in names, addresses and bank accounts made via terminals. The report contains changes in respect of account holders, guardians, representatives, pledge holders and other rights holders, and is divided into either owner accounts or nominee accounts. In addition the VPC- system produces reports on recorded attempts made to obtain access to the VPC-system without the requisite authority.

The VPC system includes functions which make it possible to monitor which user that has performed a particular registration measure. Account operators should establish rules and routines in order to determine the persons entitled to have access to information and/or the authority to perform registration measures in the VPC system, as well as routines for monitoring and reviewing the use of allocated authorizations (ES Account Rules, section B. 1.5).

The rights of the securities holders are safeguarded by access right protocols, technical system support and standard operating procedures. All which are regularly review by Risk Management, Compliance and Internal Audit.

For holdings in foreign securities held on behalf of participants ES via CSD links has semi-automated reconciliation functionality in place which runs daily. The accounting systems for securities feature extensive logging and integrity checks to ensure correctness and traceability in the accounting process. Automated reconciliation procedures are included in the settlement process throughout the settlement day. There are also different stand-alone reconciliations in conjunction with every settlement cycle.

The VPC system ensures that the amount of issued securities (legal register) at each time corresponds to the number of securities on accounts with ES. There are therefore always sufficient securities to satisfy customer rights. For any creation of securities, ES acts upon the instruction of the issuer or the assigned account operator acting in the role of issuer agent. Further to that it also requires two unique users at ES in order to complete the execution. The standard operating

procedures stipulate a control of the registration made by Swedish Companies Registration Office prior to any creation of shares and related financial instruments registered by the Swedish Companies Registration Office. As for the creation of other securities, ES acts upon the instruction by the issuer or its assigned account operator acting in the role of an issuer agent. Any prospectuses or terms and conditions are reviewed prior to the creation and any such creation of securities is subject to the same system controls as the creation of shares and similar standard operating procedures are followed.

For the issuance related to fixed income specific clearing members authorised as issuing agents on the PM-sub market¹⁸ create securities in the VPC-system. Automatic checks are made that the total nominal value of the issuance falls within the program limit. Within the fixed income settlement it is not allowed to register instructions exceeding SEK 500 million. There are multiple procedures and controls to prevent unauthorized access to the VPC-system and controls are in place to secure appropriate reconciliations between the legal register and the sum of securities held on all accounts.

Furthermore in order for ES to delete securities, the securities need to be transferred by the account operator to an account with ES. Such a deletion is then executed upon instruction by the account operator and deletions are likewise subject to system controls and standard operating procedures.

Key consideration 2: A CSD should prohibit overdrafts and debit balances in securities accounts.

No securities overdrafts are permitted or technically possible within the settlement process in the VPC system. No credit of securities to a securities account in the VPC system can occur without a corresponding debit within the settlement process.

Key consideration 3: A CSD should maintain securities in an immobilized or dematerialised form for their transfer by book entry. Where appropriate, a CSD should provide incentives to immobilize or dematerialise securities.

ES has operated as CSD since 1971 and has since 1989 had a fully dematerialised book-entry system in place for shares and certain debt instruments. Other financial instrument safe kept by ES was included into the dematerialised book-entry system in the early 1990's. The securities held with ES are issued and maintained in a dematerialised form and evidenced by and transferred by book entry. All financial instruments issued with ES are dematerialised and all transactions apply to dematerialised securities.

As stated under principle 1 no physical certificates are allowed for Swedish securities. A very limited number of foreign securities are immobilized in foreign jurisdictions and dematerialised in local systems before they are mirrored by ES, ES does not apply immobilisation.

According to the Swedish Financial Instruments Account Act, all securities held with ES shall be dematerialised.

Key consideration 4: A CSD should protect assets against custody risk through appropriate rules and procedures consistent with its legal framework.

¹⁸ General terms and conditions, section A. 3.3.

ES accounting practices and internal controls, regularly reviewed by auditors protect account holders assets. Account holders assets, are segregated from ES own assets and thereby from the risk of loss due to ES itself. Any foreign securities held by ES via a CSD link are according to the Swedish Financial Instruments Account Act afforded the same asset protection as other securities registered at ES and as such legally protected from claims by ES creditors in case of bankruptcy of ES. The legal basis for ES links is likewise found in the Swedish Financial Instruments Account Act where it is also stated that the securities must be specifically detached for ES at the relevant foreign CSD or custodian/intermediate. Daily reconciliations are performed in order to avoid erroneous creation or deletion of securities.

On top of the authorisation administration and related traceability functions as mentioned above, the VPC-system also provides its members with various reports on securities accounts and the recording of financial instruments. It also provides reconciliation reports in real time. ES does not have any specific compensation scheme, but ES and its account operators liability is specifically regulated in the Swedish Financial Instruments Account Act.

Key consideration 5: A CSD should employ a robust system that ensures segregation between the CSD's own assets and the securities of its participants and segregation among the securities of participants. Where supported by the legal framework, the CSD should also support operationally the segregation of securities belonging to a participant's customers on the participant's books and facilitate the transfer of customer holdings.

ES does not register any own assets with the VPC-system however the segregation arrangements support two types of accounts – owner accounts, which are held in the name of the beneficial owner, and nominee accounts, which are held on behalf of the participant's customers.

Any securities belonging to the participant must therefore be held on owner accounts while the participant's customer's securities can either be held by the participant on a nominee account, on behalf of the customer, or on an owner account in the name of the customer. This segregation of securities on different account types is supported by ES Rules and the Swedish Financial Instruments Accounts Act.

A clearing member could register a number of clearing identities to segregate client's assets and the VPC-system provides for any clearing member to register transactions in such a way that they are separated from other transactions related to the same entity.

Key consideration 6: A CSD should identify, measure, monitor, and manage its risks from other activities that it may perform; additional tools may be necessary in order to address these risks.

ES provides all core CSD services as defined by the CSDR. ES also provides a limited set ancillary services under CSDR such as add-on web based services to issuers, (e.g. shareholder information) and general shareholders meeting services. ES also provides a fund order routing service.

For all its services, ES identifies, measures, monitors and manages its risks in line with its Enterprise Risk Management framework. Before new services are offered, they need to be approved after a risk assessment (see principle 3).

Principle 12: Exchange-of-value settlement systems

If an FMI settles transactions that involve the settlement of two linked obligations (for example, securities or foreign exchange transactions), it should eliminate principal risk by conditioning the final settlement of one obligation upon the final settlement of the other.

Key consideration 1: An FMI that is an exchange-of-value settlement system should eliminate principal risk by ensuring that the final settlement of one obligation occurs if and only if the final settlement of the linked obligation also occurs, regardless of whether the FMI settles on a gross or net basis and when finality occurs.

ES Account Rules¹⁹ and the technical framework of the VPC-system ensures that delivery takes place if, and only if, payment is received. There is consistency between both legs of an instruction, security and cash, as both are settled within the VPC-system. The linkage of securities transfer to the funds transfer within the VPC-system totally eliminates the principle risk. This linkage guarantees delivery versus payment (DvP), that delivery of securities will only take place if the funds are transferred simultaneously.

The VPC-system is a BIS model 1 system with each transaction settled on a trade by trade basis. ES has implemented some technical netting functionality with the aim to reduce the liquidity needs of the participants.

Matched instructions are included in a pre-settlement check, a continuous process throughout the day verifying if both participants to a transaction has delivery and payment capacity in place. Should delivering participant have sufficient holdings to deliver, receiving participant payment capacity will be checked. Should the instruction fulfil settlement criteria's it will be assigned status 'ready to settle' i.e. settlement is guaranteed and settlement finality is achieved at the end of the upcoming designated time gross settlement cycle ("DTGS").²⁰

The Swedish act on Systems for the settlement of obligations on the Financial Markets does not regulate the validity of the underlying transaction, only circumstances at the system level. It can therefore not be excluded that a third party, such as a bankruptcy administrator, may have the right to recall or otherwise prevent a transaction from reaching the final recipient, even if revocation is no longer possible within the VPC-system. In the Bankruptcy Act there is a rule related to such a situation where the bankruptcy administrator has the possibility to request that a transaction to be reversed if the bankruptcy estate reimburse what the counterparty has provided. However, such a revocation would take place subsequent to the settlement in the system and would not lead to a prevention of the settlement of a transfer order in the system²¹. An instruction that have reached status 'ready to settle' will reach settlement finality in the upcoming DTGS cycle.

¹⁹ ES Account Rules - C 2.

²⁰ Please also review response to principle 8, Settlement finality

²¹ Please also review response to principle 1, Legal basis

Principle 13: Participant-default rules and procedures

An FMI should have effective and clearly defined rules and procedures to manage a participant default. These rules and procedures should be designed to ensure that the FMI can take timely action to contain losses and liquidity pressures and continue to meet its obligations.

Key consideration 1: An FMI should have default rules and procedures that enable the FMI to continue to meet its obligations in the event of a participant default and that address the replenishment of resources following a default.

ES does not provide any credit to participants and has no financial exposure to participants (except in respect of unpaid fees). Therefore, the risk related to the default of a participant should be limited to unpaid fees at the time of the default. Such a scenario should not trigger the need for the replenishment of resources following a default.

Participant default rules and procedures

The ES Account Rules clearly define an event of default. Should a participant not meet its obligations, ES is allowed to terminate the contract or suspend its access to the system.

ES will take action following receipt of actual notice of a default event in respect of a participant. Notice may be received by various means including by way of formal information from regulators, court order or relevant insolvency practitioner.

As soon as ES becomes aware of a default, ES will suspend the participant's access to the system. Previously entered instructions will be subject to matching and settlement procedures. The participant will not be able to change existing transfer orders or enter new transfer orders while being suspended. Procedures are in place to manage the situation of participant default (communication with the insolvency practitioner, regulators, national central bank, settlement banks and participants).

As ES is not party to any settlement transactions the default of a participant will have no direct impact on ES financial resources and will not lead to any losses for ES other than in respect of unpaid fees.

Key consideration 2: An FMI should be well prepared to implement its default rules and procedures, including any appropriate discretionary procedures provided for in its rules.

ES maintains internal insolvency guidelines describing the verification and decision processes applicable to the insolvency of a participant.

The guidelines further outlines to which the information regarding insolvency should be distributed, including, but not limited to regulators, other participants, stock exchanges and other group companies.

Key consideration 3: An FMI should publicly disclose key aspects of its default rules and procedures.

ES default rules and procedures are part of ES Rules, which are publicly available on its website.

The circumstances that may lead to the suspension or termination of the contract with a defaulting participant are described in the Terms and Conditions. Additionally, ES Participant default procedure Board policy is also publicly available on its website.

Key consideration 4: An FMI should involve its participants and other stakeholders in the testing and review of the FMI's default procedures, including any close-out procedures. Such testing and review should be conducted at least annually or following material changes to the rules and procedures to ensure that they are practical and effective.

ES arranges desktop exercises with market participants and clients on continuity arrangements, market awareness and readiness. Internally ES test various guidelines and procedures related to inter alia participant defaults and ES continuously conduct various crises management tests with representative parts of the organisation. Additionally, ES conducts stress test to ascertain that it has sufficient IT capabilities. The test results are shared with the management.

Principle 15: General business risk

An FMI should identify, monitor, and manage its general business risk and hold sufficient liquid net assets funded by equity to cover potential general business losses so that it can continue operations and services as a going concern if those losses materialize. Further, liquid net assets should at all times be sufficient to ensure a recovery or orderly wind-down of critical operations and services.

Key consideration 1: An FMI should have robust management and control systems to identify, monitor, and manage general business risks, including losses from poor execution of business strategy, negative cash flows, or unexpected and excessively large operating expenses.

Definition

General business risk, called Strategic & Business risk within ES, is one of the nine key risks included in ES' risk library and enterprise risk management framework.

ES defines Business risk as short term risks (<2 years) to its financial results and solvency arising from, for instance:

- business decisions
- product and client portfolios
- human capital and other resources

ES defines Strategic risk as medium to long term risks (>2 years) to its existence and our ability to deliver our strategy, arising from, for instance:

- our strategy & business model
- strategic decisions
- implementation of strategy
- technology, IT infrastructure and software

Strategy is set by the ES Board in alignment with the overall strategy of the Euroclear Group, and driven by the ES CEO, supported by the Commercial and Product Management department.

Risk Identification, measurement, monitoring and management

The responsibility to establish and operate an effective risk management system of business risk remains with ES Board and the CEO. Please refer to Principle 3 (Framework for the comprehensive management of risks) for further details on ES' enterprise risk management framework and how it helps the CEO to identify, measure, monitor and manage risks.

Risk identification, assessment and monitoring

The first Line of defence²² (in their area of business) uses the ERM framework to identify, assess, monitor and manage risks that might impact the achievement of ES' key objectives. Each Department head is required to identify, assess, monitor, manage and report on the risks resulting from poor execution of the strategy within his/her domain and the CEO has the same responsibility for ES overall strategy. The identification and assessment process is enforced by strategic workshops at senior level and interactions with the Board.

Finance coordinates a yearly budget exercise, on revenues and costs, receiving input from all key internal stakeholders and taking into account external market evolution and potential risks. Market intelligence, regulatory changes and external sources of market statistics are used to evaluate internal revenue outcome and projections (i.e. a combination of qualitative and quantitative elements are taken into consideration in the forecasting exercise, market benchmarks are considered together with qualitative elements like policy changes on the market, etc..). In addition, Finance performs a capital and cash flow projection and planning for the next 5 years. The input for this analysis is provided by Product Management for the revenue side and each operational department for the cost side. Forecasts of volumes and revenues are formally re-evaluated on a quarterly basis. Follow-up and analysis, for both revenues and costs, is managed by Finance with the input from the relevant departments and ES CEO on a regular basis.

There are several mechanisms whereby client needs are captured, evaluated, reviewed, notably via the User Committee and relationship via the Commercial and Product departments. The Commercial Department, via the Client Relationship Managers and client facing units within Operations, holds regular meetings at senior level with the users to make sure ES products and services continue to fit their business needs.

All other support department (e.g. Legal Department) contribute to the identification, assessment and monitoring of Strategic & Business risks focusing on the current and future legal and regulatory environment.

ES has a number of means to facilitate the identification, assessment and monitoring of Strategic & Business risks. Key among them are the risk appetite framework (RAF), positive assurance report (PAR) and risk & control self-assessment (RCSA) processes which facilitate identification of key Strategic & Business risks (amongst others) that might undermine the achievement of business objectives, along with identification and assessment of relevant key controls.

Further information on the risk management processes is provided under Principle 3 (Framework for the comprehensive management of risks) and Principle 3, Principle 17 (Operational Risk).

²² The three lines of defense model operated by ES facilitates the effective operation of the ERM framework. Each line plays a distinct role providing the CEO and the Board with confidence that EB is likely to achieve its key goals through the effective management of risks. For details see Principle 3, KC 1, (« Effectiveness of the risk management policies, procedures and systems»)

Risk management in first line

ES is also deploying "Risk Champions" in the Operation and IT department to, among others, promote the early identification and monitoring of new risks or the evolution of existing risks.

ES also receive input from the Euroclear Group on their strategy, (new) developments, sales, service delivery, and bottom-line P&L. Although they are not formal governance bodies as such, they facilitate the cross-department and entities coordination to ensure consistency and alignment with the overall group strategy.

For the revenue side, the Commercial department monitors business at risk and opportunities for new business and Product Management drives the quarterly review of Market Outlook and quarterly assessment of business risks and threats over a 5-years horizon.

The Finance department monitors costs as well as the overall financial drivers including actual performance towards the financial plan. Furthermore Finance monitors that ES meet the strategic goals through a balance scorecard. Finance reports the result of the monitoring to the CEO and actions are taken for material deviations.

The key controls around revenues/costs are described in the Financial Internal Control Accountability ("FICA") control framework²³.

The ES senior management and ES Board (and its Audit/Risk Committees) monitors and regularly discusses ES' financial performance, capital adequacy and if strategic objectives will be met.

The independent control function, Risk Management (RM) is responsible for facilitating and challenging the first line on the identification, assessment, monitoring and management of Strategic & Business risks. It does this through a combination of continuous risk monitoring and analysis combined with a rolling programme of independent risk assessments. Key RM concerns are highlighted to the CEO and the Board Risk Committee through the monthly respectively the quarterly Risk Report.

Furthermore, the Internal Control System (ICS) report (fed by the by-yearly Assurance Map process) is prepared yearly to report to the Board on the effectiveness of the ES internal control system.²⁴

²³ FICA is a process aimed at evidencing execution of the control activity

²⁴ See also Principle 17, KC 1

Key consideration 2: An FMI should hold liquid net assets funded by equity (such as common stock, disclosed reserves, or other retained earnings) so that it can continue operations and services as a going concern if it incurs general business losses. The amount of liquid net assets funded by equity an FMI should hold should be determined by its general business risk profile and the length of time required to achieve a recovery or orderly wind-down, as appropriate, of its critical operations and services if such action is taken.

ES holds high quality assets (cash) to cover its general business risk, as described under KC 4. ES assesses its capital requirement for business risk under three different approaches:

- a statistical approach, which models the uncertainty of the pre-tax operating profit by forecasting safekeeping income, settlement income and net interest income
- a scenario based approach, which captures the business and strategic risk and result in a potential decrease in net profit, developed as part of the group-wide capital planning exercise
- a CSDR - related minimum requirement, corresponding to three months of operating expenses²⁵

The business capital requirement is eventually determined by taking the highest of the three approaches (i.e. minimum CSDR requirement and any loss-making outcome under the above first two approaches).

The length of time required to achieving a recovery or orderly wind-down is estimated by ES in its recovery, restructuring and orderly wind-down plan. The plan assesses the time and associated operating costs of achieving a recovery or orderly wind-down against a set of parameters (speed and timing, financial aspects, preparation criteria, etc.).

ES' recovery, restructuring and orderly wind-down plan includes a range of options – as summarised under Principle 3, KC 4. Each recovery option (including recapitalisation options; see KC 4) could feasibly be executed between 1 day and 1 month. The restructuring options considered in the plan – which comprises various cost reduction, downsizing or business/asset disposal options – carry varying execution timeframes, in some cases of up to one year.

ES' plan considers three options for orderly wind-down: sale of ES; transfer of participant assets; and close-down of operations. Based on an analysis of the timeframes that would be required to execute each option in a period of stress, and considering preparatory measures taken to support such options, ES currently estimates that an orderly wind-down would be manageable within 6 months (see KC 3, below).

²⁵ Article 4 of Regulation (EU) 390/270)

Key consideration 3: An FMI should maintain a viable recovery or orderly wind-down plan and should hold sufficient liquid net assets funded by equity to implement this plan. At a minimum, an FMI should hold liquid net assets funded by equity equal to at least six months of current operating expenses. These assets are in addition to resources held to cover participant defaults or other risks covered under the financial resources principles. However, equity held under international risk-based capital standards can be included where relevant and appropriate to avoid duplicate capital requirements.

Recovery and orderly wind-down plan

ES has developed a recovery, restructuring and orderly wind-down (RRW) plan under the supervision of the ES Board (see more details under Principle 3, KC 4). This plan details a range of recovery, restructuring and wind-down options that could be taken in the event of a threat to ES' financial viability. Among other things, the plan assesses the capacity of each option, the timeframe required to implement relevant actions, and any preparatory measures required.

The plan further contains a general overview of the corporate structure of the entity, including an overview of the intragroup interdependencies and critical functions, and a description of the external interdependencies. The plan identifies a set of relevant quantitative and qualitative indicators both coincident and leading in nature, which are monitored to detect a negative trend in ES' financial health. Trigger points are specified to allow for timely escalation to decision makers in the event of a material deterioration in the financial situation of ES.

The RRW plan is updated on at least an annual basis, or in the event of a material change in ES' business model or risk profile. Any updates to the plan are approved by ES' Board, upon the recommendation of the Risk Committee. The Board approves the approach undertaken to prepare the recovery plan and the overall selection of relevant stress scenarios and tools (incl. recapitalisation), as well as the assessment of the suitability of the recovery, restructuring and orderly wind-down tools under the various scenarios. Overall, it is important that the Board is familiar with the plan and confident in its adequacy to deal with severe threats to viability, while ensuring continuity of critical service provision to the markets that ES serves. The Board also needs to understand its roles and responsibilities in the event that it is called upon to manage a crystallised threat.

To this end, a decision-making playbook has been developed to help both the CEO and the Board to take timely and effective decisions under the RRW plan in the event that a crisis situation was escalated. In such circumstances, the ES CEO would make recommendations for approval by ES' Board. Where there were group-wide implications, the ESA Management Committee and the ESA Board would also be involved in developing and implementing required actions.

As noted under KC 2, ES has assessed that the timeframe required executing the orderly wind-down under the recovery, restructuring and orderly wind-down plan would be no more than 6 months. Accordingly, in accordance with KC 3, to implement the wind-down options under the plan ES holds sufficient liquid net assets funded by equity to cover 6 months of operating expenses. Consistent with KC 3, the six months of current operating expenses are added on top of the Pillar 2 requirements²⁶ to ensure that the capital assigned to fund an orderly wind-down is clearly conceptually separated from capital to cover other risks contemplated in sizing Pillar 2 requirements.

Key consideration 4: Assets held to cover general business risk should be of high quality and sufficiently liquid in order to allow the FMI to meet its current and projected operating expenses under a range of scenarios, including in adverse market conditions.

ES' capital is currently placed in SEK with credible banks for which the lowest long term rating must correspond to A- (set by Standard & Poor or equivalent rating). This facilitates prompt access to the cash. The rating and the concentration risk is monitored continuously by the Finance Department and the independent control functions, Risk Management, monitor the risks on a regular basis. Going forward, ES might consider other solutions for the deposit of cash to further reduce the risks.

Key consideration 5: An FMI should maintain a viable plan for raising additional equity should its equity fall close to or below the amount needed. This plan should be approved by the board of directors and updated regularly.

The recovery plans for ES include an options describing how capital could be sought from other group entities or from external shareholders. Please refer to KC 3 on more details on the recovery planning. The parent company, Euroclear SA/NV is well placed to inject capital in ES in case of need. Recapitalisation via the group's excess capital can be decided on and implemented quickly. ES may decide to raise new capital from existing or new shareholders if these measures are insufficient.

²⁶ Since the Euroclear Group includes a credit institution, EB, it is defined as a consolidated situation and all entities need to comply with the requirements formulated in the transposition of the Basel Accord into European regulation - the European Capital Requirements Regulation and the European Capital Requirements Directive

Principle 16: Custody and investment risks

An FMI should safeguard its own and its participant's assets and minimize the risk of loss on and delay in access to these assets. An FMI's investments should be in instruments with minimal credit, market, and liquidity risks.

Key consideration 1: An FMI should hold its own and its participant's assets at supervised and regulated entities that have robust accounting practices, safekeeping procedures, and internal controls that fully protect these assets.

ES recognises custody risk as a key source of risk under the operational risk category (see Principle 3 for a description of the Enterprise Risk Management Framework) and as such, integrated in the Euroclear Risk Library. Custody risk relates to both the risk of a loss of own (securities and cash) and participants' assets (cash and securities) held by us at other credit institutions, CSDs or Central Banks.

ES holds its own liquid assets with supervised, credible and credit institutions (banks) regulated by recognized Financial Supervisory Authorities. The banks must meet the set rating criteria, see Principle 15, KC 3 above. ES does not hold any securities for its own purpose. The banks are monitored by 1st and 2nd line on a regular basis. See principle 15, KC 4 for more information.

Securities are held by the participant with ES. ES is either acting as issuer CSD (where securities are primarily issued with it) or as investor CSD (where ES holds the securities with another CSD, directly or indirectly). ES maintains both direct and indirect links with CSDs and intermediaries inside and outside of the European Union.

When ES holds securities or cash with another counterpart, it performs a verification of the local legislation to ensure that securities held with such counterpart are eligible in the Euroclear System for settlement by book-entry movements and benefit from a level of asset protection that has comparable effects to the Swedish regime. A review of the relevant aspects of local legislation is performed periodically. For more details, please refer to Principle 1.

ES is also collecting tax deferrals on behalf of the clients. These funds are held in segregated accounts with banks as described above until payment.

Procedural framework

ES Network Management is responsible for the set up and the maintenance of ES' network of counterparts for the issuer CSD activity, the investor CSD activity, and their respective market environment. The principles of the set up and monitoring of such markets are described in the ES Network Management Policy Handbook which is updated and reviewed when applicable and is approved on a yearly basis by the ES CEO.

Besides verifications on the legal framework, ES performs a risk based eligibility review on the counterpart before being accepted.

As a prerequisite, ES' Compliance & Ethics (C&E) department is also involved and a counterpart cannot be considered unless C&E has provided a positive feedback on the compliance framework of such counterpart in respect of anti-money laundering and anti-terrorist financing regulations.

Once this is obtained, additional criteria are assessed, amongst others:

- creditworthiness
- regulatory status
- accounting practice
- safekeeping procedures
- control environment
- risk management principles

All these criteria are monitored on an ongoing basis to capture and assess any changing parameters and mitigate any new risk identified or existing risk which has deteriorated.

Please refer to Principle 20 for further details on the set up and maintenance of CSD links.

Protecting ES' assets and participants' securities

Asset protection is ensured through different measures.

For issuer and investor CSD activity:

- ES obtains an external legal opinion on a number of key local practices and regulations. These include asset protection, insolvency proceedings and asset accessibility as the case may be
- ES sets up contractual agreements with the relevant counterpart and ensures asset protection through specific provisions:
 - the right to inspect and audit the records at any time
 - confirmation of the absence of encumbrance on the assets (absence or waiver of lien except if mandatory under local law)
 - understanding on when settlement is final
 - clear description of insolvency proceedings under the laws of the counterpart
 - Segregation of assets
 - Strong record-keeping processes and accounting practices
 - Daily reconciliation of balances and movements with the counterpart
 - confirmation that adequate insurance coverage is in place
- an annual due diligence review process is in place. ES also uses reports from the external auditor of the counterpart (such as ISAE 3402) for its annual assessment

- in case of physical securities, such securities are kept in the vaults of depositories which are selected and monitored for this additional purpose. For the issuer CSD activity, physical securities are global notes kept through common depositories.

Key consideration 2: An FMI should have prompt access to its assets and the assets provided by participants, when required.

ES cash is deposited with recognized credit institutions and the cash is available promptly. To reduce concentration risk the funds are diversified to several credit institutions. The same applies for the funds that are held on behalf of clients (tax collection).

Participant's securities

Part of ES' requirements for the establishment and maintenance of a link is asset accessibility, meaning that ES gets prompt access to the assets when required (in business as usual and contingency mode/insolvency situation).

In the normal course of business, ES ensures prompt access to securities through relevant account structure for each link allowing access to securities without undue delay and through STP communication channels allowing ES to settle transactions and get access to the relevant reporting promptly.

In case of insolvency situations of a counterpart, the external legal opinions collected by ES for each link and for funds held by ES stipulates the proceedings to claim securities from the receiver and avoid undue delays in accessing the securities.

Key consideration 3: An FMI should evaluate and understand its exposures to its custodian banks, taking into account the full scope of its relationships with each.

ES monitors its exposures on stakeholders for all the roles they may have in the system, such as participant, issuer of securities cash correspondent and treasury counterpart (cash balances), common depository, CSD and intermediary (for indirect links).

Securities

ES exposures to custodians in relation to securities held on behalf of clients are limited to foreign securities for which ES has indirect links to direct links to other CSDs.

Cash

The management of the credit risk on the cash correspondents is based on three pillars:

- a rigorous selection process of cash correspondents
- monitoring of long balances with all cash correspondents
- monitoring on a continuous basis of the exposures on cash correspondents versus risk thresholds (market risk limits, credit limits and large exposures/concentration limit)

ES has accounts with several credit institutions in order to avoid concentration of credit and liquidity risks

Key consideration 4: An FMI's investment strategy should be consistent with its overall risk-management strategy and fully disclosed to its participants, and investments should be secured by, or be claims on, high-quality obligors. These investments should allow for quick liquidation with little, if any, adverse price effect.

General Investment Strategy

ES' investment strategy is in line with CSDR requirements and is consistent with its overall objective, as an FMI, to keep a low risk profile, especially when considering the broad characteristics of the assets ES is exposed to. Currently ES investment policy does not allow investment in securities (e.g. sovereign debt).

ES makes no investments on behalf of their clients.

Principle 17: Operational risk

An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.

Key consideration 1: An FMI should establish a robust operational risk-management framework with appropriate systems, policies, procedures, and controls to identify, monitor, and manage operational risks.

Overview of the operational risk management framework

Euroclear defines Operational Risk as the risk of loss resulting from inadequate or failed internal processes, people and systems, or stemming from external events.

Euroclear Sweden's (ES) ERM Framework Policy Handbook lists the key types of operational risks considered. They are mainly based on the Basel Committee's recommendations:

- Employment practices & workplace safety
- Clients & products
- Execution, delivery & process management
- Internal fraud
- External fraud & cyber
- Business disruption & systems failure
- Damage to or loss of physical

assets but also include:

- Custody risk
- Model risk

ES has enhanced the robustness of its Operational Risk Management Framework, following recent regulatory developments (CSDR²⁷). This includes the revision of the ES Operational Risk Board Policy (ORBP), which defines the key principles for operational risk and is developed and maintained in accordance with market practices and regulatory guidelines for risk management.

The primary goal of this policy is to define the operational risk management framework that ensures that Euroclear takes the necessary steps to effectively identify, assess, monitor and manage operational risk at all levels. The Operational Risk Management Framework also describes the roles and responsibilities for managing these risks, all relevant risk processes and the information needed to make sound management decisions.

²⁷ Regulation 909/2014 of 23 July 2014 on improving securities settlement in the European Unions and on CSD

The principles set in the Operational Risk Board Policy are then detailed in other board-approved policies and handbooks for specific types of operational risks as well as in handbooks.

The Operational Risk framework details how ES identifies, measures, monitors, reports on and mitigates its operational risk. It also oversees what is considered as "operational risk", the sources to which they are related, and the different categories where they belong.

The ES CEO is responsible for translating the Board policies into Policy Handbooks that are further expanded by the first line of defence into practical standard operating procedures.

Identification

Risk Identification is described under Principle 3, KC 1.

Specifically for Operational Risk, the process for the identification of risks is described in the "ES Operational Risk Management Board Policy.

Risk Management provides a number of standard identification tools and techniques that the business (first line) uses to identify risks, including:

- monitoring performance and risk indicators in the business (e.g. settlement volumes, settlement failures, service availability, number of operational incidents, etc.)
- performing systematic risk assessments of new products or services
- identification of single points of failures (SPOFs). A SPOF is defined as part of a system - people, processes, technology, including critical utilities and critical service providers, with no alternative or redundancy in place that, if it fails, would result in a critical operation or services being stopped
- recording of incidents, caused, for instance, by inadequate or failed processes, people and systems, or by external factors.

Management and monitoring

Once risks have been prioritised, the first line assesses how best to respond to and control the identified risk. This is done through selecting and implementing an appropriate risk response strategy (or strategies) and through introducing appropriate controls. The residual risks, resulting from the implementation of mitigating actions and controls, are then reported to and presented for acceptance to the relevant bodies as per the applicable governance

The first line of defence takes full responsibility for monitoring – via, for instance, the use of KRIs (e.g. system uptime) and reporting its risks – via for instance the PAR -Positive Assurance Reporting process & risk appetite framework, which enables first line management to provide the ES CEO and Board with direct assurance on the effectiveness of ES's risk management and internal control arrangements.

Controls are essential for risk mitigation, and specific key responsibilities are linked to the control framework. The effectiveness of ES' internal controls systems is self-assessed by the first line, supported by their review and tests and then further assessed by the second and third lines of defence (independent control functions) :

- Risk Management supports the board in defining the framework and provides independent assessments which may confirm, nuance or disagree with the first line management's views
- Compliance: provides support/advice as well as performs independent monitoring and testing of the adequacy and effectiveness of controls performed by the first line. It also

reports to management and the Board on the effective management of the compliance risks. Internal Audit independently reviews and tests the controls. It also reports to management about the adequacy and effectiveness of the control environment

ES' key controls are identified, monitored and regularly assessed in the PAR. Any defects identified (e.g. incidents, control failures, external events) results in an adjustment of the control system and is recorded in the PAR. The PAR demonstrates that controls are adequate and effective or not. A summarised view, the Assurance Map and the most important control weaknesses and the related action plans are pulled together for the annual review of the Internal Control System in the "ICS report".

Operational Incident Management on IT and non-IT incidents is handled through a central Incident system, Integrated Risk Management(IRM) tool. The tool, supports a standardised workflow for the different steps of the process covered by the 'Incident Escalation" and Loss Data Collection Procedure'.

Risk Issue Tracking is performed through the I-Track database. The I-Track database is ES's dedicated risk and issue tracking tool, which allows for effective assessment and follow-up of risks, control gaps and weaknesses that have been identified by the 1st, 2nd or 3rd line of defence. ES promotes the pro- active identification and logging of risk issues. As such the I-track database is accessible to all employees. Each issue is populated with detailed action plans that set out the specific steps needed to be taken in order to mitigate the risks faced.

The effectiveness of ES' IT Tools (and thus of Operational Risk Management tools), controls and procedures at mitigating the impact of operational risks is also assessed by Internal Audit and going forward in annual effectiveness reviews.

Fraud related policies, processes and controls

ES has an Anti-Fraud Framework, described in the Anti-Fraud Policy Handbook, which complements amongst others the Code of Business Conduct, the Speak Up Policy Handbook and the Anti-Bribery and Corruption Policy Handbook. All staffs have been informed on how to report any evidence or suspicion of fraudulent activities. All staff must on regular basis follow awareness session and complete a compliance test including questions related to fraud prevention.

ES has also implemented specific fraud risk related controls (e.g. access badge controls, controls centred on Information Security -like password protection, segregation of duties, access management, clean desk policy, endpoint security²⁸) (see also KC 5).

HR related policies, processes and controls

ES has several procedures currently in place to employ, train and retain qualified personnel, as well as mitigate the effects of personnel turnover or overreliance on key personnel. ES recruits candidates that match the qualifications, skills, experience and expertise relevant for the vacant position. A series of competency-based interviews, both by business specialists and the Human Resources-department, ensure a rigorous selection process.

All applicants are subject to pre-employment screening prior to employment by the ES. Personnel security measures reduce the risks of theft, fraud or misuse of facilities by ensuring that potential

²⁸ The security around devices (PC's, iPads, ...) accessing the network of ES

employees are suitable for their prospective roles.

Projects, programmes and change management

As part of its operational risk management framework, ES has defined guidelines - outlined in ES' Project, Program and Change Policy Handbook - for project, programme and change management. These guidelines aim to mitigate the risks arising from modifications to operations, policies, procedures and controls, enabling a successful business change. These projects, programmes and changes can be IT and non-IT related.

ES takes into account market practices and recognised industry standards such as PRINCE2, MSP and Prosci. To enable further maturity increase, this policy handbook is complemented with additional procedures, providing more details on the different steps of these methodologies.

Urgent production fixes in the VPC-system are managed through the incident management process. Incident tickets are issued and managed by Corporate Technology and Team managers within Operations.

Changes to the systems as a result of projects or improvement activities are managed by the Change Advisory Board (CAB) which relies on risk assessment practices to authorise or reject such requests.

Changes to operational applications and their supporting systems and networks are planned, developed and implemented in a controlled manner as defined in ES' Project, Program and Change Policy Handbook. The system development methodology takes into account the resilience of the infrastructure and applications which need to be respected for all critical infrastructure components and applications.

IT teams test changes within specific environments, depending on the nature of the changes and in line with our software development life cycle: in development domain (unit test), functional test domain (integration and system validation), permanent test infrastructure domain (non-functional requirements) and pre-production environment (acceptance) to validate changes and ensure non-regression before launching in production.

IT prepares reviews and signs-off Launch scenarios for any planned change. A roll-back strategy and associated actions are to be defined and included in the launch scenarios.

Key consideration 2: An FMI's board of directors should clearly define the roles and responsibilities for addressing operational risk and should endorse the FMI's operational risk-management framework. Systems, operational policies, procedures, and controls should be reviewed, audited, and tested periodically and after significant changes.

Roles, responsibilities and framework

The governance structure of ES is documented under Principle 2.

ES is a licensed CSD and operates a securities settlement system. Most of its services rely on automation and use of IT systems and applications.

The primary responsibilities of the Board are to define and oversee the implementation of the strategy and objectives of the Company, its risk framework (including risk appetite and policies) and to supervise the Company's management. This encompasses the framework for identification,

management and monitoring of Operational Risk for which the ES Board has established a dedicated policy, further implemented by the ES CEO in other policy documents. For more details on the risk management framework, please refer to Principle 3.

The business objectives of ES, as endorsed by its Board, encompass systems safety, efficiency and reliability.

The ES CEO is accountable to the ES Board for the management of operational risk and has set up a specific committee, the ES Risk and Operating Committee ("**ROC**"), to ensure day to day follow up, composed of representatives of all functions (business, support and control). The ROC has mainly an advisory role on operational activity and risk exposure topics and questions.

The ROC has the delegated authority from ES CEO to:

- Act as a 'sounding board' prior to decisions on new services, products and initiatives to ensure that risks and impacts on respective departments are considered. ROC shall make a recommendation to accept or reject the residual risk and risk mitigating actions based on the NIPP (Approval of New Initiative Product and Pricing). The CEO reviews high and critical risks. Residual risks rated as critical must be mitigated and cannot be accepted unless approved by the Board
- monitor the evolution of the risk profile and control environment, including e.g. the risk review of operational issues, e.g. incidents, risk issues (I-tracks), information security matters
- monitor the service level management of outsourced services
- monitor continuity matters as well as local security matters (e.g. health and safety, personnel security)

The ES CEO has also installed an Outsourcing- and Critical service providers Committee ("**Outsourcing Committee**"). The Outsourcing committee has the delegated authority from the ES CEO to:

- monitor the service level management of outsourced services and critical service providers
- ensure that service delivery measures are in place and are monitored on at a regular basis
- ensure actions are taken if a key service is not delivered according to plan
- ensure that the service provider meet the set capabilities i.e. financial strength, staffing, skills, contingency, information security
- ensure risk assessments are performed on a regular basis both on the service provider but also on ES capabilities to govern the service provided
- Report on a regular basis to the RC and Board on provider governance, performance, and risks.

Finally, the three lines of defence model designed by the Board and managed by the CEO facilitates the effective operation of ES' operational risk. Each line plays a distinct role in the effective management of risks:

- the first line is the owner of the risk and takes all necessary actions to identify, monitor,

manage and report the risks

- in the second line,
- Risk Management provides a robust and independent oversight of management's risk-taking activities
- the Compliance & Ethics department (C&E) ensures there is adequate monitoring of compliance with legal and regulatory requirements
- the third line (Internal Audit) provides the ultimate level of independent assurance to the CEO and Board on the adequacy and effectiveness of governance, risk management and internal controls.

More information regarding ES' three lines of defence model and Risk Management Framework is provided in Principle 3.

Review and testing

There are various mechanisms in place to ensure regular review and testing of risk policies and procedures, and control systems at large.

First of all, policies, handbooks and implementing procedures are reviewed as per defined frequency or when deemed necessary. The review shall i.e. capture changes triggered by regulation, market practices or business evolution).

Updated policies, handbooks and procedures are reviewed by adequate governance, approved in relevant governing body and followed by roll-out and implementation.

Regular business control and monitoring processes are in place, supporting the adequate and effective risk and control environment, in line with policies. Their outcome is reported and discussed in management performance meetings at different levels in the organisation (from first line white board meetings and processes monitoring to reviews by the ROC and the ES CEO).

First line testing covers a broad range of topics (for instance business continuity as part of the BCPs tests- see KC 629, - IT testing – see KC 130, and KC 4, etc.).

Testing of control design and effectiveness is performed by first line control units applying a risk based approach to derive the nature and frequency of control testing. The results are integrated into the PAR and reported to Management.

Moreover, the annual Internal Control System (ICS) review (combined with ES' "I-track" review: a systems to track the actual and timely deployment of identified remediation actions) will aim to ensure a quality review for operational procedures.

Furthermore, the risk management framework, including the operational risk management framework, is subject to both internal and external audits, by the company's external auditor. The Internal Audit department provides independent assurance on the adequacy and effectiveness of ES' system of internal controls. Control testing is performed by Internal Audit as part of their annual

²⁹ Review and Testing

³⁰ In the section Project, Program and Change Management

audit plan and by external auditors, that review internal control procedures are in place to facilitate correct financial statements.

Key consideration 3: An FMI should have clearly defined operational reliability objectives and should have policies in place that are designed to achieve those objectives.

Operational reliability objectives

The ES Risk Appetite, as approved by ES Board, includes clear targets for Business disruption and system failure, whereby ES actively seeks out weakness in its IT system and conducts tests to understand vulnerabilities. ES addresses those vulnerabilities aiming at system recovery time in less than 2 hours. ES has sufficient internal knowledge and capacity to ensure an adequate monitoring of the services provided to its clients received from its service providers. This objective is then supported by risk metrics, which are regularly updated to meet its goals.

Euroclear SA/NV supports ES on the corporate technology side (network and datacentres) under an outsourcing arrangement. The performance of Euroclear SA/NV is assessed and monitored on a regular basis through the use of qualitative and quantitative Key Performance Indicators.

Qualitative objectives are stated in the Operational Risk Management Board Policy, the risk appetite framework and in implementing procedures and published on the intranet for employees. Further quality statements can be found in the sets of control objectives used and within the departments' own internal process and standards documentation. The reliability objectives are also part of the personal staff objectives for certain staff categories.

ES is maintaining appropriate IT tools, ensuring high standards of operational reliability and security, adequate capacity and integrity and confidentiality of the information. This is defined in ES' Information Technology Framework Board Policy.

Key consideration 4: An FMI should ensure that it has scalable capacity adequate to handle increasing stress volumes and to achieve its service-level objectives.

Capacity Management

ES operates a capacity management process, resulting in a capacity plan for critical IT services, to ensure that IT capacity meets current and future business requirements. There is a continuous monitoring of defined infrastructure services (daily review and dashboards) to identify potential issues ahead of time. The capacity is monitored 24/7 towards set thresholds and actions are taken to increase capacity (or re-balance workload) as thresholds are approaching.

The capacity and system usage is analysed within CT at regular basis to ensure proactive measures can be taken.

Capacity management within project lifecycle

In the case of introduction of new technology, capacity requirements are defined in the project as part of the Project Life Cycle methodology, including necessary performance testing.

Key consideration 5: An FMI should have comprehensive physical and information security policies that address all potential vulnerabilities and threats.

Physical security

Depending on the criticality of the information/data to be protected, requirements for physical security are defined in the Information Security Management System (ISMS) Policy Handbook and further documented in the Physical Security implementing procedure.

The policy aims to ensure the implementation of physical security measures to prevent unauthorized physical access, loss, damage, theft, interference to ES' information assets and processing facilities and interruption of ES' operations. ES continuously monitor the areas where critical information is stored or processed to protect them from physical and environmental threats. Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises are specifically controlled and isolated from information processing areas.

The physical security takes into account applicable legislation, general best practices, both as defined by the parent group and as recommended by international standards like ISO 27000.

Information security

Consistent with the Basel Committee's recommendations, information security risk is a component of operational risk. Information security is defined within ES Operational Risk Board Policy and the Information Security Management System (ISMS) Board Policy as the protection of critical assets, by preserving their:

- confidentiality: ensuring that information is accessible only to those authorised to have access and is not misused
- integrity: safeguarding the accuracy and completeness of information
- availability: ensuring that authorised users have access to information when they need it
- compliance: ensuring that relevant legal and regulatory requirements in relation to the protection of information are adhered to

is ongoing.. The ISMS describes the high-level scope of ES' information security control framework as well as roles & responsibilities. The domains such as access management or vulnerability detection and remediation are provided in supporting documents (policy handbooks and implementing procedures) aligned with the ISO 27002 controls. Key controls are defined in the ISMS Board Policy covering the different domains of information security in line with ISO 27001, such as Human Resources security, Information Asset security, Access control, Cryptography, Operations security, etc. .

ES aim to ensure that its ISMS is holistic and addresses threats to confidentiality, integrity and availability in line with its low risk appetite for operational risks. All control activities are expected to be implemented by 2022

The ISMS Board Policy contains a specific section related to Cyber security. ES aims to achieve a level of cyber resilience commensurate to its role as critical financial market infrastructure.

ES monitors and manages the cyber threat landscape, regularly reviews and actively mitigates cyber risks.

ES' ISMS Board Policy sets the principles on how ES maintains the required level of information security and how ES safeguards its information assets, the interest of its key stakeholders as well as its reputation and brand. This policy is based on market best practices and recognised industry standards such as ISO27001:2013, COBIT and ITIL. It is designed to address information security's legal requirements for financial market infrastructures.

ES control and policy framework strives to be aligned with ISO 27001:2013 (main reference). In addition, ES uses other frameworks where they bring value in terms of control definition, implementation or measurement. For example, CIS controls for technical implementation on platforms or CCM controls for Cloud deployments. All these references will be mapped with the ISO to obtain global and homogenous assurance.

The ISMS Policy applies to all ES employees, contractors and third parties including any materials/facilities needed in supporting ES' business operations. Regular awareness trainings are held for all staff.

Together with the ES CEO, the Chief Information Security Officer (CISO) oversees and coordinates information security efforts across ES and supports the development of information security policies that are consistent with business objectives, risk appetite and the Enterprise Risk Management framework. The ES CEO retains responsibility for monitoring and overseeing policies, issues and exceptions that are relevant to ES and reports any relevant issues to the Business Resilience and Information Security team.

Key consideration 6: An FMI should have a business continuity plan that addresses events posing a significant risk of disrupting operations, including events that could cause a wide-scale or major disruption. The plan should incorporate the use of a secondary site and should be designed to ensure that critical information technology (IT) systems can resume operations within two hours following disruptive events. The plan should be designed to enable the FMI to complete settlement by the end of the day of the disruption, even in case of extreme circumstances. The FMI should regularly test these arrangements.

Please refer to Principle 13 ("Participant-default rules and procedures" for further elaboration on the cases of participants default which is a specific type of possible incident that could cause disruption).

Objectives of Business Continuity Management framework

The Business Continuity Management framework comprises 3 main documents:

- ES Business Continuity Strategy Board Policy: This Policy includes a description of the IT infrastructure and disaster recovery strategies of ES IT systems provided by Euroclear

SA/NV.

These strategies support the resumption of critical services with the set Recovery Time Objective ("RTO") of 2 hours and the completion of the settlement day on the scheduled date. It also describes the ESA datacentre infrastructure, with a second datacentre, providing an additional level of resilience

- ES Business Continuity Management Policy Handbook: This Policy Handbook details the requirement for IT and offices resilience which are implemented at ES. It also details the incident escalation and crisis management processes.
- ES Business Continuity and Disaster Recovery Plan (These documents are complemented by departmental BIAs³¹ and specific response plans)
- ES IT Disaster recovery plan, a description of ES' IT disaster recovery capabilities and serve a reference document for contingency/disaster recovery awareness targeting all IT staff.
- ES Cyber Response plan that describes actions to be taken in case of a Cyber event.

In accordance with legal requirements, ES' Business Continuity Management (BCM) framework describes roles and responsibilities, and the adopted approach. It also includes objectives supporting the business targets for the timely resumption of critical operations. The ES board approves the business continuity objectives and plans. The documents are updated when deemed necessary but at least annually. For any material incident a revise of the documents is considered. The scenarios of a possible long IT outage and related response plans are continuously enhanced and tested.

BCM standards are outlined in the ES Business Continuity Strategy Board Policy including:

- key definitions and principles related to Business Continuity Management
- critical business functions and key operational activities
- recovery strategy: outlines the recovery strategy to ensure the timely recovery of operations and the fulfilment of ES' obligations in case of disruptions

Governance

The first line is responsible for the coordination of the Business Continuity and Disaster Recovery Plan (BCP). Every key component of the BCP is tested once a year along the requirements set in the policy. The BCP is designed to foresee that IT systems can resume operations within two hours and includes all reasonable steps to ensure that settlement is completed by the end of the business day even in case of a disruption.

Risk Management's (second line) role to review, challenge and identify gaps in the Business Continuity Risk Assessments performed by the first line and challenge the adequacy of the documentation including Business Impact Analysis, their completeness, proposed risk responses

³¹ Business Impact Analysis

and the overall consistency. The Compliance & Ethics' (second line) role is to challenge compliance with regulations.

Internal audit (third line) performs assessments on a regular basis to ensure that ES continuity procedures are adequate, effective and efficient.

Business Impact Analysis

The Business Impact Analysis (BIA) is the foundation of ES' BCM process.

A formal BIA is used to identify the critical activities and their recovery time objectives for each of the business processes. During the BIA, threats and risks associated with business process' interruptions are identified and assessed by determining the effect of loss, interruption or disruption to business on the function of each department and thus on the organisation as a whole. The analysis considers both the short and long-term effects of an incident, and identifies dependencies on people, information, technology and facilities. The output of the BIA is used to form the Business Continuity strategy and plans, in accordance with the Operational Risk Board Policy.

The BIAs are reviewed when deemed necessary but at least annually for functions that are needed to perform the critical operations (core services in CSDR).

Business Continuity Plans

Business continuity plans have been developed to cover a number of defined scenarios, including the loss of an office, loss of staff and an IT disaster recovery incident. They contain the following elements:

- guidelines on how to use the plan
- the process to alert and activate the crisis management team
- responses and recovery procedures meant to return the business to normal operations following an incident or disaster
- procedures to continue to maintain critical activities following a widespread loss of staff
- communication guidance and contact list with supervisors, employees, key clients, critical suppliers, shareholders, management and other stakeholders
- critical contact information on continuity teams, affected staff, clients, suppliers, public authorities and media

The Corporate Business Continuity and Disaster Recovery Plan is the overarching document designed to help the organisation respond to incidents. It sets operational priorities and includes checklists and supporting information for different scenarios.

The departmental plans provide sufficient information for team members to respond to an incident. The actual content of each departmental plan varies depending on the criticality of activities.

In addition to their departmental response plans, following departments develop specific response plans:

- HR to cover all people aspects, including social unrest
-
- Facilities, to cover response to building evacuation / invacuation and access control issues (e.g. demonstrations)

- Corporate Technology plans also include procedures to achieve data / transactions consistency³²
- Corporate communication that details how ES will communicate with internal and external audiences during a crisis
- Business operations to provide a response to different financial crisis scenarios

Data centres

ES has an outsourcing arrangement with Euroclear S/A with regards to data centres. Euroclear S/A has three data centres:

- two data centres (DC1 and DC2) provide real-time synchronised data mirroring and act as the primary and secondary data centre. The distance between these two data centres is sufficient to prevent that the secondary site is affected by an event affecting the primary site. ES' critical services are supported by resilient/adequate:
 - IT platforms (hardware and software)
 - networks configurations
 - communication means
 - capacity to process all transactions before the end of the day even in circumstances where a major disruption occurs
- a third data centre (DC3) receives asynchronously replicated data. It allows recovery of critical data in the event of a regional disaster affecting both other data centres (like a coordinated attack or a major earthquake).

System resilience

The system development methodology adopted by the IT department includes principles and guidelines with regard to resilience of the infrastructure and applications which need to be respected for all critical infrastructure components and applications. Compliance with these principles and guidelines is evaluated for every project or change as part of the production acceptance criteria. The core processing systems and networks are designed to provide resilience through the use of mechanisms including mirroring (synchronous) of production data, the use of fault tolerant computers or resolving single points of failure. The provision of the communication lines is split across a number of telecommunications suppliers thereby providing additional protection against a single point of failure.

³² Reconciliation procedures exist to deal with the limited data loss that may occur in extreme circumstances (simultaneous failure of DC1 and DC2, rolling disaster).

Implementing procedures

The objectives of the Business Continuity Management (BCM) Policy Handbook which are embedded into ES' business culture, are to:

- *outline the BCM system in which ES operates*
- *ensure that:*
 - ES is prepared to respond to impacts resulting from a disruption to service
 - all Employees understand their roles and responsibilities when responding to disruptions and have a clear understanding of the course of actions to be followed to respond to such disruptions

Procedures and checklists are maintained and made available in various ways to enable that all involved staff (including members of the ES MC or of the Board as the case may be) can perform effective management and control of the services at all times, also in case of emergency.

Standard introductory training for new ES staff explicitly covers business continuity in general and personal responsibilities. BCP awareness updates, exercises and training are provided regularly each year to all ES group staff, using different communication channels and tools.

Synchronous mirror production

The core processing systems synchronously mirror production data between DC1 and DC2. Hence, the status of all transactions is known even in case of a disruption affecting one data centre.

Data Loss Response plans have been developed by operations specialists to minimise the impact of data loss whilst aiming to resume computerised operations in a time period which does not cause unnecessary strain on market stability. Depending on the circumstances, ES could decide to resume operations while some reconciliation activities are still being run in parallel (see ES' Terms & Conditions for more details).

The Data Loss recovery principles are:

- records of transactions held by National Central Banks (NCBs), Central Securities Depositories (CSDs) occurring during the suspected period of data loss will be considered by ES to be the 'master' source
- at all times ES is the 'master' source for clients. This may result in previously executed transactions requiring re-execution by clients following resumption of operations
- clients will be informed of their obligation to evaluate the status of trades throughout and following recovery

Crisis management

In order to ensure a systematic and coordinated response to unexpected events, ES established a three-tiered Bronze-Silver-Cross Silver - Gold crisis management structure. These levels deal with operational - tactical - strategic issues respectively.

Communication to internal and external parties during and after an incident forms an essential part

of the incident response. The Crisis Management teams are required to assess the need for communication and if so, to communicate to clients, clients facing staff, other staff, and, from Silver on, also to supervisory authorities and to the press.

Client communication is to be initiated as soon as possible, with a threshold set at 30 minutes after the calling of the Bronze meeting. The *Crisis Management* guide also gives guidelines on the message contents.

Secondary site for office services

ES has implemented a 'dual office' as a backup site strategy for staff, with geographically -dispersed business operation sites to limit the risk that a single event will impact a main site and its back up. Business resumption is tested at least four times per year to make sure that in case one site is unavailable, all critical activities can be operated from another site.

Review and testing

The Business Continuity Policy is reviewed annually and considers changes to ES' risk profile, business objectives, operational environment, legal and regulatory requirements and market expectations.

The main BCP scenarios tested include all scenarios listed in CSDR such as loss of office, staff, infrastructure, critical provider and financial crisis impacting the market. The different root causes that may lead to such impacts are identified in ES' Business Continuity Strategy Board Policy.

A formal BCP test framework is maintained indicating how and when each element of the plan is tested. The test framework helps ensure that all elements of the plan are tested at least once a year along the requirements set in the policy.

First line has the overall role of coordinating and promoting BCP testing and reviews. It also consolidates management reporting of the testing and its outcome to management, Audit and Risk Committee and to the group. These tests include:

- IT disaster recovery testing: Production is transferred from data centre one to data centre two at least four times per year
- office switch tests, simulating the loss of a single office is organised at least four times a year for each department running any critical function
- several crisis management exercises (alerting tests or simulation exercises) are organised each year
- testing of agreed arrangements with external parties (clients, business partners, critical providers, other FMIs...)
- involvement in market-wide exercises where and when they are organised

The BCP solution and recovery plan including the switch of processing between sites is designed not to be impacting clients. This means that clients will not know from which of the IT centres the services are provided or if there was a switch of the processing site. There is not any particular action for a client to take during a BCP test.

Key consideration 7: An FMI should identify, monitor, and manage the risks that key participants, other FMIs, and service and utility providers might pose to its operations. In addition, an FMI should identify, monitor, and manage the risks its operations might pose to other FMIs.

Risks to the ES own operations

ES defines Operational Risk as the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. ES continuously seeks to identify and manage risks posed to its business and the effective delivery of its services. ES also endeavours to limit its own contribution to systemic risk and ensure it remains within its risk tolerance.

The Operational Risk Board Policy sets out key operational risk management principles, while the underlying handbooks defines specific methods for the identification, measurement, monitoring and reporting of operational risks, in line with the general framework.

ES has also developed tools and techniques for the handling of specific risks³³, e.g. single points of failures, incidents, manual intervention, etc.

The operational risk framework is further elaborated in dedicated frameworks, including:

- business continuity management
- client admission & on-going monitoring
- information security management
- Information Technology
- services by Third Parties (covering Outsourcing/Critical Service Providers and Links, Market infrastructure)

Key Participants and key agents (network management) are covered by the BCP arrangements. Furthermore, ES has uplifted its approach to systemic risk, both from the perspective of its own resilience to systemic risk (i.e. a systemic risk crystallising in the market and hitting ES) and its potential contribution to systemic risk (i.e. a systemic risk coming from ES and impacting the market).

Critical Service Providers (CSP)

ES may outsource certain services and activities to third party providers, wherever those providers are, inside or outside of the Euroclear Group. ES has designed a robust outsourcing framework, which consists of a defined life cycle which relies on a strong governance, an internal control system and Euroclear best practices around the management of risks, including conflicts of interests.

Service delivery is reviewed on a regular basis. Services are measured and compared with targets to identify whether the objectives are met, and where applicable, what actions need to be taken to improve the service. See KC2 for details on the Outsourcing Committee.

IT Services

ES has its internal IT team focusing on the settlement system (VPC). ES has outsourced critical IT

³³ Reconciliation procedures exist to deal with the limited data loss that may occur in extreme circumstances (simultaneous failure of DC1 and DC2, rolling disaster).

services (i.e. Network and Datacentres) to Euroclear SA/NV which is the parent company of ES. The relationship with the provider is defined in a formal agreement including service level agreements. Service delivery is reviewed on a regular basis through qualitative and quantitative Key Performance Indicators (KPI). Corrective actions are requested when the agreed KPI's are not met. See KC2 for details on the Outsourcing Committee.

Users and links

ES has defined access criteria to avoid that a participant could be disruptive for the system (see Principle 18 ["Access and participation requirements"] for more information).

ES furthermore continuously invests to encourage participants to manage and contain the risks they pose to Euroclear, by keeping them informed- through user documentation, operational reporting and training, relationship (via user committee or client facing relationship) and by applying other types of measures (i.e. charges to deter riskier behaviour, sponsorship process at admission) – as detailed in Principle 18 ("Access and participation requirements") and Principle 3 ("Framework for the comprehensive management of risks") KC 2. There are procedures in place to continuous monitoring of system usage and by incitements by clients to follow the established user rules.

In the framework of its links reviews, ES reviews operational risks aspects, including the business continuity plans of all counterparts involved in the CSD link. See earlier in the text, under Business Continuity considerations and Principle 20 for more details.

Risks posed to other FMIs

The risks that ES bears from or poses to other FMIs are identified and assessed under the principles set out in the ERM Framework Policy Handbook and in the Systemic Risk Policy Handbook.

To operate a comprehensive risk management framework built on established standards and market practices, ES has enhanced its framework for Systemic Risk Management, which will allow ES to better identify, monitor and manage those risks. This includes the use of interdependency maps and horizon scanning and the outcome from cooperation in relevant for a on the Swedish market (i.e. Fidinans, FSPOS).

The enhancements to the systemic risk framework are mentioned also in Principle 3 KC 3. Principle 20 ("FMI links") further elaborates on the risks posed to or by other FMI's.

Principle 18: Access and participation requirements

An FMI should have objective, risk-based, and publicly disclosed criteria for participation, which permit fair and open access.

Key consideration 1: An FMI should allow for fair and open access to its services, including by direct and, where relevant, indirect participants and other FMIs, based on reasonable risk-related participation requirements.

ES operates a transparent participation process on a non-discriminatory basis with participation criteria's publicly disclosed on home page through ES Account Rules. Additionally, ES retain a fully disclosed participation process detailing necessary documentation for a complete ES membership application³⁴ and to support interested parties. A document detailing the ES affiliation process, Participation in ES³⁵ is available through the webpage.

Different memberships are offered at ES and interested parties can apply for one or more roles depending on business needs. All membership applicants are assessed against the same access criteria, though depending on the role applied for. While they may differ in details the structure of criteria's remain harmonized cross the various roles.

While ES maintains the membership structure on non-discriminatory basis only applicants able to demonstrate the ability to be coherent with ES requirements, including in applicable cases legal requirements, are approved for membership. Applicants will be subject to a risk assessment on a non-discriminatory basis.

Account operator

Account operators is the role that have a technical connection with ES allowing them to register instructions in the VPC-system including the right to set up VPC accounts for account holders on ES' behalf and to make registrations in the account on the instructions of the account holder and in accordance with the LKF. The account operating functions are accessed via terminals, file transfers and/or computer to computer communications.

Requirements for participation as account operator are specified in Chapter 3, section 1, 2, 4, 6a, 6b and 6c of the Central Securities Depositories and Financial Instruments Accounts Act and in section A 3 in ES Account Rules.

Only legal entities having a valid Legal Entity Identifier (LEI) code may be accepted as account operators.

Issuer Agent

An issuer agent is an account operator with a special authorisation to act in conjunction with the issuance of financial instruments or other kinds of corporate actions where the participation of an issuer agent is required to cater for e.g. response handling from holders of financial instruments in accordance

³⁴ https://www.euroclear.com/dam/wew/Brochures/Documents_in_English/Euroclear-Sweden-Application-Instruction.pdf

³⁵ https://www.euroclear.com/dam/wew/Brochures/Documents_in_English/Participation-in-Euroclear-Sweden.pdf

with the ES Issuer Rules³⁶.

An issuer agent acts on instructions from the issuer and carries out the registrations resulting from the issuance or corporate action. In order to be permitted to process issuance and corporate actions in the PM sub-market, an issuer agent must also participate as a clearing member.

Nominee

A nominee is the role that in accordance with Central Securities Depositories and Financial Instruments Accounts Act can hold financial instruments on behalf of others, i.e. as the representative for one or more investors in relation with ES. A nominee can therefore hold so called nominee accounts. By request of ES, nominees are required to provide information about underlying owners (known as nominee reporting). A nominee, who is not an account operator and therefore does not have a technical connection to ES, must utilize the services of an account operator for this function.

Nominees normally manage the holdings of individual investors in their own custodian system, where holdings are mirrored on an aggregated level to one or more nominee accounts at ES. A nominee shall ensure that the customer's securities do not become intermingled with any of its own holdings.

A nominee is responsible towards the underlying customer for the administration, for example notification of holdings and the processing of corporate action. A nominee is also responsible for withholding of taxes and reporting to the Swedish Tax Agency.

Participation as a nominee may be granted to companies that may be registered as nominees as specified in Section 3, subsection 7 of the Central Securities Depositories and Financial Instruments Accounts Act and section A 4 in ES Account Rules.

Only legal entities having a valid Legal Entity Identifier (LEI) code may be accepted as nominees.

Clearing Member

A clearing member participates in ES's clearing and settlement and is responsible for trade instructions entered to the VPC-system by an account operator for settlement. The clearing member is responsible for ensuring that securities and payments are settled on intended settlement date. Where the clearing member is not itself a settlement bank, a settlement bank authorised by ES shall be appointed for making payments.

Clearing members may participate in the clearing process in one or more sub-markets and currencies, i.e. the AM (Equity market) and/or PM (Money Market) and regarding SEK and EUR.

A clearing member participating in the AM sub-market, not acting as an account operator, is obliged to utilise an account operator for registration on the securities account of the buyer or the seller. A clearing member participating in the PM sub-market must, however, be an account operator itself as the transfer instructions reported by the clearing member to the VPC-system for settlement in the PM sub-market also entail registration in the buyer's or the seller's securities account.

A clearing member can participate with various clearing member identities (CIDs), for example, one CID for own activities and another CID for a customer.

³⁶ <https://www.euroclear.com/sweden/en/om-oss/regelverk-Euroclear-Sweden.html>

Only legal entities having a valid Legal Entity Identifier (LEI) code and eligible to be a participant in a settlement system pursuant to section 8 in the Swedish Act on Systems for the Settlement of Obligations on the Financial Market (SFS 1999:1309) and section A 5 in ES Account Rules may be accepted as clearing members.

Settlement Bank

A settlement bank supplies services related to the settlement of payments. A settlement bank operates on behalf of one or more clearing members, and handles the disbursement or receipt of payments at settlement. Settlement banks may choose to participate in one or more sub-markets and in one or more currencies. A settlement bank that is not an account operator and therefore does not have technical connection to ES must utilize the services of an account operator for this function.

As a settlement bank for payments in SEK, the institute must be an authorized participant in the payment system of the Riksbank.

As a settlement bank for payments in EUR, the institute must be a participant in a payment system at a central bank and thereby have access to deposits in EUR, or by means of an agreement with such participant, have access to deposits in EUR on terms equally efficient as those applying to participants in the system.

Key consideration 2: An FMI's participation requirement should be justified in terms of the safety and efficiency of the FMI and the markets it serves, be tailored to and commensurate with the FMI's specific risks, and be publicly disclosed. Subject to maintaining acceptable risk control standards, an FMI should endeavour to set requirements that have the least- restrictive impact on access that circumstances permit.

The requirements for participation are justified in terms of safety and aim to limit specific risks, including operational risks (such as Technical connection, organisation and risk management), financial risk (capital resources) or legal risks and risks in general (Suitability in general).

The requirements are viewed as objective as they are focused on minimizing the risk for a participant causing disturbance in the processes within the VPC-system. All classes of participation are subject to the same set of criteria. However there may differences depending on specifics of the role or specific needs due to regulation.

A prerequisite for access as clearing member³⁷ is that the applicant have the necessary authorization from SFSA or there counterpart in regards of foreign applicants. In regards of the role as settlement bank for SEK, a prerequisite is that the applicant is a member of the RIX – system.

ES continuously assess the admission criteria's from a risk and regulatory perspective with the application process review at least annually. ES Account Rules are publicly disclosed on our homepage including

criteria's and requirements for SSS participation.

³⁷ Section 21, subsections 1 – 5, Section 8, the Swedish Act on Systems for the Settlement of Obligations on the Financial Market (SFS 1999:1309)

Key consideration 3: An FMI should monitor compliance with its participation requirements on an ongoing basis and have clearly defined and publicly disclosed procedures for facilitating the suspension and orderly exit of a participant that breaches, or no longer meets, the participation requirements.

ES maintains an operational structure for real time monitoring of the settlement process including participant's operational performance. This includes assessment of participants and their ability to adhere to the requirements.

ES operational staff monitor the settlement process in real time with monitoring tools set up to detect participants violating the operational requirements, this could be participants not supplying enough funds to allow transactions to settle or other actions that may be detrimental to overall market efficiency. Violations will result in ES Market Supervision functionality releasing an Incident report within 24 hours, this is expected to be answered by involved participants no later than 5 business days from receive date. Participants are expected to describe underlying reason and steps taken to prevent future violations. ES actions following an incident can differ however may be one of the following measures; such as setting up a meeting with management at the participant, urging them to attend our training sessions etc.

Serious breaches of ES rules will result in an escalation of the incident to operational management and ES CEO.

ES Account Rules states that any information that may affect the right for a participant to act within the VPC-system³⁸ must be reported to ES without any delay. Additionally, the ES Account Rules give us the right to conduct any necessary inspection at the premises of the participant³⁹.

The participant has the right to terminate its membership at ES, though with the responsibility to wind down its operations in orderly fashion⁴⁰. ES has the right to terminate a membership of a participant if the participant contravenes the provisions set forth in ES Account Rules, the participant runs into a insolvency proceeding (or similar) or the conditions for applying ES rules in the participants home country no longer exists⁴¹. ES also have the right to temporarily exclude a participant, giving the participant the possibility to take corrective measures⁴².

The procedures for termination of a participants membership is part of ES Business Continuous Plan (BCP). Also, in our ES Account Rules there is a section covering the termination of a membership⁴³.

Our ES Account Rules are available on our website. Termination of membership is part of the ES Account Rules. ES publicly disclose a high level BCP on the homepage.

³⁸ General terms and conditions A 9 section 9.2.

³⁹ General terms and conditions A10 section 10.1

⁴⁰ General terms and conditions A10 section 10.1

⁴¹ General terms and conditions A 10 section 10.2.1.

⁴² General terms and conditions A 10 section 10.2.2. and 10.2.2.1

⁴³ General terms and conditions A10.

Principle 19: Tiered participation arrangements

An FMI should identify, monitor, and manage the material risks to the FMI arising from tiered participation arrangements.

Key consideration 1: An FMI should ensure that its rules, procedures, and agreements allow it to gather basic information about indirect participation in order to identify, monitor, and manage any material risks to the FMI arising from such tiered participation arrangements.

Tiered participation arrangements

ES has established a plan to ensure we meet CSDR requirements in relation to key participants (including any material dependencies with their underlying clients). ES only has a contractual relationships with its direct participants (direct participation model) and it does not pose itself in the relationship between participants and their underlying clients.

Clearing members are responsible for the execution of all transfer orders registered in the VPC-system on behalf of the clearing member. Even in cases where the trade initiated, the transaction has been initiated by a party other than the clearing member itself, it is nevertheless the duty of the clearing member to ensure that the delivery of the securities and the payments registered under the clearing member identity of the clearing member can be settled on the agreed settlement day⁴⁴.

Participants can choose to open segregated accounts for their underlying customers, yet remain opaque as to who these clients are since tiered participation arrangements can exist in several layers.

There are members to a market place or other trading facilities who provides settlement services by use of an ES participant. This indirect participant may in turn provide clearing and settlement services to a stock exchange Non Clearing Member hence a the direct participants settlement purposes becomes layered against ES. In these cases, the direct participant takes full responsibility vis-à-vis ES, and is liable to ES for all activities and for transactions submitted. From this follows that the direct participant should impose such rules on its underlying customers, so that the direct participant is able to fulfil its obligations with regard to settlement in the VPC-system.

Risks to the FMI

As ES has no contractual relationship with participant's clients, there is no credit, legal, market or liquidity risk to ES from them. Nor do ES have technical connections to them, and thus no system participation commitments vis-a-vis them

Risks from underlying customers need to be mitigated by the participants, as only they are liable to ES. ES handles risks from participants (participation criteria, regular due diligence checks, etc.), but not beyond the participant. Actions undertaken and transactions submitted to ES from a participant, includes what comes from their underlying customers. Risks to ES are therefore seen as risks stemming from the direct participant.

⁴⁴ General terms & Conditions, section C3.

Clients to our participants do impact volume and turnover level of the participants hence these are included in ES overall assessment of members from a performance point. This is the case from a funding especially from a funding perspective with standardized tools, processes and measures in place to monitor the performance of participants in these aspects.

Key consideration 2: An FMI should identify material dependencies between direct and indirect participants that might affect the FMI.

ES have no information of the contractual relations and dependencies between participants and their clients.

As said above, due to the nature of the CSD business there are no credit, legal, market, or liquidity risk from participants clients that can have impact on ES.

For operational risk there might be impact on the CSD from these dependencies:

- Volume fluctuations from underlying clients can be visible in the CSD transaction flow (as far as they are not netted in other systems before reaching ES). Huge volume fluctuations can cause operational problems for a participant.
- Delays (e.g. in securities deliveries or meeting other deadlines) from underlying client can be propagated to ES, unless the direct participant can absorb the risk e.g. with securities loans. Delays can affect the settlement ratio.

These risks are ES controlled by the leverage ES has on its contractual parties, i.e. the participants: if the participants fulfil the contractual obligations to ES (the participation criteria, the ES rules, the ES deadlines, the need to have sufficient capacity, trained staff, etc.), then ES have operational risks from them. If participants do not fulfil the above, they carry the full responsibility via ES and they are the ones ES can exercise sanctions against.

There are also dependencies from the underlying clients point of view:

If an FMI chooses to go to ES via another party, i.e. via a direct participant, they are of course creating a dependency of the ES-functioning of that participant. Should the participant get operational problems or even default, it may have large negative impact on the underlying FMI. It must be a conscious assessment and business decision of the FMI on the option whether to be a direct participant or to go to ES via one or several other FMIs.

ES encourages FMIs to be direct participants to the CSD in order to minimize their risks and dependencies.

Key consideration 3: An FMI should identify indirect participants responsible for a significant proportion of transactions processed by the FMI and indirect participants whose transaction volumes or values are large relative to the capacity of the direct participants through which they access the FMI in order to manage the risks arising from these transactions.

For the purpose of orderly and robust settlement ES monitor the participant behaviour to preserve operational stability and to maintain efficient settlement of transactions. Part of this is to have members oblige to very high standards of the ES rules and regulations in terms of robust operational resources partly it is to ensure members behave in a way that is not detrimental to the overall

market efficiency.

Through extensive arrangements, it is ensured that members are able to access and settle own and client trades under severe circumstances. While ES is not itself financially exposed to the performance of indirect members to the SSS this is the case for direct members settling on behalf of such actors. ES monitors the performance on membership level for both sub-markets, and even on trading counterparty level for the AM-submarket, trends to volume and turnover are observed by use of detailed member & market data available to ES. Through market analysis trends that may impact settlement at ES are detected and if possible appropriately addressed by ES. For bilateral settlement of trades at ES there is retained transparency as to a preserved one to one relationship between trade and settlement on direct participant, indirect participant or in some cases a non-clearing participant level (majority of ES settlement stems from trades executed at market place). Hence ES may observe behaviour detrimental to operational robustness and market efficiency even for indirect members and decide on necessary actions based on the contractual relationship with the direct member. Though this approach is limited to the operational risk in the sense that ES ensure that even though the direct participant is exposed to severe disturbances it can maintain its operation functionality i.e. settlement of transactions and book-entry transactions. This to prevail the overall market stability by through the operational functionality of the securities settlement system. With the possibility of very opaque multiple layering between market participants ES has no means or need to track such participation instead this form part of the assessment of the direct participant. ES focuses on securing that the direct participants are fulfilling their obligations to ES, including having sufficient capacity to handle its volumes, wherever they originate.

Key consideration 4: An FMI should regularly review risks arising from tiered participation arrangements and should take mitigating action when appropriate.

The required rules and procedures concerning ES settlement services are documented in the ES Account Rules, published on the Euroclear website. Transactions and other business interaction from tiered participants are covered by ES Account Rules when they pass via direct participants. Changes to ES Account Rules are further described under Principle 23.

ES monitors the system and participants for capacity, volumes, settlement ratio and other measurements. ES also pay due diligence visits to direct participants to verify that the participation criteria are fulfilled. ES take mitigating actions when relevant, e.g. to cater for changed volumes, changed market practices or unsatisfactory participant performance, e.g. concerning the settlement ratio or incurred delays.

Principle 20: FMI links

An FMI that establishes a link with one or more FMIs should identify, monitor, and manage link-related risks.

Key consideration 1: Before entering into a link arrangement and on an ongoing basis once the link is established, an FMI should identify, monitor, and manage all potential sources of risk arising from the link arrangement. Link arrangements should be designed such that each FMI is able to observe the other principles in this report.

ES primarily establishes FMI links directly against CSDs or (I) CSDs though for some markets ES has indirect (use of intermediary) FMI links in place. All links are setup as per the standard CSD link model⁴⁵

i.e. ES (Investor CSD) maintains a securities account by becoming member to the corresponding (i)CSD (Issuer CSD). This provides all ES arrangements with a very clear and robust legal, operational and supervisory framework surrounding all aspects of the link agreement especially with regard to responsibilities of involved parties“.

Prior to enter into link agreements, ES performs a comprehensive due diligence that covers link arrangements, market characteristics while also including the assessment of the Issuer’s ability to be compliant with ES Account Rules. The due diligence builds around a risk analysis of the link emphasizing contingency routines and operational risks with regard to link arrangements. Furthermore the due diligence includes a legal and an operational part detailing characteristics such as the availability of segregated accounts, local market practice, applicable local legislation and other legal issues assessed against ES policies. For links that are in place ES ensures that arrangements remain appropriately designed by an annual assessment based on the same principles as the due diligence.

Where ES members are also FMIs, the relationship is regulated as per the ES Account Rules and regulation. Several FMIs have established direct links with ES with four CCPs and the Riksbank currently being members of ES. As all FMIs are members of ES, they are all subject to ES Account Rules while also being subject to ES IT & and operational procedures for monitoring of settlement.

Key consideration 2: A link should have a well-founded legal basis, in all relevant jurisdictions, that supports its design and provides adequate protection to the FMIs involved in the link.

ES ensures that any counterparties to link arrangements are under supervision by local regulatory authorities and that its legal framework and domestic law do comply with ES Rules. Design and procedures of the link are assured to be adequate in relation to the legal framework within which ES operates when service level agreements and account structure are setup. Additionally, to safeguard ES and its participant’s real time reporting through network carriers such as SWIFT, provide data for reconciliation and confirmation of performed instructions thus making sure that adequate protection is continuous.

While all links agreements are established only for the purpose of free of payment transfer no links

⁴⁵ Here Standard model refers to a CSD being a standard participant to the correspondent “foreign” CSD, interested readers can find more information relating to the model at

are setup unless ES can ensure that the integrity of its operations remains intact with no legal uncertainty regarding settlement finality allowed. This setup provides members a clear and sound framework providing transparency in terms of settlement finality and legal obligations.

Currently ES has security links established with

- the British securities depository Euroclear UK & Ireland,
- the ICSD Euroclear Bank; and
- the Swiss securities depository SIX SIS AG (SegaInterSettle).

Additionally, security links are in place, this is the case with

- BBH (US markets),
- Nordea Bank (Estonia),
- Nordea Bank (Finland), and
- Danske Bank (Denmark)

ES has IT surveillance in place 24/7 and operational staff in place between 06:45-17:00 CET monitoring links settlement. Established links are annually assessed by ES.

Key consideration 3: Linked CSDs should measure, monitor, and manage the credit and liquidity risks arising from each other. Any credit extensions between CSDs should be covered fully with high-quality collateral and be subject to limits.

ES does not act as a credit institution, nor does ES grant credit to its participants in any form. ES handles all cash distributions in accordance with its routines and procedures.

Key consideration 4: Provisional transfers of securities between linked CSDs should be prohibited or, at a minimum, the retransfer of provisionally transferred securities should be prohibited prior to the transfer becoming final.

ES does not allow preliminary transfers.

Key consideration 5: An investor CSD should only establish a link with an issuer CSD if the arrangement provides a high level of protection for the rights of the investor CSD's participants.

With all links setup as ES becoming member to the Issuer CSD it is essential that membership rules and the regulatory framework of the Issuer CSD does not defer any of the obligations ES has with its participants. Given the preparations and due diligence performed by ES prior to engaging in link activities with an Issuer CSD the rights and obligations relating to ES participants are ensured. For example this will create clarity and transparency surrounding finality, ownership rights and obligations.

Once a link has been established, i.e. ES becoming Investor CSD to the Issuer CSD, arrangements are assessed at least on annual basis and continuously monitored through electronic real time access to accounts offered by the provider. Additionally real time reporting through network carriers such as SWIFT, provide data for reconciliation and confirmation of performed instructions. ES has IT

surveillance is in place 24/7 in addition to ES having operational staff in place between 06:45-17:00 CET monitoring link settlement. Established links are also, at least annually, assessed by ES to ensure compliance with ES standards. ES also performs legal assessments on its link arrangements on a regular basis.

Key consideration 6: An investor CSD that uses an intermediary to operate a link with an issuer CSD should measure, monitor, and manage the additional risks (including custody, credit, legal, and operational risks) arising from the use of the intermediary.

ES FMI links are setup as per the standard model arrangement i.e. access is achieved by to the other FMI and only for the purpose of free of payment transfers. When an indirect yet standard CSD link is setup, access is achieved by use of intermediary. For ES This is the case for links against the US markets (BBH), Finland (Nordea), Estonia (Nordea) and Denmark (Danske Bank) and the principle is the same as with direct membership thus ES oblige to membership criteria's at the corresponding Intermediary to access the Issuer CSD. Hence relationship and liabilities in such a case are regulated as per ES being a member to the intermediary yet by performing extensive due diligence, risk analysis emphasizing contingency routines and potential operational risks it is ensured that agreements do not contradict ES low risk profile and that the arrangement of the link corresponds to the supervision regime under which ES operates. Additionally ES annually assess link arrangements to ensure that this remains observant of ES policies. ES also performs legal assessments, on its link arrangements on a regular basis.

Besides at least annually assessing its link arrangements ES has stringent operational procedures in place for all Intermediary relationships. Besides 24/7 IT monitoring ES has operational staff in place between 06:45 and 17:00 monitoring settlement with all holdings to a minimum tied out on a daily basis.

Key consideration 7: Before entering into a link with another CCP, a CCP should identify and manage the potential spill-over effects from the default of the linked CCP If a link has three or more CCPs, each CCP should identify, assess, and manage the risks of the collective link arrangement.

Not applicable for ES

Key consideration 8: Each CCP in a CCP link arrangement should be able to cover, at least on a daily basis, its current and potential future exposures to the linked CCP and its participants, if any, fully with a high degree of confidence without reducing the CCP's ability to fulfill its obligations to its own participants at any time.

Not applicable for ES

Key consideration 9: A TR should carefully assess the additional operational risks related to its links to ensure the scalability and reliability of IT and related resources.

Not applicable for ES

Principle 21: Efficiency and effectiveness

Key consideration 1: An FMI should be designed to meet the needs of its participants and the markets it serves, in particular, with regard to choice of a clearing and settlement arrangement; operating structure; scope of products cleared, settled, or recorded; and use of technology and procedures.

Euroclear Sweden, part of Euroclear Group which is user-owned and user-governed, operates in a competitive environment and constantly strives to meet the needs of its participants and the markets it serves.

Euroclear Sweden, as Sweden's CSD, has established an advisory committee together with the market, the User Committee. It is the primary source of feedback and interaction between Euroclear Sweden and its user community on all significant matters affecting the market: the User Committee serves to voice the opinions of the market participants.

To ensure that the suggestions of the User Committee accounts for the variety of participants in the Swedish market, the committee's membership reflects Euroclear Sweden's client base, and it is composed of representatives of the main relevant market segments.

The User Committee is regularly informed of the performance of the Euroclear system, as well as audit findings relating to the topics covered by its mandate. The terms of reference of the User Committee are available on the Euroclear website.

Client Survey

Regular day-to-day contact is maintained with clients by commercial, product management and operational teams. In addition to the day-to-day contacts with its clients, ES also monitors the evolutions in client demands and conducts an annual client survey to receive feedback on its performance and client perception of its business ("ES Client Survey"). All participants are encouraged to participate and complete the survey which covers topics such as ES approach to the market, product and service satisfaction, operational satisfaction and ease of doing business with ES. Results from the survey are generally discussed with clients throughout the year. The purpose is to capture specific needs by the market or participants. The ES Client Survey is used as a feedback and benchmark tool in terms of how well ES is performing and serving its market as an FMI. It not only allows ES to evaluate its performance against the Swedish market, but also against other Euroclear entities and CSD's. Currently the trend is positive and customer satisfaction is increasing.

All significant developments and changes to systems, services, rules, terms and conditions and tariffs are discussed with relevant participants and other stakeholders and where relevant subject to publicly available consultations.

Market Watch

ES also monitors market developments continuously and analyses performance of the Swedish market

in relation to the settlement ratio while also maintaining a very transparent policy with regard to the settlement efficiency. Detailed information can be found on our webpage, and, ES also sends out monthly data, presents statistics on member meetings and presents market trends to the FSA and the Riksbank at supervision meetings held on quarterly basis. Even though no official target for settlement efficiency is set, the market has every opportunity to react on changes in settlement and suggests targets or any potential mitigating action.

Key consideration 2: An FMI should have clearly defined goals and objectives that are measurable and achievable, such as in the areas of minimum service levels, risk- management expectations, and business priorities.

Corporate Objectives

The goals and corporate objectives for ES are decided and monitored by the Board of Directors. They are measured in the Balanced Scorecard ("BSC") and are follow-up on a regular basis by the ES CEO. The Balanced Scorecard is also used by the Board in its yearly evaluation of the company to assess the performance of the company against strategic priorities.

Key Performance Indicators

For each of Euroclear Sweden's corporate objectives there have been defined one or more measurable and specific Key Performance Indicators to support objective evaluation of the company's performance. The KPI's are monitored in the BSC.

Quantitative and Qualitative Assessment

The quantitative assessment, i.e. based on measurable KPI's, is supplemented by a qualitative assessment performed by the Board of Directors when it evaluates senior management's performance to ensure that all aspects of corporate performance, even when difficult to measure in a specific KPI, are considered.

Key consideration 3: An FMI should have established mechanisms for the regular review of its efficiency and effectiveness.

The efficiency and effectiveness are measured at different levels. The Balanced Scorecard is central in our measurement of efficiency and effectiveness at company. It includes measures around:

- Operational Performance (including e.g. uptime of our core systems, security measures, etc)
- Business Performance, Projects and Initiatives (including e.g. new products, regulatory compliance, etc)
- Financial Performance
- Client Satisfaction
- People Satisfaction and Organization

The departments of Euroclear Sweden use the corporate objectives to define their own internal objectives aligned to those in the Balanced Scorecard so that they contribute to the overall objectives. They will also set and monitor their own KPI's so that they are tailored to their specific functions and

have the most relevant measurement for efficiency and effectiveness. ES reached its goals and objectives for 2020.

Principle 22: Communication procedures and standards

An FMI should use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, settlement and recording.

Key consideration 1: An FMI should use, or at a minimum accommodate, internationally accepted communication procedures and standards.

ES uses internationally well accepted communication procedures while offering members several options in establishing communication for transfer of data between themselves and ES. Members have the choice of accessing ES via the private Network or SWIFTs own globally established IP based network (SWIFTnet). For back up purposes ES also have a VPN connection via Internet. Members can connect to the private Network via data transfer protocols (file, message and screen).

With the exception of file transfer, ES uses the same communications procedures for its cross-border operations as for the domestic ones.

ES applies ISO15022 communication as per SMPG⁴⁶ standards enabling use of the standard for clearing, settlement and transfer of securities while also available by use of a proprietary interface. For the purpose of transfer cross border i.e. CSD- links of securities ES participants are using ISO standardized messages.

In the area of corporate actions message standards, both proprietary and ISO15022 standards are available. While all messages are available on proprietary standards, ES has invested over the last two years to become more compliant towards SMPG standards and will continue improving compliance with ISO15022 standards⁴⁷. Development is a continuous process though impacted by market demand and market standards as gaps sometimes exist due to difference in market practice. Based on market needs and demands, these gaps are mitigated. Meanwhile the information is handled via proprietary messages.

ISO2022 compliant communication is offered where this has become the standard, for example for the SRDII shareholder identification communication.

ES also uses, where applicable, various standards related for definitions of securities (ISIN code, CFI code, Issuer LEI), participants (BIC code, LEI) and other reference data such as ISO standard for country codes, currencies etc.

⁴⁶ File Transfer Protocol

⁴⁷ ES has also established a dialogue with the market participants through the SWIFT Securities Committee forum regarding a migration from ISO15022 to ISO20022

Principle 23: Disclosure of rules, key procedures, and market data

An FMI should have clear and comprehensive rules and procedures and should provide sufficient information to enable participants to have an accurate understanding of the risks, fees, and other material costs they incur by participating in the FMI. All relevant rules and key procedures should be publicly disclosed.

Key consideration 1: An FMI should adopt clear and comprehensive rules and procedures that are fully disclosed to participants. Relevant rules and key procedures should also be publicly disclosed.

Rules and procedures

The main documents that comprise ES Rules are:

- The General Terms and Conditions - Account Operations and Clearing (ES Account Rules)
- ES Rules for Issuers and Issuing Agents (ES Issuer Rules)

The ES Account Rules govern the relationship between ES and the account operators, nominees, clearing members and settlement banks. The ES Issuer Rules govern the relationship between ES and the Issuer and the Issuer Agents.

Also included in ES Rules are product specifications, technical interface and user manuals, including appendices belonging to these documents. Special Resolutions are also issued in accordance with these frameworks.

ES Rules are based on national legislation, as well as EU legislation, and the main documents are communicated to clients upon affiliation and publicly available on the web page.

Disclosure

All suggested and performed amendments to ES Rules are communicated and relevant stakeholders are invited to consultations to discuss the suggested amendments. The consultation process gives the market participants an opportunity to provide their comments on e.g. how clear and understandable the changes are and that they are consistent with applicable laws. There is also a formalised process whereby participants can request changes to ES Account Rules.

Final changes to ES Rules are published on ES web page one month before they enter into force and clients will receive an email with a link to the web page where any changes in the rules are clearly marked. The latest changes that have been proposed in ES Rules, mainly driven by CSDR, are planned to enter into force on 1 March 2019, after consultation with the market as described above.

Changes to the interfaces affecting participants are communicated two months prior to the implementation. In conjunction with this the participants are invited to test in the external test environment.

ES is, where necessary and as a consequence of serious market disruptions, serious disruptions in communications, serious technical problems, or for other extraordinary reasons, entitled to take immediate measures as required in order to enable ES to maintain its operations in a secure manner. Upon the execution of such measures, ES shall, to the utmost extent possible, attempt to limit the damage incurred as a consequence of such disruptions. The above-mentioned provisions shall not be construed as limiting any liability which may be imposed on ES, account operators, nominees, clearing members or settlement banks⁴⁸.

ES shall notify all account operators, nominees, clearing members and settlement banks as soon as possible of such extraordinary measures and, where ES deems necessary, other persons affected by the measures. Account operators, nominees and clearing members shall, to the extent such measures or disruptions affect their customers, inform them as soon as possible and in an appropriate manner.

Key consideration 2: An FMI should disclose clear descriptions of the system's design and operations, as well as the FMI's and participants' rights and obligations, so that participants can assess the risks they would incur by participating in the FMI.

ES provides its clients information on their rights, obligations and risks incurred through participation in the FMI. These topics are covered by the ES Account Rules, by the application instruction and by the accession agreements. The ES Account Rules and the application instructions are available on ES web site and a copy of the generic accession agreements are attached to the ES Account Rules, as further described under Principle 1.

ES also provide product specifications, technical interfaces and user manuals to all clients and these are accessible to clients through ES website. The structure of the website is described under key consideration 4.

The website also includes a generic description of ES business contingency and crisis management process. Other contingency measures including fail over tests and internal set-ups like the on-duty manager and the crisis response teams are communicated at client meetings and in bilateral meetings with clients.

Key consideration 3: An FMI should provide all necessary and appropriate documentation and training to facilitate participant's understanding of the FMI's rules and procedures and the risks they face from participating in the FMI.

ES requires all participants to undergo mandatory training and participants have the availability to use the test environment of the VPC system for free. In order to facilitate the understanding and the communication, ES provides all participants with a dedicated operational client manager and provides services through a technical help desk.

ES annually performs supervisory meetings with all participants. Following these meetings ES would ask the participants for corrective measures including additional mandatory training if needed. ES also conducts participant meetings regularly where training issues could be addressed. The annual

⁴⁸ ES Account Rules, section A 11.1.

client survey provides feedback to ES in this area and the survey is an important tool on top of client meetings for ES to identify areas to improve.

Key consideration 4: An FMI should publicly disclose its fees at the level of individual services it offers as well as its policies on any available discounts. The FMI should provide clear descriptions of priced services for comparability purposes.

ES website is divided into one public section and one which requires you to log in. The log in section is called MyEuroclear.

In the public section, ES provide information about our service offerings, new products from across the Euroclear group as well as news and press releases. The section also includes insight and commentary on current industry trends.

In the MyEuroclear section more in-depth information about our service offering is published as well as access to tools, operational news, statistics, user guides, tariffs and rules etc.

Everyone can access MyEuroclear but this area is password protected so you first need to create a user profile to log in. In the MyEuroclear section, registered clients can access a wider range of information than non-clients.

ES presents the infrastructure set-up, including inter alia references to communication providers on the web page under the MyEuroclear section. Changes to the interfaces affecting participants are communicated 2 months prior to implementation. In conjunction with this the participants are invited to perform testing in the external test environment.

ES publishes its list of fees including high level service descriptions on the web under the MyEuroclear section together with fee calculations. On a general level such descriptions could be used as a comparison across similar FMIs. In accordance with ES Rules, clients are in general informed about changes to the list of fees one month prior to implementation⁴⁹. ES does not provide general discounts.

Key consideration 5: An FMI should complete regularly and disclose publicly responses to the CPSS-IOSCO disclosure framework for financial market infrastructures. An FMI also should, at a minimum, disclose basic data on transaction volumes and values.

In 2013 ES for the first time responded to the CPMI/IOSCO framework and assessment methodology dated December 2012. Previously ES has been assessed regularly by ECB/CESR principles. ES has after that published an updated Disclosure Framework in 2016 and 2018 in accordance with the CPMI/IOSCO framework.

The main source of public communication for ES is the web page where information related to ES is published in Swedish and English. ES provides a selective number of statistics covering clearing and settlement and shareholder information on a monthly basis on the web page. The web page is also continuously up-dated with various news covering current affairs and updates from the ES and the various entities in the group

⁴⁹ ES Account Rules A 3.5, A 4.7, A 5.5 and A 6.5, ES Issuer Rules A 2.8

V. LIST OF PUBLICLY AVAILABLE RESOURCES

This section lists publicly available resources, including those referenced in the disclosure, which may help a reader to understand the FMI and its approach to observing each applicable principle.

ES does not refer to any sources in this section instead footnotes are used in the text.