

Principles for financial
market infrastructures:

Disclosure framework

**Committee on Payments and
Market Infrastructures (CPMI)**

Status as of 31 December 2025
Clearstream Europe AG

Document number: 7512

September 2026

Information in this document is subject to change without prior notice.

This document is available in electronic format and may be provided in other formats at the discretion of Clearstream Europe AG (referred to hereinafter as CEU). CEU grants its participants permission to reproduce, store and print this document to the extent deemed reasonable and necessary for receiving from CEU the services described herein. Any software provided, as set out in the present document, shall be provided under the applicable licence terms.

Unless otherwise stated, all times are given in Central European Time (CET).

© Clearstream Europe AG (2026). All rights reserved.

Contents

Preface	5
Principle 1: Legal basis	19
Principle 2: Governance	26
Principle 3: Framework for the comprehensive management of risks	43
Principle 4: Credit risk	52
Principle 5: Collateral	58
Principle 6: Margin	62
Principle 7: Liquidity risk	63
Principle 8: Settlement finality	71
Principle 9: Money settlements	76
Principle 10: Physical deliveries	80
Principle 11: Central securities depositories	82
Principle 12: Exchange-of-value settlement systems	92
Principle 13: Participant-default rules and procedures	94
Principle 14: Segregation and portability	96
Principle 15: General business risk	97
Principle 16: Custody and investment risks	102
Principle 17: Operational risk	109
Principle 18: Access and participation requirements	123
Principle 19: Tiered participation arrangements	127
Principle 20: FMI links	132
Principle 21: Efficiency and effectiveness	138
Principle 22: Communication procedures and standards	142
Principle 23: Disclosure of rules, key procedures, and market data	144
Principle 24: Disclosure of market data by trade repositories	148

Responding institution: [Clearstream Europe AG](#)
Jurisdiction(s) in which the FMI operates: [Germany](#)
Authority(ies) regulating, supervising or overseeing the FMI:
[Bundesanstalt für Finanzdienstleistungsaufsicht \(BaFin\) and Deutsche Bundesbank](#)

Date of this disclosure: 24 September 2026
This disclosure can also be found at www.clearstream.com
For further information, please contact: css-clientduediligence@clearstream.com

Preface

Executive summary

Clearstream Europe AG (CEU) is a central securities depository (CSD) within the meaning of Article 2 (1) number 1 of 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 (hereinafter “Central Securities Depositories Regulation” or “CSDR”), and a leading pan-European post-trade services provider with approximately 300 participants as at December 31, 2025. CEU offers settlement, asset services, as well as various cash management services. The company contributes to the safety and efficiency of financial markets and provides its participants and providers with an exhaustive suite of connectivity.

CEU is linked to financial markets worldwide as follows:

1. **Direct T2S/investor-CSD link:** CEU establishes a TARGET2-Securities (T2S) link to another CSD directly connected to T2S (T2S In-CSD); settlement is processed in T2S. CEU usually appoints a local bank as an asset servicing provider.
2. **Direct link:** CEU establishes a link to another market where it holds an account at the local CSD; settlement is processed directly between CEU and the local issuer CSD.

Additionally, CEU offers settlement and custody in around 60 domestic markets via Clearstream Banking S.A. (CBL). CBL’s access to the domestic markets is either direct or via a foreign custodian whereby the securities are held in the local CSD in a CBL-dedicated client account. Cash settlement takes place via foreign correspondent banks.

As part of the Clearstream group (hereinafter “Clearstream”, see the [General organisation of the FMI](#) and [Summary of the major changes since the last update of disclosure](#) sections for details), CEU discloses information about its governance structure via the [Corporate Governance](#) section of its website:

- The company’s [operational structure](#)
- The company’s [shareholding structure](#)
- The names and titles of the members of its [Supervisory Board](#)
- The names and titles of the members of its [Executive Board](#)
- The roles and functioning of [Clearstream group committees](#)

Clearstream has a multifarious array of stakeholders:

- Stakeholders to whom Clearstream provides a service, that is, issuers, issuer agents and participants
- Stakeholders who provide a service to Clearstream, that is, CSDs, ICSDs, Transfer Agents and Order Handling Agents

- Stakeholders involved in the formation of the legislative and regulatory framework in which Clearstream operates, that is, Clearstream's regulator, market associations
- Stakeholders with a direct influence on Clearstream's equity, that is, parent company and end investors

As a CSD, CEU is authorised by Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin, German Federal Financial Supervisory Authority) pursuant to Article 16 (core and non-banking type ancillary services) and Art. 54 (banking-type ancillary services) of Regulation (EU) No 909/2014 (CSDR). Please refer to the [ESMA CSD register](#) for details.

Furthermore, CEU is an authorised and regulated credit institution according to the Kreditwesengesetz (KWG, German Banking Act). Accordingly, it is subject to the supervision of BaFin, which operates in close cooperation with Deutsche Bundesbank (German central bank).

In addition, CEU is designated as an operator of securities settlement systems (SSSs) by Deutsche Bundesbank in accordance with section 24b (1) of the KWG, transposing Article 10 (1) of Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems (SFD), amended by Directive 2009/44/EC of the European Parliament and of the Council of 6 May 2009 and by Directive 2010/78/EU of the European Parliament and of the Council of 24 November 2010.

Risk management is an elementary component of CEU's management and control. Effective and efficient risk management is fundamental to safeguarding the company's interests (both in terms of corporate goals and continued existence). The risk management policy documents CEU's risk management concept by describing the risk management framework in terms of processes, roles and responsibilities applicable to all staff and organisations within all legal Clearstream entities. The company has developed its own corporate risk structure and distinguishes between five aggregated risk types: operational, financial, business, pension, as well as winding-down and restructuring risk.

CEU has default management process (DMP) rules and procedures in place, which define the circumstances under which a participant is considered to be in default. Referring to the products and services offered, CEU defines two types of default, legal and contractual default. In order to take pre-emptive measures even before a default occurs, CEU has also established the Early Warning Framework as an integral part of its DMP.

CEU's Business Continuity Management System (BCMS) Policy defines the legal entity specific principles and requirements for Business Continuity. It defines the overall management system for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving the ability to continue providing services during a disruption, as applicable within the context of the organisation. The objective of the BCMS is to mitigate availability risks and to maintain management control to ensure customer and market confidence, to fulfil contractual obligations and to safeguard revenues and shareholder value.

When CEU decides to enter a new market, it will request proposals (request for proposals, RfPs) from leading banks in this market, who meet CEU's stringent requirements for a depository/ agent bank, as well as a cash correspondent bank (CCB), along with criteria such as appropriate licensing for banking and custody services, credit rating, industry rank, management competence, liquidity etc. This RfP process ties together a detailed operational due diligence of each individual business process with legal and compliance review of the entire infrastructure as well as credit reviews of the various intermediaries.

Summary of the major changes since the last update of disclosure

There have been the following main changes to CEU's organisation, services, design, rules, markets served and regulatory environment since the last disclosure as of December 31, 2023:

Legal and regulatory topics

- **Renaming of Clearstream Banking AG to Clearstream Europe AG:** Effective September 26, 2025, Clearstream Banking AG (CBF) was renamed to Clearstream Europe AG (CEU). The renaming reflects the entity's significant pan-European footprint and its strategic commitment to an integrated European capital market. The naming change is a legal entity naming update only: BIC and LEI remain unchanged, and all existing contractual agreements, service level agreements, and powers of attorney remain legally valid without requiring repapering. The account naming convention has been updated from Clearstream Banking AG/Clearstream Banking Frankfurt (CBF) to Clearstream Europe AG/ Clearstream Europe (CEU) accordingly.
- **Digital Operational Resilience Act (DORA):** The Digital Operational Resilience Act entered into application on January 17, 2025, following its entry into force on January 16, 2023. As a central securities depository (CSD) and authorised credit institution under the Kreditwesengesetz (KWG, German Banking Act), CEU falls within the scope of DORA as a financial entity pursuant to Article 2 (1) (a), (g) of the Regulation. DORA establishes a comprehensive and harmonised framework for information and communication technology (ICT) risk management across the EU financial services sector. In Germany, Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin, German federal financial supervisory authority) is the designated competent authority responsible for ICT incident reporting under DORA and coordinates with Deutsche Bundesbank (German central bank), Bundesamt für Sicherheit in der Informationstechnik (BSI, German federal office for information security), and the European Central Bank. CEU has implemented the necessary frameworks and procedures designed to comply with DORA requirements.
- **CSDR Refit:** This review of the CSDR by the European Commission made selected amendments to the initial regulation in five main areas: settlement discipline regime, passporting regime, banking-type ancillary services, third-country CSD oversight, and supervisory cooperation. The Refit entered into force on 16 January 2024 and is currently under work with ESMA, ESCB and EBA who are developing the CSDR's Regulatory Technical Standards (RTS). On 26 June 2025, ESMA published their final Technical Advice on the scope of the Settlement Discipline. ESMA specifies the cases in which settlement fails are not caused by participants, and operations that should not be considered as trading. The report also contains implementation periods regarding the exemptions, and alignments with cash penalties and mandatory buy-in regimes. Under the Market Integration and Supervision Package (MISP), published on 4 December 2025 (please see paragraph below), the EC has reopened the initial CSDR.
- **Savings and Investments Union (SIU):** Since 2023, the European Commission's initiative to make European capital markets more competitive evolved from the Capital Markets Union (CMU) to a Savings and Investments Union (SIU). In 2024, the debate was significantly shaped by three reports – the Letta, Noyer and Draghi reports – which called for deeper market integration, harmonised supervision, and increased competitiveness. The most current and impactful development is the Market Integration and Supervision Package (MISP). It represents a critical step in translating high-level ambitions into concrete regulatory action. Clearstream is fully committed to the objectives of the SIU and welcomes the Commission's MISP proposal. We are actively engaged in this regulatory process, championing reforms that foster a genuinely integrated, efficient and innovative post-trade ecosystem.

Organisational matters

In Q2/2024, Deutsche Börse Group introduced a Group-wide Written Rules Framework. CEU, as part of Deutsche Börse Group, is subject to this framework. The framework establishes a lean, consistent, and comprehensive structure for written rules within the Group, reducing the number of internal document types from fifteen to three (policy, guideline, procedure) and fostering transparency and easier maintenance. “Written rules” means a written, binding specification of requirements and definitions that must be implemented and adhered to by employees (or board members where applicable) within a defined scope of applicability. These rules are published centrally, reviewed, updated and approved at regular intervals to ensure they are up to date.

CEU's Information Security Framework has been updated in 2025 to reflect this Group-wide alignment.

Products and services

- **Enhancement of the D7[®] platform:** Following the official launch of the digital financial market infrastructure called D7 in 2021, Clearstream has expanded the platform with additional components, including the launch of D7 Generation 2 in June 2024. The enhanced architecture, developed in conjunction with Google, brings improvements designed to make the issuance process faster, easier, and more efficient, enabling up to 45,000 issuances per day performed within eight seconds. In November 2025, Clearstream launched D7 DLT, which has been developed for the issuance of live, CSDR-compliant securities based on distributed-ledger technology (DLT). The launch follows first successful live use cases during 2024 ECB Trials.

Clearstream will continue to expand the D7 offering, including stablecoin-ready settlement, wholesale CBDC readiness via the ECB's project Pontes, and the interoperability between traditional infrastructure and D7 DLT.

- **Collateral management:** With the transfer of central bank pledges as part of the ECMS project in June 2025, Clearstream continued the transition of its collateral management activities for the German domestic business previously conducted on CEU's Xemac[®] platform onto CBL's CmaX platform that supports its international triparty collateral management business. This transition was completed with the last service transition and subsequent Xemac decommissioning in summer 2026. Since 2023, the CmaX platform has centralised all triparty collateral management services for cleared and uncleared repo business with settlement on T2S and Creation. In doing so, Clearstream aims to provide standardised operational procedures and interoperability across the services offered by its Luxembourg-based ICSD and its CSD in Germany. For participants, the aim is to offer efficient mobilisation, optimisation and allocation of collateral across their international and domestic activities from a single pool of securities accounts.
- **Streamlining channels for communication with T2S:** Effective June 8, 2024, CASCADE-PC, CEU's graphical user interface for settlement instructions, was decommissioned. Participants had been migrated to alternative solutions such as CASCADE-Host, Xact Web Portal and ISO 15022 messages to benefit from short processing times and real-time access to information.
- **“Unified for New Opportunities” project:** The regulatory changes introduced by the CSDR Refit allow CEU to reshape its business to core CSD services, centralise banking services to its sister company CBL (ICSD) and enhance T2S settlement with increased volumes. The new organisational setup will reduce operational complexity. CEU participants will benefit from efficient and reliable services, with settlement conducted in CEU, using central bank money to the highest extent possible, thereby reducing risks. Additionally, the full interoperability between CEU and CBL enables efficient collateral usage and choice of settlement across both platforms.

- **Transition to T+1 settlement:** The European Union, along with the UK and Switzerland, is set to shorten the securities settlement cycle from two business days (T+2) to one (T+1) on October 11, 2027. The EU T+1 Industry Committee has published a High-Level Roadmap (HLRM) with recommendations for participants to implement to ensure readiness for T+1. Clearstream's core systems across all group entities are settlement-cycle agnostic and already largely compliant with the EU T+1 Industry Committee's HLRM. Required adaptations are minimal and will be delivered well in advance of migration: CEU and LuxCSD will implement the relevant T2S change requests in the June 2027 release, while CBL and Bridge optimisations will go live by August 2027. This timeline ensures market participants have ample opportunity to test all enhancements within the industry community testing windows prior to go-live.

Market coverage

With CEU having migrated to TARGET2-Securities (T2S), it acts as single gateway for settlement in T2S. The OneClearstream service level – Clearstream's Investor CSD model – provides participants with a single point of access to all T2S markets with comprehensive instrument coverage.

In March 2024, the OneClearstream service level was activated for the Slovak Republic. In November 2024, it was activated for Slovenia and Ireland.

General background on the FMI

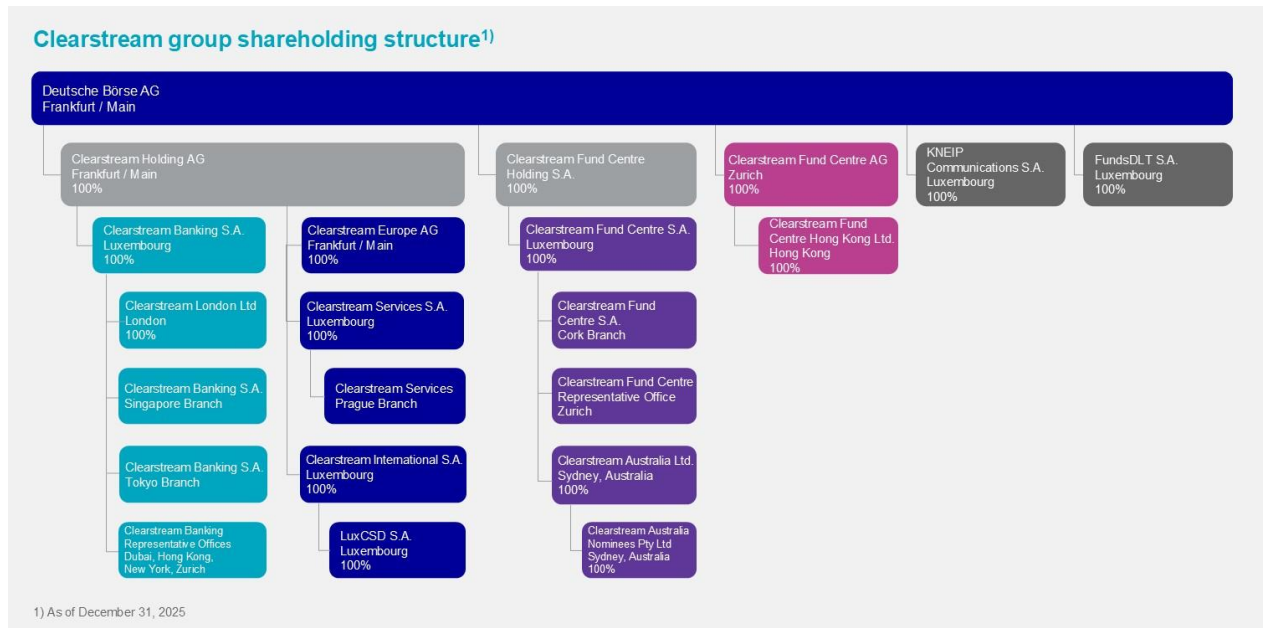
General description of the FMI and the markets it serves

Clearstream provides access to the network of all T2S CSDs which have been fully assessed for monetary policy operations. Additionally, Clearstream participants will have access to all CSD and ICSD counterparties from both CSD and ICSD accounts and benefit from realignment of any Clearstream accounts independent of any system outside Clearstream, including T2S, in real-time and at any time. Participants choose whether the transactions are to be effected in central bank money (via the CSD in Germany) or via commercial bank money, which is offered via the ICSD in Luxembourg.

Clearstream offers access to a large number of securities markets across the globe, providing direct and secure access to domestic liquidity pools and the international market. As the demand for access to new markets and instruments develops, the company will continue to expand its global network and to deliver market access solutions that meet the participants' needs.

General organisation of the FMI

Shareholding structure of the Clearstream group



Clearstream Holding AG acts as a holding company for companies of the Clearstream group¹ (hereinafter “Clearstream”). The German CSD Clearstream Europe AG (CEU) and the ICSD Clearstream Banking S.A. (CBL) are highly integrated into the structure of Clearstream within Deutsche Börse Group.

Governance structure of CEU

CEU is governed by a two-tier board structure. This approach features a clear separation between the powers of the Supervisory Board, which monitors and advises the Executive Board, and the Executive Board itself, which carries out day-to-day business. As of December 31, 2025, the company’s Supervisory and Executive Boards consisted of the following:²

Supervisory Board

Stephanie Eckermann (Chairperson), Dominik Schmidt-Kiefer (Vice-Chairperson), Christina Bannier, Peter Eck, Peter Gomer, Norfried Stumpf

Executive Board

Dirk Loscher (Chief Executive Officer), Martina Gruber, Udo Henkelmann, Volker Riebesell

¹ Except for LuxCSD which is held indirectly via Clearstream International S.A.

² The current composition of both bodies can be found on the [Clearstream website](#).

List of publicly available sources

The following documents are available on [Clearstream's general website](#):

[General Terms and Conditions](#)

[Becoming a Clearstream client](#), including the Client and Access Acceptance Policy

[Client Handbook](#)

[Fee Schedule](#)

[Cash Timings Matrix](#)

[Default Management Process](#)

[Market coverage](#)

[BaFin Three-Point Declaration](#)

[Association of Global Custodians disclosure](#)

[CSDR Article 38 disclosure](#)

[Pillar III Disclosure Report](#)

[Annual accounts](#)

[Corporate governance information](#)

[Remuneration information](#)

[Gender Diversity Policy](#)

List of abbreviations

This list is intended for information purposes only and is designed to help readers to understand the terminology used by CEU in this document. In some cases, the way in which the terms are used in CEU may differ from how the terms may be applied in another context. The descriptions given are not to be considered as legally binding definitions of the terminology used. CEU gratefully acknowledges that some definitions given here are based on those used by the Group of Thirty, the International Society of Securities Administrators (ISSA), the European Central Bank (ECB) and in other market publications.

Abbreviation	Explanation
AMA	Advanced measurement approach; one of four options under the Basel II framework that banks can use to calculate regulatory capital for operational risk. The AMA is based on internal models using internal risk variables and profiles, and not on exposure proxies such as gross income. Only risk-sensitive approach for operational risk allowed and described in Basel II.
AMI-SeCo	Advisory Group on Market Infrastructures for Securities and Collateral; group that counsels the Eurosystem on issues related to the clearing and settlement of securities and to collateral management. The advisory group is composed of market participants (banks active in the EU, CCPs, CSDs and national central banks) and chaired by the ECB .
AFME	Association for Financial Markets in Europe
AML	Anti-money laundering
ARM	Asset Reevaluation Manager; function within Clearstream's SSS to perform collateral reevaluation in predefined cases (market price fluctuation, redemption, security reference data change).
AZs	Availability zones; distinct, physically isolated locations within a cloud provider's region. Each zone has independent power, cooling and network infrastructure, ensuring that a localised failure does not disrupt services in other zones.
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (German Federal Financial Supervisory Authority); located in Bonn and Frankfurt/Main, BaFin supervises banks and financial services providers, insurers and securities trading.
BAIT	Bankaufsichtliche Anforderungen an die IT: Banking prudential requirements for IT; BaFin circular, which, on the basis of the KWG , provides a framework for the technical and organisational equipment of credit and financial services institutions in Germany and, in particular, for the management of IT resources and IT risks.
BCM	Business continuity management; all of the organisational, technical and staffing measures employed in order to ensure continuation of core business activities in the immediate aftermath of a crisis; and gradually ensure the continued operation of all business activities in the event of sustained and severe disruption.
BIA	Business impact assessment

Abbreviation	Explanation
BRA	Business requirements analysis
BRRD	Bank Recovery and Resolution Recovery Directive; Directive 2014/59/EU of the European Parliament and of the Council establishing a harmonised framework for the recovery and resolution of credit institutions and investment firms; amended by Directive 2019/879 (BRRD II).
CAAP	Client and Access Acceptance Policy; set up by Clearstream in accordance with the requirements of the CSDR and DR (EU) 2017/392 to support the management of access to the company's SSS . The policy explains the approach adopted by CBL , CEU and LuxCSD to comply with the aforementioned requirements and provides guidance for the analysis and subsequent actions to be taken in order to identify, measure, monitor, manage and enable reporting on the risks incurred by CEU, CBL and LuxCSD and/or their clients and other participants.
CBL	Clearstream Banking S.A., Luxembourg
CCB	Cash correspondent bank; a bank appointed by CEU as its agent to handle external receipt and payment of funds in a specified currency.
CCMT	Clearstream Crisis Management Team; a team at the Clearstream group, comprised of senior managers and subject matter experts with the objective to ensure that a crisis is addressed in an efficient and timely manner to the Executive Board and all relevant stakeholders of the Clearstream group.
CCO	Chief Compliance Officer
CCP	Central counterparty; an entity that interposes itself, in one or more markets, between the counterparties to the contracts traded, becoming the buyer to every seller and the seller to every buyer and thereby guaranteeing the performance of open contracts.
CDM	Clearstream Default Management; unit within the Clearstream group that maintains and continuously improves the default management process in order to prepare for a crisis situation in the most efficient manner.
CeBM	Central bank money; liabilities of a central bank, in the form of either banknotes or bank deposits held at a central bank, which can be used for settlement purposes.
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team; central unit at Deutsche Börse Group for all cyber situational analysis (pro-active, detective and forensic). This includes information security (IS) incident management, IS monitoring, threat and vulnerability management and internet watch to identify new vulnerabilities.
CEU	Clearstream Europe AG, Frankfurt
CISO	Chief Information Security Officer

Abbreviation	Explanation
CoBM	Commercial bank money; commercial bank liabilities that take the form of deposits held at a commercial bank which can be used for settlement purposes.
CRC	Clearstream Risk Committee; internal committee at the Clearstream group that steers risk, compliance and cyber security matters in order to foster an effective first line of defence across all Clearstream legal entities. The CRC plays an important role in identifying, mitigating and monitoring the company's risk exposures.
CRD	Capital Requirements Directive; Directive (EU) 2024/1619 of the European Parliament and of the Council amending Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms as regards supervisory powers, sanctions, third-country branches, and environmental, social and governance risks (CRD VI). The CRR III/CRD VI package ("banking package") implements in the EU the outstanding elements of the Basel III regulatory reforms (i.e. output floor, credit risk, market risk, operational risk). It also introduces changes in other non-Basel key areas such as fit and proper, third-country branches and environmental, social and governance (ESG) risks.
CRR	Capital Requirements Regulation; Regulation (EU) 2024/1623 of the European Parliament and of the Council amending Regulation (EU) 575/2013 on prudential requirements for credit institutions and investment firms. The CRR III/ CRD VI package ("banking package") implements in the EU the outstanding elements of the Basel III regulatory reforms (i.e. output floor, credit risk, market risk, operational risk). It also introduces changes in other non-Basel key areas such as fit and proper, third-country branches and environmental, social and governance (ESG) risks.
CSD	Central securities depository; an entity that enables securities transactions to be processed and settled by book entry, provides custody services (for instance, the administration of corporate actions and redemptions), and plays an active role in ensuring the integrity of securities issues. Securities can be held in a physical (but immobilised) form or in a dematerialised form (that is, as electronic records).
CSDR	Central Securities Depository Regulation; Regulation (EU) 2023/2845 ("CSDR Refit") amending Regulation (EU) No 909/2014 of the European Parliament and of the Council on improving securities settlement in the European Union and on central securities depositories as regards settlement discipline, cross-border provision of services, supervisory cooperation, provision of banking-type ancillary services and requirements for third-country central securities depositories and amending Regulation (EU) No 236/2012.
DCA	Dedicated cash account
DCP	Direct connected participant
DDV	Due diligence visit
DepotG	Depotgesetz, German Securities Deposit Act

Abbreviation	Explanation
DR 2017/392	Commission Delegated Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories
DvP	Delivery versus payment; the irrevocable exchange of securities (the delivery) and cash value (the payment) to settle a transaction. True DvP involves the simultaneous exchange of securities and cash, as in the case of transactions between CEU counterparties.
EaR	Earnings at risk
EB	Executive Board
EBA	European Banking Authority; based in Paris, has the aim of creating a common legal framework for the national banking supervisory authorities in the EU. Like ESMA and the European Insurance and Occupational Pensions Authority (EIOPA), EBA is part of the European System of Financial Supervision (ESFS).
EBITDA	Earnings before interest, tax, depreciation and amortisation
ECB	European Central Bank
ECSDA	European Central Securities Depositories Association
EPTF	European Post Trade Forum
ESMA	European Securities and Markets Authority; based in Paris, ESMA aims to create a uniform legal framework for the national supervisory authorities in the EU. It is one of the European Supervisory Authorities established on 1 January 2011, alongside EBA and the European Insurance and Occupational Pensions Authority (EIOPA).
EWI	Early warning indicator; parameter monitored within Clearstream to identify triggers or events, which could potentially change the credit standing of a participant and as such jeopardise the fulfilment of contractual obligations to Clearstream (i.e. scheduled repayment obligations) or even lead to default of a participant.
EWS	Early warning signal; result of EWI monitoring against defined thresholds. A breach of an EWI threshold triggers an EWS, which anticipates the vulnerability of a participant to financial distress.
FMI	Financial market infrastructure; a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling or recording payments, securities, derivatives or other financial transactions. Examples: central counterparty (CCP), central securities depository (CSD), clearing house, payment system, securities settlement system (SSS), trade repository (TR).
FX	Foreign exchange
GRM	Group Risk Management; central function at Deutsche Börse Group.

Abbreviation	Explanation
GTCs	General Terms and Conditions
HQLA	High-quality liquid asset
HR	Human Resources
ICAAP	Internal capital adequacy assessment process
ICMA	International Capital Market Association; created in July 2005 by the merger of the International Securities Market Association (ISMA) and the International Primary Market Association (IPMA). ICMA is an organisation with a broad franchise across the primary and secondary international capital market. This association has the mandate and the means to represent the interests of the investment banking industry in maintaining and developing an efficient and cost-effective international market for capital.
ICMSA	International Capital Market Services Association
ICP	Indirect connected participant
ICS	Individual client segregation
ICSD	International securities depository
ILAAP	Internal liquidity adequacy assessment process
IRM	Information risk management
ISLA	International Securities Lending Association
ISMA	See ICMA
IS	Information security
ISO	International Organisation for Standardisation; international federation of standardisation bodies for various industries that seeks to set common international standards in a variety of fields.
ISSA	International Securities Services Association
KPI	Key performance indicator
KRI	Key risk indicator
KWG	Kreditwesengesetz, German Banking Act
KYC	Know your customer
LCR	Liquidity coverage ratio
MaRisk	Mindestanforderungen an das Risikomanagement; administrative instructions from BaFin for the structuring of risk management in German credit institutions.
MCP	Material change process; represents a methodology implemented at Deutsche Börse Group to ensure analysis of risks associated with

Abbreviation**Explanation**

material changes, risk mitigating measures being derived in terms of systems and processes. A robust control framework needs to be carried out and documented accordingly before business is commenced in new products, product variants, product combinations, new distribution channels or go to market activities or before specific changes to the business model and setup become effective.

MCWG	Material Change Working Group
MIS	Management information system
MMR	Market member readiness
MREL	Minimum requirement for own funds and eligible liabilities
MT	Message type; refers to Swift message types that can be used by participants to send instructions and messages, and to receive reports. For example, "MT54x" refers to Message Types 540, 541, 542 and 543.
NAV	Net asset value
NM	Network Management; business area of the Clearstream group that is responsible for developing and maintaining relationships and services with CEU's network of suppliers, such as agents, CSDs, central banks or market infrastructures.
NRA	National Resolution Authority
OCS	Omnibus client segregation
PFMI	Principles for Financial Market Infrastructures
QLR	Qualifying liquidity resource
RfI	Request for information
RfP	Request for proposal
RoPs	Rules of procedure
RTGS	Real-time gross settlement; processing and settlement on a transaction-by-transaction basis in real time.
RT0	Recovery time objective
RTS	Regulatory technical standard
SB	Supervisory Board
SCV	Security collateral value
SFD	Settlement Finality Directive; Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems.
SLA	Service level agreement

Abbreviation	Explanation
SRD II	Shareholder Rights Directive II; Directive (EU) 2017/828 of the European Parliament and of the Council of 17 May 2017 amending Directive 2007/36/EC as regards the encouragement of long-term shareholder engagement.
SSS	Securities settlement system; a system which allows the transfer of securities, either free of payment (FoP) or against payment (DvP).
STP	Straight-through processing; the swift, safe and efficient processing of a securities transaction, from order placement to delivery versus payment (DvP) and to the subsequent safe custody of the securities.
Swift	Society for Worldwide Inter-Financial Telecommunications
T2	Third-generation TARGET system that settles payments in euro in CeBM; based on a single IT platform, to which all payment orders are submitted for processing; legally structured as a multiplicity of RTGS systems (TARGET = Trans-European Automated Real-time Gross Settlement Express Transfer System).
T2S	TARGET2-Securities; the Eurosystem's single technical platform enabling CSDs and national central banks to provide core, borderless and neutral securities settlement services in CeBM in Europe.
U2A	User to application
UCoD	Unauthorised creation and or deletion of securities
VaR	Value at Risk; quantifies the risks to which a company is exposed. It indicates the maximum cumulative loss that CEU could face if certain independent loss events materialise over a specific time horizon for a given probability. CEU's models are based, in line with the Basel framework, on a one-year time horizon.
VPN	Virtual private network

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 of CEU's activities and relevant regulatory framework

CEU is a central securities depository ("CSD") with registered seat in Frankfurt/Main, Germany.

CEU is authorised in accordance with Article 16 and 54 of 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, as amended (together with all related annexes, hereinafter referred to as "**CSDR**").

CEU is:

- supervised by Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin, German Federal Financial Supervisory Authority) in its capacity as designated competent authority in accordance with Article 11 of CSDR and section 6 (1c) Kreditwesengesetz (KWG, German Banking Act); and
- as operator of a securities settlement system ("**SSS**"), also subject to the oversight supervision of Deutsche Bundesbank (German central bank) in accordance with the article 127 (2) and (5) of the Treaty of the Functioning of the European Union and section 7 KWG.

The different regulatory statuses of CEU can also be found in the following databases maintained by:

- a. ESMA:
 - (i) for the [CSD register](#), including the list of the authorised services (hereinafter referred to as the "**CSD Register**")
 - (ii) for the [list of the designated payment and SSSs](#)
- b. European Central Bank for the [list of the eligible SSSs for use in Eurosystem's credit operations](#)
- c. BaFin for the [list of authorised banks, financial services providers, insurance undertakings & pension funds, asset management companies](#) (hereinafter referred to as the "**Database of companies**").

The scope of the activities of CEU is limited by the scope of its authorisation. These services are listed in the CSD Register and are categorised as follows:

- Core CSD services of Section A of the CSDR Annex, such as the settlement of transactions in domestic and foreign securities, notary services (initial recording of securities in a book-entry system), as well as central maintenance services (providing and maintaining securities accounts at the top-tier level); and

- Non-banking-type ancillary services of Section B of the CSDR Annex (explicitly and not explicitly listed in Section B of the CSDR Annex) supporting the core activities of CEU, such as, among others, CSD link and asset servicing; and
- Banking-type ancillary services of Section C of the CSDR Annex, such as, among others, providing cash accounts to participants and accepting deposits from them, providing cash credit to holders of securities accounts and payment services involving the processing of cash and foreign exchange transactions.

Accordingly, the material aspects of CEU's activities are:

- (i) Initial recording of the financial instruments confided to and held with CEU
- (ii) Registration of eligible financial instruments immobilised or in dematerialised form for book-entry transfer
- (iii) Recording and servicing rights and interests in financial instruments under deposit and sub-deposit
- (iv) Operating an SSS ensuring the finality of the settlement
- (v) Integrity of the issues

To provide services described above in line with CSDR, CEU is further authorised and regulated as a credit institution according to the provisions of the Kreditwesengesetz (KWG, German Banking Act). Accordingly, CEU is subject to banking supervision, which is carried out by BaFin in close cooperation with Deutsche Bundesbank (German central bank). The latter also has an oversight responsibility for CEU as operator of a securities settlement system ("SSS"). In addition, CEU acts as a central registrar in the meaning of the Gesetz über elektronische Wertpapiere (eWpG, German Electronic Securities Act).

Securities can be held in custody with CEU under the following main structures:

- Girosammelverwahrung (collective safe custody, CSC)
- Lagerstellenverwahrung (vaults services for third parties)
- Streifbandverwahrung (individual safe custody)
- Wertpapierrechnung (non-collective safe custody, NCSC)

For further details on these safekeeping structures, see [Principle 11](#).

Legal basis for the material aspects of CEU's activities

Germany is the principal jurisdiction of CEU's operations.

The corporate structure and governance of CEU as a public limited company, CEU's contractual terms of participation and services (including liability), the deposit and circulation of securities, and CEU's recovery, resolution, insolvency and winding-down proceedings are governed by German law.

The European Union's legal framework, as well as the national laws, regulations and circulars ("German law") applicable to the financial services sector constitute CEU's key legal basis relevant to the operations of CEU as CSD. These are in particular:

- CSDR and its delegated regulations, such as Commission Delegated Regulation EU 2017/390 on certain prudential requirements for CSDs and designated credit institutions offering banking-type ancillary services ("**RTS 2017/390**"), Commission Delegated Regulation EU 2017/392 on authorisation, supervisory and operational requirements for CSDs ("**RTS 2017/392**") and Commission Delegated Regulation EU 2018/1229 on settlement discipline, as amended ("**RTS SDR**");

- Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems (SFD), amended by Directive 2009/44/EC of the European Parliament and of the Council of 6 May 2009 and by Directive 2010/78/EU of the European Parliament and of the Council of 24 November 2010;
- Regulation (EU) No 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012, as amended (CRR);
- Aktiengesetz (AktG, German Stock Corporation Act) for general rules, including company law aspects as well as vindication, transfer of (co-)ownership, regular custody contracts, good faith acquisition, mandate and agency;
- Bundesschuldenwesengesetz (BschuWG, German Federal Government Debt Act) for the entry of a CSD into debt ledger equaling the existence of a pool of certificates (Wertpapiersammelbestand) and the respective acts of the federal states;
- Bürgerliches Gesetzbuch (BGB, German Civil Code);
- Depotgesetz (DepotG, German Securities Deposit Act) on the safe custody and acquisition of securities;
- Gesetz über elektronische Wertpapiere (eWpG, German Electronic Securities Act);
- Insolvenzordnung (InsoO, German Insolvency Code) in relation to the segregation of assets in the case of CEU's insolvency;
- Kreditwesengesetz (KWG, German Banking Act);
- Sanierungs- und Abwicklungsgesetz (SAG, German Banking Resolution Act) including the default and resolution procedures;
- Schuldverschreibungsgesetz (SchVG, German Bond Act) in relation to restructuring of bonds.

The rules for participation in CEU and applicable to the CSD services are set forth in the following main (governing) documents and published in the Key Documents section of the [Clearstream website](#):

1. [General Terms and Conditions \(GTCs\)](#)
2. [Special Conditions for reporting and payment obligations following from the French Financial Transaction Tax and services provided by Clearstream Europe AG](#)
3. [Special Conditions for the re-entry of internal instructions on 6-Series Accounts](#)
4. [Special Conditions of Investment Fund Services of Clearstream Europe AG](#)
5. [Fee Schedule](#)
6. [Market Link Guides](#)
7. [Disclosure Guides](#)

The GTCs and the Special Conditions are accompanied by technical rules (including but not limited to the [CEU Client Handbook](#)) which contain a description of services and procedures and various technical aspects.

Furthermore, CEU publishes on its website announcements in relation to participant information and specific services on a regular basis.

When becoming a participant of CEU, the relevant participant has to accept CEU's GTCs.

CEU will notify its participants via email and on its website of any changes in relation to the GTCs and the effective date thereof. Unless the participant informs CEU in writing of any objection within six weeks after the modification has been communicated to him, the participant will be deemed to have accepted such amendments.

For other CEU contracts and documentation entered into by the participant, amendments follow the procedures agreed by the participant and CEU therein.

In principle, these documents are governed and shall be interpreted by German Law and any disputes arising in relation to them shall be submitted to the competent courts of Germany (see, for instance, the GTCs).

CEU's contracts with its participants contain explicit choices of law and jurisdiction clauses designating mainly German law as applicable law and courts of Germany as competent forum for the disputes arising from and in relation to the services.

Where CEU conducts an activity in another jurisdiction or has to elect another governing law, such information is made available in the relevant section of its website, such as for the CSD links (within the meaning of CSDR, referred hereinafter as "**CSD Links**"). The relevant domestic laws and regulations governing the custody and the settlement are described in the [Market Coverage](#) section of CEU's website and include the Market Link Guide, Market Taxation Guide and Disclosure Requirements.

The CSD Links are generally governed by contractual arrangements subject to the law and rules of the receiving CSD (for the direct links) or the intermediary operating the direct links or involved in the indirect links (the "**Intermediary**") in accordance with Article 85 of RTS 2017/392 (referred hereto as "**Links Agreements**").

The Link Agreements set forth, among other things, the scope of the services, the entitlement and the nature of the rights in book-entry financial instruments deposited in CEU's accounts with such Intermediary or receiving CSD, the liability rules as well as the rules of protection of the assets deposited, the segregation rules, the termination and the choices of law and jurisdiction.

For the purpose of the assessment of the CSD Links and the Links Agreements, legal opinions are requested annually. The purpose of such reviews is to verify whether the conditions applicable in the receiving jurisdictions are equivalent to the conditions applicable in Germany, to achieve the same level of protection offered by CEU. These opinions should generally cover the following main legal topics:

- (i) the capacity and authority of the receiving CSD to enter into the Links Agreements;
- (ii) the validity and enforceability of the relevant Links Agreements;
- (iii) the nature of entitlement (i.e. confirming the recognition of the rights and interest of CEU in respect of the financial instruments sub-deposited on behalf of its participants) and the law applicable to proprietary aspects;
- (iv) liability standards;
- (v) rules on the enforceability of netting, if applicable; and
- (vii) confirmation that there is no upper tier attachment.

In addition, the legal opinions shall also address the other legal aspects listed in Article 84 (1), last paragraph of RTS 2017/392, such as confirmations of the absence of encumbrances, liens, pledges and set-off rights on the securities deposited abroad; the impact of insolvency proceedings opened against the receiving CSD/depository regarding the segregation requirements, settlement finality; as well as procedures and time limits to claim the securities in the relevant jurisdiction.

Finally, CEU entered into the T2S Framework Agreement with the Eurosystem for the participation in T2S and the outsourcing of its settlement of securities. This agreement governed by German law sets out the rights and obligations of the Eurosystem and each contracting CSD and covers the operation of T2S.

The terms of the T2S Framework Agreement have been subject to a legal assessment to determine any potential legal risks and gaps with respect to CEU's applicable legal framework. Accordingly, corresponding rules dedicated to the T2S settlement have been included in the relevant CEU's governing documents to ensure a level of certainty for the settlement activities.

Key consideration 2

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

CEU has set up clear and understandable rules, procedures and contracts in accordance with Article 43 of CSDR.

CEU's rules and contracts (see list in [key consideration 1](#)) are published electronically on the Clearstream website. In order to ensure that the CEU's participation documentation remains consistent with relevant laws and regulations, the company generally reviews it on a regular basis and on an ad hoc basis, in particular when:

- (i) An update of a key law or regulation applicable to the financial services industry is relevant for CEU and/or its participants;
- (ii) The implementation of remedial measures is needed due to a claim affecting a participant or caused by a provision of the governing documents;
- (iii) Typos or inconsistencies are detected in the governing documents and/or specific agreements;
- (iv) A change of laws or regulations in the local markets shall be reflected;
- (v) A court order or a decision from a regulator is taken in favour of the clarification of certain provisions of the governing documents;
- (vi) There is a global enhancement of CEU's technical system (such as change of deadlines);
- (vii) There are changes of the professional standards (for instance, at the level of the ECSDA, ICMA or ICMSA) to be reflected in the governing documents and/or the specific agreements;
- (viii) Major projects need to be implemented;
- (ix) Any other events occur that the control functions (Audit, Risk, Compliance) and/or the legal department consider as essential to be incorporated in the participant documentation.

The review is carried out by CEU's control functions teams and the legal department on a continuous basis. In addition, the company involves, whenever appropriate, independent external legal counsels to assist in the review and drafting of the documentation and/or updates.

CEU's core governing documents (such as the GTCs) and any amendments are reviewed, discussed and approved by the various competent internal committees and the competent management body of CEU. Once corporate approval is granted, such document is made available to the participants with the relevant information, notably the effective date. The approved amendments to the GTCs are notified via email to CEU's participants prior to their effective date and are published on the company's website. The revised versions of the other governing documents are directly published on this website.

Key consideration 3

An FMI should be able to articulate the legal basis for its activities to relevant authorities, participants, and, where relevant, participants' customers, in a clear and understandable way

CEU articulates the legal basis for material aspects of its activities by using well-reasoned legal opinions or analyses, carried out – where reasonably required – with the support of independent law firms of good reputation. Please see [key consideration 1](#).

The rights and interest resulting from the participation to CEU's system are addressed in the documentation supporting CEU's activities and the German legal and regulatory framework.

The contractual framework applicable to CEU's settlement services reflects (i) the finality rules applicable by CEU's system to the transfer orders, as prescribed by SFD, the German laws transposing SFD (in particular, InsoO, KWG and DepotG); and (ii) the CSDR, its delegated regulations and, in particular, RTS SDR (Settlement Discipline Regime).

CEU's rules and their enforceability are tested from time to time during self-assessment reviews with the regulators which can be accompanied by legal opinions issued by external lawyers for such specific purposes.

In addition, CEU maintains an inventory of the laws and regulations, as well as the main rules relevant for the material aspects of its activities and main business areas in the various markets to ensure proper articulation with the applicable legal framework. This inventory is set up and reviewed at least on an annual basis by the compliance function.

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.

CEU aims at a high degree of certainty for the validity and enforceability of its rules and procedures. As the company's operations are mainly located within the territory of Germany, its rules, procedures and contracts are governed by and are enforceable in accordance with German law. Please refer to the explanations provided under [key considerations 1](#) and [2](#).

CEU's GTCs as well as its contractual documentation have a severability clause (salvatorius clause) in order to maintain the legal substance of the relationship with the participants in accordance with German contractual law practice should an article be declared invalid, illegal or incapable of being enforced.

Regarding the settlement of participants' transactions, a high degree of certainty is achieved by the recognition of the finality of the settlement whereby transactions having reached the moment of irrevocability and finality cannot be revoked, respectively unilaterally (when the moment of irrevocability is reached) or by any third party (when the moment of finality is reached).

However, reversals and stays in the execution of certain actions could still result, other than the contractual right of CEU set forth in its governing documentation, from the default of a counterparty (for instance, in case of insolvency/liquidation); or (ii) court order; or (iii) resolution authorities' decisions under BRRD or equivalent laws; or (iv) laws, resolutions, market practices applicable in certain jurisdictions (in particular for those jurisdictions not recognising the finality of settlement).

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.

CEU conducts business across jurisdictions, in particular:

- when it grants access to its system to participants or issuers incorporated under and subject to the laws and regulations of another jurisdiction;
- for the custody and settlement of securities held via a CSD link.

For such purposes, CEU's documentation clearly outlines a choice of law for each aspect of its operations. The access to CEU's system is notably subject to CEU's governing documentation applicable to the securities accounts of CEU's participants and their deposited securities. The law chosen by CEU to govern this legal relationship and its services is German law (see also [key considerations 1](#) and [4](#)).

Accordingly, the nature of the entitlement over the deposited securities held with CEU shall be determined by German conflict-of-laws rules, as Germany is the "place of the relevant intermediary" (or "PRIMA") and the jurisdiction of the "system" notified by Deutsche Bundesbank to the European Securities and Markets Authority ("ESMA") as securities settlement system in accordance with SFD and the KWG.

Regarding the identification and the mitigation of the legal risks arising from a potential conflict of laws for the custody and settlement activities carried out abroad via the CSD Links, please refer to [key considerations 1](#). The Link Agreements are generally not governed by German law, but by the law applicable to the receiving CSD. They are reviewed internally and submitted to the assessment of an external/local law firm qualified in the relevant jurisdiction to provide comments and issue legal opinions covering, among other things, the validity of the choice of the law and jurisdiction and the identification of potential conflicts of laws.

With such assessment, CEU is aware of the applicable constraints on its abilities to choose the law that will govern its activities and when there is a difference in the substantive laws of the relevant jurisdictions. CEU also informs its participants by publishing the main legal features applicable in these jurisdictions, in particular for the CSD Links (in the Market Link Guides), in order to enable them to assess their own risks by using such services in accordance with Article 34 (5) of CSDR.

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.

CEU's objectives contributing to its own safety and efficiency

As part of Deutsche Börse Group, Clearstream Europe AG (CEU) aims to be a leading European supplier of post-trading services. Thus, pursuant to the Articles of Incorporation of CEU, the "Articles", the main objective of the company is the operation of:

- A securities clearing and deposit bank and the performing of all tasks relating to this, including data and information transfer between shareholders, institutions and issuers as well as the provision of appropriate systems;
- A central accountancy and clearing office in order to facilitate the international securities clearing system;
- A system for collateral provision and management (collateral management).

To achieve this objective, CEU aligns its strategy with that of Deutsche Börse Group. The focus of the three-year strategic and financial planning currently is on business growth, built on the following pillars:

1. Driving secular growth
2. Advancing key transformation themes
3. Strengthening the unified operating model
4. Applying disciplined capital-allocation principles to scale the business sustainably beyond the current planning cycle

CEU's business strategy is implemented across five vectors:

- Reinforcing European core and global connectivity
- Expanding and diversifying client access
- Future-proofing the post-trade value chain
- Embedding data and AI in the core
- Ensuring operating model scalability and regulatory excellence

In 2025, Clearstream Banking AG was rebranded to Clearstream Europe AG (CEU). CEU's Pan-European CSD solution provides a single entry point for settlement in central bank money, enabling clients to settle, safekeep, and manage securities across 19 T2S markets through a unified platform and a single account.

In parallel, the launch of Project UNO and the establishment of D7® as a fully digital post-trade infrastructure remain the main strategic priorities. The D7 platform is a core element of CEU's transition to a fully digital operating model.

In addition, CEU continues to invest in its core custody business: network expansion, asset servicing enhancements, harmonizing onboarding and API-based connectivity are set to increase safety and further strengthen the value proposition for participants.

Together, the above initiatives help CEU uphold high industry standards while advancing the digitalisation of the European capital markets.

CEU's business strategy outlined above is accompanied by a comprehensive risk strategy to ensure that objectives are met in a secure and efficient manner and by respecting an appropriate risk appetite, the latter being defined as risk limitation, which protects and ensures continuity of operations. See [Principle 3](#) for details. A high emphasis is placed on the elimination or minimisation of risk, as also described in detail in the Pillar III report, published and available to participants on the [Clearstream website](#).

Monitoring and control of the above objectives including the related risk management are performed primarily by CEU's Executive Board (EB). This EB is itself supervised by the company's Supervisory Board (SB). The SB Risk Committee advises the SB on CEU's overall risk strategy and the current and future risk appetite. Furthermore, it assists the SB in its mission to assess the correlation between the risks incurred, the company's ability to manage these risks and the internal and regulatory own funds and liquidity reserves. In addition, CEU's User Committees submit non-binding opinions to the EB and advise on key arrangements that may affect its members pursuant to the CSD Regulation (EU) 909/2014 (CSDR). Furthermore, the following tools are used to ensure the quality of CEU's own operations, respectively of the operations that are outsourced to other Deutsche Börse Group entities:

- (i) Forum for structured, systemic and creative solution identification, including post-claim analysis and identification of appropriate measures;
- (ii) Key performance indicators (KPIs): quantified, objective view on service delivery of operations, for example on effectiveness, efficiency, operational quality, and operational risk;
- (iii) Key risk indicators (KRIs): early warning system for operational risk, periodically collected and analysed to observe the trend and, if necessary, initiate mitigating measures;
- (iv) KPI engine: data warehouse, linked to major production systems, enabling standard and ad hoc reporting and detailed data analysis;
- (v) Report on the performance of the settlement system and committed service level targets.

Continuous documentation and reporting of the said indicators, tools and processes are key for CEU to monitor and – wherever necessary – adjust its business and risk strategies or individual objectives.

Please refer to [Principle 21](#) for more details on the mechanisms applied for the review of CEU's efficiency and effectiveness.

CEU's objectives supporting financial stability and the efficiency of financial markets

As a financial market infrastructure provider, Deutsche Börse Group considers its primary responsibility as ensuring transparent and stable capital markets. CEU, as an integral part of the Group, upholds this mandate by maintaining the highest standards of asset protection and applying a strong focus on risk management practices.

As a neutral FMI, CEU contributes to strengthen the safety, efficiency, and transparency of financial markets. Its infrastructure ensures that securities transactions are processed accurately and on time, even under conditions of extreme market stress. Thus, CEU supports overall market stability and participant confidence.

This guiding principle is reflected in CEU's comprehensive range of non-banking and banking-type ancillary services in line with CSDR. These services are designed to enhance the efficiency of securities settlement while ensuring full adherence to the applicable regulatory requirements.

CEU's business objective to expand partnerships with electronic trading platforms, CCPs, other CSDs and agent banks further contributes to market efficiency and stability from the perspective of its participants.

To safeguard financial stability and maintain orderly markets, CEU has established transparent, objective and non-discriminatory participation criteria, as set out in its [Client and Access Acceptance Policy](#). The Policy outlines the rules governing interactions between the CSD and its participants, ensuring clarity and consistency.

Finally, Clearstream contributes to the stability of the financial system as a whole by engaging in industry and regulatory discussions on post-trade topics. It participates in various organisations and working groups. Further details are provided in the section "[Stakeholders involved in the formation of the legislative and regulatory framework in which the Clearstream group operates](#)" of key consideration 7.

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

CEU's governance arrangements as well as the rules governing its activities are described in detail in a number of documents which are publicly accessible to all stakeholders on its [website](#).

These documents are annually reviewed and include:

- [Articles of Incorporation](#)
- [Rules of Procedure for the Executive Board](#)
- [Rules of Procedure for the Supervisory Board](#)
- [Terms of Reference of the User Committees](#)
- [Gender Diversity Policy](#)

To ensure proper conduct and compliance with regulatory and legal provisions throughout the entire company, CEU has adopted further governance arrangements, such as the following:

- Deutsche Börse Group's framework to manage conflicts of interest: aims at addressing all types of – actual or potential – conflicts of interest within the group, including (i) corporate conflicts of interests, (ii) personal conflicts of interests, as well as (iii) specific conflict situations, see [key consideration 3](#) for more details;
- Whistle-blower policy: provides guidance to employees for reporting non-compliant behaviour to an external ombudsman. The said policy specifies the types of behaviour and situations that can be reported and describes the protection and confidentiality framework offered to whistle-blowers.

With regard to governance arrangements that may have a direct impact on CEU's participants, the company's [Client Handbook](#) provides an overview of the FMI, its organisation and operational procedures.

The mandatory board structure of a German stock corporation (Aktiengesellschaft, AG) like CEU is the two-tier system: It is composed of an Executive Board and a Supervisory Board. The Executive Board is the corporate body managing and representing CEU in accordance with section 76 of the Aktiengesetz (AktG, German Stock Corporation Act). The Supervisory Board is supervising and advising the Executive Board in accordance with section 111 of the AktG.

As a public limited liability company, the general principles as set out in the AktG are applicable. Control over the company is exercised by the shareholder(s) in the General Meeting, the roles and the responsibilities of the Executive Board and the Supervisory Board are defined by the AktG, the Articles of Incorporation and the Rules of Procedure for the respective bodies.

General Meeting

The General Meeting is the most significant body of the stock corporation. It appoints the Supervisory Board, ratifies the acts of the Executive and Supervisory Board members and passes resolutions on all fundamental issues.

The Articles of CEU do not expressly reserve specific power to the General Meeting of the shareholders other than the powers set out by the law in sections 119 et. seq. of the AktG. Shareholders may exercise the membership rights that result from holding shares in the General Meeting. CEU has only one shareholder and is therefore wholly-owned. The rights of the General Meeting are listed in section 119 of the AktG. The General Meeting may decide on:

- Appointment (and removal) of Supervisory Board members (unless they are elected by the employees; for CEU, one third of the Supervisory Board members must be elected by the employees due to the One-Third-Participation Act);
- Appropriation of the net income;
- Ratification of the acts of the members of the Executive Board and of the Supervisory Board;
- Appointment of the auditor;
- Fundamental measures, for example, the amendment of the Articles of Incorporation, capital increases or decreases and the approval of the conclusion of intercompany agreements (control and/or profit and loss transfer agreements) and transformations (mergers, spin-offs etc.).

The annual financial statements are prepared by the Executive Board and must be approved by the Supervisory Board. The adopted and approved annual financial statements are then presented to the Annual General Meeting, but a formal approval by the shareholders is usually not required.

Finally, the sole shareholder takes note of the report on the remuneration of the members of the Executive Board, which the chairperson of the Supervisory Board submits for information. The sole shareholder also notes that the Supervisory Board appointed an external auditor for the respective financial year.

In addition, Deutsche Börse AG and CEU entered into a domination agreement according to which Deutsche Börse AG is authorised to issue instructions to the Executive Board of CEU regarding CEU's management, except where the execution of such instructions would cause CEU or its corporate bodies to breach the obligations imposed on them under the KWG (German Banking Act) and its ancillary provisions.

Supervisory Board

Supervisory Board members are elected by the General Meeting for a term of office ending at the closing of the General Meeting which votes on the approval for the fourth fiscal year after the commencement of the term of office. It consists of six members and is bound to advise and supervise the Executive Board while strictly maintaining business information confidential (chapter 9 (1) of the Articles of CEU).

The Supervisory Board has – inter alia – the following tasks:

- Appointment of the members of the Executive Board pursuant to section 84 of the AktG;
- Decision on which of the Executive Board's transactions need previous Supervisory Board consent without violating the Executive Board's representation rights concerning business correspondence (chapter 9 (2) of the articles of CEU).

The [Rules of Procedure](#) ("RoPs") of the Supervisory Board set out the procedures for its functioning, including the procedures to identify, address and manage conflicts of interest.

Processes for ensuring performance accountability are defined in the RoPs but also in other internal policies such as the Policy on Conflicts of Interest and the Business Continuity Management Policy. Furthermore, the design of the risk management and internal controls are defined in the corresponding risk management, internal audit and compliance policies/charters in order to provide clear and direct lines of responsibilities and accountability for key functions.

Executive Board

The members of the Executive Board are appointed by the Supervisory Board for a term no longer than five years. They conduct the business of the company in accordance with the applicable law, in particular the AktG, the Kreditwesengesetz (KWG, German Banking Act), relevant EU Regulations and EU Directives—notably the European Central Securities Depositories Regulation (CSDR)—, the Articles of Incorporation of the company, the RoPs, the schedule of responsibilities and their service contracts as well as applicable policies, in particular the Conflicts of Interest Policy.

The Executive Board manages and represents CEU, designs and establishes CEU's business strategy, the risk strategy and the strategy regarding capital adequacy and liquidity. It determines and coordinates the various departments of CEU. The Executive Board reports to the Supervisory Board.

Processes for ensuring performance accountability are defined in the RoPs but also in other internal policies such as the Policy on Conflicts of Interest, and the Business Continuity Management Policy. Furthermore, the design of the risk management and internal controls are defined in the corresponding risk management, internal audit and compliance policies/charters in order to provide clear and direct lines of responsibilities and accountability for key functions.

Committees

In line with CSDR, CEU has set up the following committees: Audit Committee, Risk Committee, Remuneration Committee. The members as well as tasks and responsibilities of the committees are described on the [Clearstream website](#).

In addition, CEU established two [User Committees](#) pursuant to Article 28 of CSDR in order to advise the Executive Board of CEU (see [key consideration 7](#) for details).

Disclosure of governance arrangements

CEU discloses information about its governance structure publicly in the [Corporate Governance](#) section of its website.

In addition, CEU also publishes a [link to its banking licence](#) on its website.

Additional information related to governance provided to the public in the About Clearstream section includes, but is not limited to:

- [Articles of Incorporation](#)
- [CEU's CPMI-IOSCO disclosure framework](#)
- [Remuneration information](#)

Moreover, CEU publishes annually its [Association of Global Custodians Questionnaire disclosure response](#) on its website.

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.

As set out in [key consideration 2](#), the mandatory board structure of a German stock corporation such as CEU follows the two-tier system. The Executive Board is the corporate body managing and representing CEU, the Supervisory Board monitors and advises the Executive Board.

Roles and responsibilities of CEU's Executive and Supervisory Boards

The Supervisory Board, which is appointed by the General Meeting, is bound to advise and supervise the Executive Board while strictly maintaining confidential business information. The Supervisory Board may choose which of the Executive Board's transactions needs their previous consent without violating the Executive Board's representation rights concerning business correspondence.

Processes for ensuring performance accountability are defined in the respective RoPs but also in other internal policies. Furthermore, the design of the risk management and internal controls are defined in the corresponding risk management, internal audit and compliance policies/charters, including a specific Conflict of Interest Policy, in order to provide clear and direct lines of responsibilities and accountability for key functions.

CEU is accountable to (i) its shareholder(s); (ii) the German authorities in accordance with the Kreditwesengesetz (KWG, German Banking Act) and relevant EU Regulations such as, in particular, the European Central Securities Depositories Regulation (CSDR) and (iii) its participants pursuant to the provisions of its General Term and Conditions (GTCs).

How CEU handles EB and SB members' conflicts of interest

CEU has adopted Deutsche Börse Group's conflicts of interest framework which is detailed within the Group's Code of Business Conduct and, more specifically, the Policy and Guideline on Conflicts of Interest. The framework aims to address all types of conflicts of interest that could arise, and has identified, among others, the following potential sources of conflicts:

- (i) Corporate conflicts of interests: arising on entity level (including CEU)
- (ii) Personal conflicts of interest: originating from a source beyond the employee's professional obligations, and interfering with its objectivity to make decisions or to participate in decision making processes in the course of professional obligations
- (iii) Specific conflict situations: examples might be misuse of information or misuse of relationships

Section 15 of the RoP for CEU's EB details the procedure to identify, address and manage conflicts of interest with regard to respective board members. The corresponding rules and procedures applicable to members of CEU's SB are set out in Section 15 of the RoP for this board.

In addition, a Conflict of Interest Register is set up and continuously maintained for each of Deutsche Börse Group's CSDs, including CEU, to document and track potential and actual conflicts of interest. The Register is maintained by Group Compliance, who upon notification runs conflict assessments and defines mitigating measures with the parties concerned by the (potential) conflict situation. CEU's Chief Executive Officer (CEO) decides on the procedures to be followed and the measures to be adopted in order to manage conflicts of interest at the level of the company's EB. The CEO takes their decision in close cooperation with Group Compliance supported by CEU's CCO. The same applies to the chairperson of the Supervisory Board with regard to conflicts at the level of the SB.

Clearstream currently runs a bi-annual survey of related parties, where the members of the CEU EB and the SB must disclose whether they have been related to any other entity of Deutsche Börse Group. Material legal transactions between companies within Deutsche Börse Group and members of the company's EB (including related parties or related enterprises) require the prior consent of the SB.

Role and responsibilities of CEU's Supervisory Board committees

CEU's SB has established three committees to provide the board with critical assessments with respect to the organisation and operation of CEU in order to enable the SB members to fulfil their supervisory mission and to take on their responsibility pursuant to the applicable national and European laws. These SB committees are:

- (i) **Risk Committee:** advising the SB on the overall risk strategy and the current and future risk appetite and assisting the SB in assessing the adequacy between the risks incurred and CEU's ability to manage these risks as well as the internal and regulatory own funds and liquidity reserves
- (ii) **Audit Committee:** assisting the SB with the fulfilment of its supervisory mission related to reporting and accounting, internal audit, and external audit
- (iii) **Remuneration Committee:** assisting the SB in any tasks in relation to the remuneration of employees, remuneration policy and remuneration system

The SB committees include members of the SB who are not members of the EB. Each committee is composed of at least three members. To ensure separation between the committees, the chairpersons as well as most of their members are different.

As mentioned in [key consideration 2](#), CEU has established two User Committees, gathering participants and issuers of CEU's SSS, in charge of advising the management body as laid down in Article 28 of CSDR. See [key consideration 7](#) for more details.

Review of performance

In order to be compliant with regulatory requirements, candidates and members of the Executive and Supervisory Boards individually and collectively, must run through a suitability assessment, which is initiated by the chairperson according to the provisions of the KWG and the respective Suitability Assessment Policy of the company.

The performance of the Supervisory Board of CEU is assessed yearly. In addition, the performance of the Supervisory Board of CEU is assessed every fifth year by an external third party, this was last performed in 2023.

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).

As required for companies with a two-tier board structure, none of the members of the Supervisory Board (SB) of CEU has an executive function within CEU. In addition, one third of the members of the Supervisory Board, i.e. two members, are fully independent of the company in accordance with Article 27 (2) CSDR. The chairpersons of both the Audit Committee and Risk Committee are independent members of the Supervisory Board.

Members of CEU's SB and EB are subject to a thorough suitability assessment to ensure that both boards fulfil the criteria regarding skills and incentives. The guiding principles for such assessment are set out in the following documents:

- [Joint ESMA and EBA guidelines on the assessment of the suitability of members of the Management Body and key function holders \(EBA/GL/2017/12\)](#)
- Deutsche Börse Group's Suitability Assessment Policy
- Side letter to Deutsche Börse Group's Suitability Assessment Policy (adopted by CEU; provides job descriptions for SB and EB members as well as key function holders)
- [Clearstream Group Remuneration Policy](#)

The Suitability Assessment Policy is reviewed by the SB at least once a year to ensure that it remains appropriate and complies with the legal and regulatory requirements applicable to CEU.³ The objective of the policy is to ensure that all members of CEU's SB and EB are suitable with respect to the following governance criteria stipulated in the joint ESMA and EBA guidelines:

- Time commitment
- Knowledge, skills and experience
- Reputation, honesty and integrity
- Independence of mind

³ Owner of the policy is Deutsche Börse Group's Human Resources (HR) function. It designs and organises the regular review with the assistance of Group Legal and the Boards & Committees units for the individual group entities. CEU's Corporate Governance Post-Trading unit is responsible for content and review regarding the suitability assessment for CEU's SB and EB members. HR assumes responsibility for content and review regarding the suitability assessment for key function holders.

- Diversity
- Independence (for SB members)

CEU's SB is responsible for ensuring that the individual SB and EB members, as well as the SB and EB collectively, fulfil the above suitability criteria both upon new appointments and on an ongoing basis. To this end, individual and collective suitability assessments are conducted once per year and prior to any appointment by the SB. In addition, the assessment of the SB's and EB's collective suitability will be initiated in the following situations:

- (i) When members of CEU's SB or EB must be reappointed, and the requirements of the position have changed or the members are appointed to a different position within the respective board
- (ii) When members cease to be members of CEU's SB or EB
- (iii) Whenever appropriate, e.g. due to a material change to the scope of CEU's business model, risk appetite or strategy

In addition, the SB initiates a suitability assessment for individual SB and EB members whenever appropriate (for instance, in the event of reduced working time, a change in the scope or nature of the mandate, or negative event with regard to the reputation of the appointed board member).

Should the suitability assessment conclude that an SB or EB member is not compliant with the requirements in total, CEU will take appropriate measures to rectify the situation and will inform the competent authority (BaFin) accordingly.

CEU's annual suitability assessments in 2024 and 2025 concluded that both the SB and EB are suitably skilled to perform the responsibilities entrusted to them.

With respect to the above criterion of independence of the SB, CEU's SB includes both non-executive and independent members. In accordance with Article 27 (2) CSDR and KWG, CEU considers an independent director one who has no business relationship (e.g. no relationship with a competitor of CEU), family or other relationship (including an employment relationship) that raises a conflict of interest regarding CEU, its controlling shareholders, its management or its participants, and who has had no such relationship during the five years preceding the membership in the SB. The board is composed of at least one third, and in any case no fewer than two independent members.

Different measures ensure that the long-term achievements of the institution's objectives are reflected in the remuneration:

1. The Clearstream group has a remuneration policy pursuant to CRD which integrates CEU's risk appetite. The interests of investors are taken into consideration and remuneration systems are in line with the company's risk strategy.

Variable remuneration at CEU can be paid only if a certain number of performance criteria are met by the institution. As mentioned in the remuneration policy, the determination of the total amount of the variable remuneration: (i) "shall take due account of the risk-bearing capacity, the multi-year capital planning and the profitability of the Group and/or respectively Clearstream Europe AG", (ii) "must ensure the Group's and respectively Clearstream Europe AG's ability to maintain or recover appropriate own funds and liquidity and the combined capital buffer requirements in accordance with the German Banking Act (KWG)".

2. The remuneration structure and the pay-out schedule of variable remuneration for EB members are aligned with sustainable and long-term performance (deferral mechanism and instruments ensure an incentivising of sustainable achievement of CEU's financial and non-financial objectives). In principle, performance-based variable remuneration is not guaranteed, and, under performance conditions, EB members are eligible to receive a performance-based variable remuneration.

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 CEU's Supervisory and Executive Boards

The roles and responsibilities of CEU's SB and EB are described in detail in several documents, notably in the company's Articles of Incorporation and the Rules of Procedure (RoPs) for the two boards (see also [key considerations 2 and 3](#)).

Without prejudice to the powers of the SB, the EB assumes, among others, the following tasks:

- Prepare and implement procedures, policies and processes by which the EB operates
- Establish clear objectives and strategies for CEU
- Establish adequate remuneration policies for employees of the company
- Ensure the surveillance of the risk management function and take decisions related to risk management
- Ensure the independence and adequate resources of the risk management, technology, compliance and internal audit functions
- Approving and regularly reviewing the outsourcing policy and monitoring outsourcing arrangements
- Monitor and ensure compliance with all relevant regulatory and supervisory requirements
- Be accountable to shareholders or other owners, employees, users and other relevant stakeholders
- Approve the internal audit planning and review
- Review and update regularly the governance arrangements of CEU
- Where the EB delegates tasks, retain the responsibility for decisions that may affect the smooth provision of services by CEU
- Hold the final responsibility for managing CEU's risks
- Set CEU's risk strategy, including risk appetite and global framework for taking, managing and monitoring all risks
- Ensure that CEU's policies, procedures and controls are consistent with its risk strategy and risk appetite and that these policies, procedures and controls address how CEU identifies, reports, monitors and manages risks

Without prejudice to the powers of the general meeting of shareholders and of the EB, CEU's SB assumes, among others, the following tasks:

- Review and ensure that well-established procedures, policies and processes by which the EB, the SB and the Committees shall operate, exist and are well implemented

- Acknowledge the objectives and strategies of CEU proposed by the EB
- Effectively monitor the EB
- Establish adequate remuneration policies for the members of the Executive Board and review the remuneration policies established by the Executive Board for other employees of the Company
- Monitor the EB in ensuring the surveillance of the risk management function and in taking decisions related to risk management
- Monitor the EB in ensuring the independence and adequate resources of the risk management function, technology function, compliance function and internal audit function
- Monitor the EB's setting of guiding principles governing central administration and outsourcing arrangements
- Monitor the EB in monitoring and ensuring compliance with all regulatory and supervisory requirements
- Be notably accountable to the shareholders and partially to other owners, employees, users and other relevant stakeholders
- Acknowledge the internal audit planning and review
- Review and update regularly the procedures applicable to the EB and SB
- Hold the final responsibility for monitoring the performance of the management body as well as the systems that ensure an effective risk management
- Acknowledge the risk strategy (including risk appetite and global framework for taking, managing and monitoring all risks) as set by the EB
- Monitor the EB in ensuring that CEU's policies, procedures and controls are consistent with its risk strategy and risk appetite and that these policies, procedures and controls address how CEU identifies, reports, monitors and manages risks

Experience, skills and integrity

As set out in the joint ESMA and EBA guidelines on the assessment of the suitability of members of the Management Body and key function holders, CEU's SB and EB members must fulfil certain criteria (see also [key consideration 4](#) for details). Among others, each member shall be of sufficiently good repute and shall have appropriate skills, knowledge and experience.

In order to ensure that CEU's SB and EB members have the appropriate experience, a mix of skills, and the integrity necessary to discharge their responsibilities for the company's operation and risk management, candidates for and members of CEU's SB and EB are subject to a suitability assessment. This assessment is performed for both boards on an annual basis, as well as on an ad hoc basis when changes in the respective board occur. Please refer to [key consideration 4](#) for details on the conditions and implementation of the assessment procedure.

The scope of responsibilities—and hence, implicitly, the related required skills—of the individual members of CEU's EB is linked to the departments they are responsible for. These departments are defined in a schedule of responsibilities. This schedule must be announced to the SB without delay following its definition. Enactment, modification and revocation of the schedule of responsibilities require a unanimous resolution of the EB. If a unanimous resolution does not pass, the CEO must petition the SB to approve the schedule of responsibilities. Every EB member has sole managerial authority within the framework of the department assigned to them by the schedule. Without prejudice to the division of responsibilities, each EB member remains responsible for the management of the company as a whole.

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 crises and emergencies. Governance arrangements should ensure that the risk management and internal control functions have sufficient authority, independence, resources, and access to the board.

Effective and efficient risk management is an elementary component of the management and control of CEU. The different aspects of CEU's risk management framework including risk tolerance, responsibilities and accountability for risk decisions, as well as decision making processes in crises and emergencies, are clearly described, among others, in the following key documents:

- Deutsche Börse Group's Risk Management (GRM) Policy
- Deutsche Börse Group's Risk Taxonomy⁴
- Deutsche Börse Group's and Clearstream's risk type-specific handbooks
- Clearstream Risk Strategy and Risk Appetite Framework
- Clearstream Risk Governance Guideline
- Clearstream Stress Testing Handbook
- Clearstream Model Risk Management Policy and Model Validation Guideline
- CSDR Application
- Deutsche Börse Group's Incident and Crisis Management Policy and Guideline

The risk management framework in terms of processes, roles and responsibilities is applicable to all CEU staff. Its overall objective is to enable CEU's EB to monitor the company's overall risk profile, as well as specific material risks, so that developments that could jeopardise the interests of CEU can be identified at an early stage and suitable countermeasures deployed. This is achieved through periodic and ad hoc reporting on all significant risk developments to CEU's EB. The reporting procedures are further described in the handbooks for every risk type. For example, operational risk reporting is documented in the Operational Risk Handbook.

CEU has been included throughout the development of Deutsche Börse Group's Risk Taxonomy. The taxonomy distinguishes between five aggregated risk types:

- Operational Risk
- Financial Risk
- Business Risk
- Pension Risk
- Winding-down and Restructuring Risk

⁴ The Risk Taxonomy is a comprehensive list of all potential risk items that the Group (and its entities) may be exposed to due to its current and future business operations, with a focus on a twelve-month time horizon.

Clearstream's risk appetite framework is based on its business strategy and sets limits specifying the maximum risk permitted for the above risk types as well as the company's overall risk. This is done by laying down respective requirements for risk management, control and limitation. CEU ensures that appropriate measures are taken to avoid, reduce and transfer, or intentionally accept, risk. See also [Principle 3](#).

CEU's Risk Committee is responsible for advising the SB on the CSD's overall current and future risk tolerance and strategy. Its tasks and responsibilities are to:

- Advise the SB on the institution's overall current and future risk appetite, risk tolerance and risk strategy and assist the SB in overseeing the implementation of that strategy
- Support the Supervisory Board in fulfilling its supervisory duties with regard to information and communication technology (ICT) and information and communication technology security, including cyber risks, and oversees the monitoring of information security services and risks, including the ICT risk management framework
- Review whether the conditions offered to clients take into account the institution's business model and risk structure. If this is not the case, the risk committee submits proposals to the Executive Board, how the conditions to clients in accordance with the business model and the risk structure could be created, and
- Examine whether incentives provided by the remuneration system take into consideration the risk, capital and liquidity structures of the institution, and the likelihood and timing of earnings. The tasks of the SB's Remuneration Committee remain unaffected

CEU's risk management processes and measurement systems are subject to regular reviews performed by the Internal Audit function, as well as external auditors. Ultimately, Internal Audit acts as third line of defence by providing assurance via independent audits, which verify that risk control and risk management are performed adequately. The results of these audits are part of CEU's risk management system.

Regarding decision making in crises and emergencies, the incident and crisis management processes applicable to CEU are set out in Deutsche Börse Group's Incident and Crisis Management Guideline. This guideline aims to facilitate the coordinated and rapid reaction to an incident/crisis in a controlled and effective manner, in order to contain and resolve the incident, minimise business and market impact and return to normal activity as quickly as possible.

In case of crisis events such as a credit crisis, recovery crisis, or other types of events that could affect the financial stability and resilience of the company, a Clearstream Crisis Management Team (CCMT) may be activated. The main role of the CCMT is to gather and coordinate all relevant information related to a crisis in order to mitigate the adverse effects on Clearstream, its participants and other market participants. The CCMT monitors the crisis, elaborates mitigating measures and develops an adequate response strategy to resolve the crisis.

CEU's governance arrangements ensure that the company's risk management and internal control functions have sufficient authority, independence, resources, and access to the board: according to its rules of procedure, the SB is tasked with monitoring the internal control system, risk-taking and risk management framework and their effectiveness to manage risks, including whether the company has adequate resources.

Furthermore, CEU's chief risk officer, chief compliance officer, chief technology officer, chief information security officer and chief internal auditor have direct access to the SB. For this purpose, the respective officer shall usually contact the SB's chairperson and/or the chairpersons of the relevant committee, as appropriate.

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

For the description of CEU's design and strategy, please refer to [key consideration 1](#). For its rules, please refer to [key consideration 4 of Principle 1](#).

CEU has a multifarious array of stakeholders, which can be broadly categorised into four groups as follows:

Stakeholders to whom CEU provides a service, that is:

- Issuers
- Issuer agents
- Participants
- Clients of participants
- (I)CSDs

Stakeholders who provide a service to CEU, that is:

- (I)CSDs (domestic and international CSDs)
- Domestic depository banks, agent banks and international depositories (i.e. common depositories, common service providers and common safekeepers)
- Transfer Agents and Order Handling Agents
- Cash Correspondent Banks (CCBs)
- Connectivity providers such as Swift
- Eurosystem⁵, as provider of the settlement platform T2S

Stakeholders involved in the formation of the legislative and regulatory framework in which the Clearstream group operates, that is:

- Market associations
- National governments
- Supranational legislative bodies (such as the EU Commission)
- CEU's regulators

⁵ In the case of CEU, Deutsche Bundesbank acting in the name of the Eurosystem as signatory of the T2S Framework Agreement

Stakeholders with a direct influence on CEU's equity, that is:

- Parent companies
- End investors

Stakeholders to whom CEU provides a service

CEU follows an active approach towards its participants, among others, organising regular participant meetings, forums and trainings, as further described in [Principle 21, key consideration 1](#) and [Principle 23, key consideration 3](#). All participants are assigned a relationship manager who maintains permanent communication with them and may report any individual participant issues to CEU's decision making bodies. In the context of the review of CEU's General Terms and Conditions (GTCs) and other governing documents, amendments are notified to all participants.

Additionally, CEU has established two [User Committees](#) for the securities settlement systems (SSS) it operates. According to their Terms of Reference, these committees have the mandate to advise CEU's EB on key arrangements that impact the users, including the criteria for accepting issuers or participants, and the service level. The User Committees may moreover submit non-binding opinions to CEU's EB, containing detailed reasons, regarding the company's pricing structure. The meeting minutes of the User Committees are regularly presented to the EB. The EB of CEU takes account of the interests of the FMI's participants and other relevant stakeholders in its decision-making through advice received from the User Committees, as mentioned above, on key arrangements that impact the users, including the criteria for accepting issuers or participants, and the service level. The User Committees meet at least twice a year. CEU promptly informs the User Committees as well as the competent authority (BaFin) of any decision in which the EB decides not to follow the advice of the committee. In addition, BaFin receives an annual report including any decision of CEU's EB regarding following or not following the advice of the User Committees. A description and the Terms of Reference of the User Committees are published on the [Clearstream website](#).

Furthermore, CEU also participates in public consultations that may be directly relevant to its services and impact its participants, either initiated by law makers or regulatory bodies. CEU also participates in a number of industry related associations and forums which aim at promoting standards and defining guidelines for the industry (for example, ECSDA, ICMA, ICMSA, ISMA, ISLA and ISSA; see also [key consideration 1](#) and below). Thus, the company actively aligns with its stakeholders, allowing participants to be informed of market needs or changes and to be able to voice and discuss new regulatory requirements, potential new services or participants' concerns which may lead to changes in existing services.

CEU supports issuers and issuer agents in making their securities eligible on its platform and to best harmonise and standardise the market in the interest of all participants.

Stakeholders who provide a service to CEU

Existing relationships with CSDs and/or depositories/agent banks, transfer agents (TAs), CCBs, Euroclear Bank and connectivity providers are reviewed on an ongoing basis. In addition to periodic visits according to defined schedules, CEU may also choose to visit a supplier at any time to review the relationship and ascertain that all governing documents remain relevant to the activities and regulations of the market or request that the supplier visits CEU's premises. The service level agreements with its suppliers are updated as and when necessary, and on average, this is done on an annual basis.

For T2S, the T2S Framework Agreement is the core contractual document between the Eurosystem (acting via the ECB and participating euro-area national central banks) and each Contracting Central Securities Depository (CSD). It sets out the detailed rights, duties, operational rules, and governance arrangements covering the provision and use of T2S services. The CSD Steering Group (CSG) assess on an annual basis whether an update of the T2S Framework Agreement is required. CEU participates in that review process. Updates apply to all Signatory CSDs.

Institutions providing links to domestic markets abroad inform CEU of any changes to market practice and regulation in the market in question. Similarly, Clearstream's Network Management team informs such providers of upcoming changes to CEU's services, as well as working with them to develop new service offerings. Furthermore, a legal opinion per country is obtained on an annual basis.

Stakeholders involved in the formation of the legislative and regulatory framework in which the Clearstream group operates

Clearstream is represented in more than 35 market organisations globally, through which it is able to identify and take into consideration a wide range of stakeholders' interests. CEU's participation in the regulatory debate and in industry forums has allowed the company to refine its core securities settlement and custody infrastructure in various areas such as the fund industry, collateral management services and securities financing. CEU cooperates with German regulators in many areas. As such the company takes into account their views, or seeks their approval, for taking major decisions like significant changes to its system design as well as to its rules and procedures.

Clearstream entities are represented in numerous market organisations globally:

- International Capital Markets Association (ICMA)
- European Repo and collateral Council (ERCC)
- International Securities Services Association (ISSA)
- International Capital Markets Services Association (ICMSA)
- International Securities Lending Association (ISLA)
- Securities Market Practice Group (SMPG)
- Society for Worldwide Interbank Financial Telecommunications (Swift)
- Association of National Numbering Agents (ANNA)
- Within Europe, the Clearstream group plays a leading role in various working groups and associations at EU level:
 - T2S Governance Bodies – CSD Steering Group, related technical groups and Task Forces
 - European Central Securities Depositories Association (ECSDA)
 - ECB's Advisory Group on Market Infrastructure for Securities and Collateral (AMI-SeCo), related groups, Task Forces and National Stakeholder Groups (NSGs)
 - ESMA's Post-Trading Working Group (PTWG)
 - EU T+1 Industry Committee and technical workstreams

On a national level, the Clearstream group maintains a strong network across several domestic markets and is particularly well represented in its home markets: Germany and Luxembourg. In Germany CEU is a member of the Bundesverband deutscher Banken e.V. (Federal Association of German Banks).

CEU delivers roughly 55% of T2S settlement volumes, and Germany is the home market of the Deutsche Bundesbank, one of the four European central banks mandated to develop and operate the T2S platform (4CB). The Clearstream entities (CEU and LuxCSD) were among the first CSDs to sign the T2S Framework Agreement. Clearstream continues its leading role by contributing actively to the further enhancement of the pan-European settlement platform, establishing links with all CSDs in T2S where possible and initiating Change Requests to streamline T2S in line with the T2S ambition of an efficient cross-border settlement platform for the European capital markets.

CEU additionally consults and obtains approval from its regulators before making significant changes to its design, rules and procedures.

Stakeholders with a direct influence on CEU's equity

Clearstream Holding AG is the sole shareholder of CEU. Thus, it assumes all powers conferred to the General Meeting of Shareholders (see [key consideration 2](#)). Clearstream Holding's decisions are recorded in a minutes register held at the registered office. Concerning the disclosure of major decisions made by CEU's Executive and Supervisory Boards to relevant stakeholders, that is, Clearstream Holding AG, receives extensive reporting on CEU activities.

CEU's Annual Accounts and Management Report are sent to its regulators and made available to its participants via the [website](#).

Major decisions are clearly disclosed to relevant stakeholders and the public: Major changes to CEU's SSSs, its operations and its rules are usually communicated to participants via announcements before they are being integrated into the documentation ([Key Documents](#)), like [General Terms and Conditions](#), the [Client Handbook](#) and other.

Principle 3: Framework for the comprehensive management of risks

An FMI should have a sound risk-management framework for comprehensively managing legal, credit, liquidity, operational, and other 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.

The Clearstream Risk Management function is responsible to develop strategies, policies, procedures and handbooks to identify, measure, monitor and report risks that arise in or are borne by the company. A crucial aspect of this process is establishing a clear risk appetite framework. Clearstream's risk appetite defines the type and level of risks the organisation is willing to accept in pursuit of its strategic objectives and business plan. Clearstream Risk Management comprises coverage of the three CSDs, being CEU, CBL and LuxCSD.

Risk management policies and procedures

Deutsche Börse Group's overarching Group Risk Management (GRM) Policy, as applicable to CEU, describes the enterprise-wide risk management concept, including the risk management framework in terms of processes, roles and responsibilities applicable to all staff and organisational units and levels. The GRM Procedure outlines the five-step risk management process applicable to CEU:

1. Risk identification
2. Notification
3. Assessment
4. Treatment
5. Monitoring/Reporting

The Treatment step describes the relevant risk response options, and encompasses risk avoidance, risk reduction, risk transfer and intentional risk acceptance.

All organisational units and employees must perform risk control, implement mitigating actions, and monitor these actions according to the established processes.

The Risk Taxonomy/Inventory, included within the GRM Procedure, stipulates the risk taxonomy for CEU. The Risk Taxonomy/Inventory is a comprehensive and complete list of all the potential risks that CEU may be exposed to due to its current and future business operations. The inventory includes all of the risks that CEU is aware of. Level 1 of the Risk Taxonomy/Inventory consists of the five aggregated key risk types as outlined below.

CEU undertakes a consistent, regular, structured identification and assessment process of all risks the entity might be exposed to due to its business model and industry environment. In addition to the annual risk inventory process, risk type specific risk items and drivers may be identified.

Risk types

CEU defines risk as a potential negative impact on its financial, revenue and liquidity situation. In line with Deutsche Börse Group's Risk Taxonomy, CEU differentiates between five aggregated risk types which are managed and controlled with distinct methods. The aggregated risk types are: operational risk, financial risk, business risk, pension risk, as well as winding-down and restructuring risk.

Operational risk

CEU defines operational risk as the risk of loss resulting from people, systems, inadequate or failed internal processes, or external events. The definition aligns with the industry-standard Basel formulation and is consistently applied across all Deutsche Börse Group entities, including CEU.

Operational risk comprises the following 17 risk clusters: compliance risk, contagion risk, corporate tax risk, custody risk, data integrity risk, information security risk, information technology risk, legal risk, model risk, operational project risk, people risk, physical security risk, process risk, product tax risk, risk management risk, secondary reputational risk and third-party risk.

Operational risks that CEU does not want to run and that can be insured against at reasonable cost are transferred by closing insurance policies. All insurance policies are coordinated centrally for entire Deutsche Börse Group thereby ensuring the uniform risk-cost benefit insurance coverage. Operational risk is assessed as a major risk type within CEU.

Financial risk

CEU is exposed to financial risks in the form of credit, market, and liquidity. Exposure to the above-mentioned risks is mitigated through the existence of effective control measures. These cover the risks inherent to market transactions, the ability to meet financial obligations, lending activities and settlement, such as the risk of default of business partners and entities performing specific functions.

Credit risk

Credit risk describes the risk that a counterparty might not meet its contractual obligations in parts or in full. Credit risk mainly arises in the short term and with credit institutions or governmental counterparties (risk of losses arising from the default of counterparties). Measurement criteria include the credit rating of the counterparty, the degree to which a credit line has been utilised, the collateral deposited and concentration risk. Historically, there have been no material credit losses at CEU.

CEU grants loans to its participants in order to increase the efficiency of securities settlement. However, these lending operations cannot be compared with those of other credit institutions. Firstly, the loans are extended solely on an extremely short-term basis (intra-day). Secondly, they are extended solely for the purpose of increasing the efficiency of securities settlement. These loans are fully collateralised and only granted to creditworthy participants with very good credit ratings. Furthermore, credit lines granted are uncommitted and can be revoked at any time.

The creditworthiness of potential participants is assessed before entering into a business relationship. In addition, CEU establishes participant-specific credit lines on the basis of both regular reviews of the participant's creditworthiness and ad hoc analyses as required.

Furthermore, credit risk can arise from cash investments and cash holdings at cash correspondent banks (CCBs) and at CBL. CEU reduces this risk by secured investing via collateralised overnight placements with CBL. CEU establishes credit limits based on annual credit assessments and ad hoc analyses as required. The creditworthiness of CEU's CCBs and counterparties is also assessed on an annual or, if necessary, ad hoc basis.

Market risk

Market risk is the risk of losses arising from holding assets and liabilities – on- or off-balance sheet – with different maturity dates, creating exposure to changes in the level of interest rates, foreign-exchange rates or market prices. Market risk consists of the following risk clusters: credit driven market risk, equity price risk, foreign-exchange rate risk, interest rate risk, market concentration risk, market risk of non-consolidated entities and market volatility risk.

Market risk may arise in the form of interest rate risk (as a result of fluctuations in interest rates in connection with cash investments or borrowing), currency risk (in the operating business, when recognising net revenues denominated in foreign currencies or when holding positions in foreign currencies) and in the form of equity price risk.

CEU is exposed to interest rate risk in connection with cash investments as part of its capital is invested in securities with the highest credit quality. Some of these securities have floating interest rates, with a low sensitivity to interest rate fluctuations, but also fixed coupon bonds have been bought leading to increased interest rate risk. Interest rate risk is mitigated using a limit system that only permits maturity transformation to a small extent. Open currency positions are avoided whenever possible.

Liquidity risk

Liquidity risk is the risk of losses arising from the inability to meet payment obligations when they come due or without incurring excessive costs. Liquidity risk consists of the following risk clusters: funding/refinancing risk, illiquidity risk, intraday liquidity risk, market liquidity risk and liquidity concentration risk.

CEU is exposed to liquidity risk in that it may lack sufficient liquidity for its intra-day cash operations or incur increased refinancing costs in the event of liquidity shortage. Daily and intra-day liquidity is monitored closely by the Treasury and Risk departments and managed with the help of a limit system. Sufficient credit lines and funding sources are available to provide cover in extreme situations. Further details on the robust framework to manage CEU's liquidity risk are described under [Principle 7, key consideration 1](#).

Business risk

CEU's business risk is the loss (including losses arising from missed opportunities) arising from strategic decisions and/or their implementation, or from the inability to adapt to external factors.

Unexpected loss due to deviations (positive or negative) from earnings before tax is calculated using Earnings at Risk (EaR). The methodology is based on quarterly relative deviations between expected and actual profit and loss figures. Business risk is reported, if calculated Value at Risk (VaR) is higher than budgeted earnings before tax for the next four quarters. Business risk is considered material for CEU. In addition, CEU applies a scenario-based approach to assess the impact on material revenue and cost drivers by estimating potential loss scenarios. Business risks for CEU mainly arise from macroeconomic, geopolitical, and corporate strategic developments. Such business risks may affect revenue and cost development, for example, if revenues fall short of the corresponding planning assumptions or if costs increase.

Pension risk

Pension risk is defined as the risk of losses due to increased costs from post-employment benefit plans based on non-market risk factors. The expected pension payments and therefore the overall pension risk is influenced by several factors: longevity in terms of unexpected changes compared to the anticipated life expectancy, inflation in terms of unexpected changes compared to the projected inflation rate, salary growth in terms of unexpected changes compared to the forecast salary growth and discount rate in terms of unexpected changes compared to the anticipated discount rate.

CEU is exposed to pension risk by its pension debt obligations, primarily managed through a Contractual Trust Arrangement (CTA). Pension risk is quantitatively shown to be immaterial for CEU. However, pension risk is chosen to be managed as a material risk for CEU, that is, it is considered as an immaterial risk in the risk profile, but processes are applied treating it as a material risk type.

Winding-down and restructuring risk

Winding-down and restructuring risk is defined as the risk of losses due to insufficient capital being held for an orderly winding-down or restructuring of operations and services, in the case where new capital cannot be raised. This risk type is addressed by the capital requirements outlined by CSDR as well as by comparable requirements laid out in BRRD for CRR institutions (MREL which targets financial and operational continuity). Winding-down and restructuring risk is considered material for CEU.

Risk management handbooks

The Operational Risk Handbook gives a comprehensive description of the objectives, overall approach and scope of operational risk management at Clearstream, considering that operational risk management is an essential component of management and controls of operations. The Handbook includes topics such as the definition of and categories within operational risk, organisational structure, roles and responsibilities, operational risk instruments and methods used as well as the respective reporting.

Since January 1, 2025, CEU has adopted the Standardised Measurement Approach (SMA) to assess the operational risk capital requirement from a normative perspective under Pillar I. An enhanced Pillar II operational risk model has been implemented to assess the operational risk capital requirement from an economic perspective. CEU has established a comprehensive operational risk framework and a set of instruments meeting both the requirements from a regulatory and business perspective. The roles and responsibilities within operational risk management are assigned to the organisational units at a local level as well as to Clearstream Risk Management at a central level.

Clearstream Risk Management established an operational risk procedure that serves as a guide in addition to the Operational Risk Handbook, primarily for the business departments within the organisation. This procedure describes the approach and major instruments applied within the process of managing operational risks on a high level. Furthermore, it sets the internal standards regarding roles and responsibilities as well as the related duties of different legal entities within the Clearstream group.

Clearstream Risk Management also established Financial Risk Handbooks. The main objective of these handbooks is to provide a comprehensive description of the organisational structure, processes, models and methodologies that constitute CEU's financial risk approach. Financial risk comprises the risk of losses arising from the default of counterparties (credit risk), from holding assets and liabilities for on- and off-balance sheet items, for instance, interest rate risk or currency rate risk (market risk), the risk of losses arising from the inability to meet all short- and long-term obligations resulting from on- and off-balance sheet liabilities (liquidity risk).

In addition, Clearstream Risk Management has established a Business Risk Handbook and a Pension Risk Handbook. The objective of these handbooks is to provide detailed descriptions of the approaches and instruments applied within the management of business and pension risks. The handbooks include a detailed explanation of the frameworks and information on the functional organisation (governance). The description of the models and validation processes and reporting responsibilities are also provided in the handbooks.

The risk management framework including the underlying policies, procedures and handbooks is subject to periodic reviews, at least annually.

Risk measurement

CEU has installed a unified internal measurement framework for economic capital to measure and report all operational, financial and business risks across its organisation: the concept of “Value at Risk” (VaR). The purpose is to allow the overall risk appetite to be expressed in a comprehensive and easily understandable way and to facilitate the prioritisation of risk management actions. Furthermore, risk reporting consolidates all risk measures across the company (operational, financial and business risks), except for liquidity risk, which is covered in the CEU’s Liquidity Stress Testing Model.

The VaR quantifies the risks to which a company is exposed. It indicates the maximum cumulative loss that CEU could face if certain independent loss events materialise over a specific time horizon for a given probability. CEU’s models are based, in line with the Basel framework, on a one-year time horizon. Correlations between individual risk estimates are recognised when calculating the capital charge for operational risk. Between the individual risk types, the most conservative approach of a correlation of “1” is implemented.

CEU also performs VaR calculations in order to detect potential risk concentrations, as well as stress test calculations, which consider even more conservative model parameters than the regular VaR calculations.

The aim of CEU’s risk management framework is to set adequate and comprehensive risk management standards to ensure the sustainability of its operations and thereby smooth and efficient market operations.

This framework ensures that CEU:

- can identify, measure, monitor, manage and report risks it may be exposed to, and limits the risks it poses to others.
- applies appropriate risk control and monitoring measures to safeguard the integrity of financial markets and limit potential exposures and systemic risks.

CEU has put in place a wide range of internal control processes and procedures, including security, technical and operational organisational arrangements, as well as risk control measures, to ensure they protect both CEU and the interests of the external stakeholders, that means its users and their respective clients, the CSD links, CCPs, trading venues, payment systems, settlement banks, liquidity providers and investors.

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.

CEU puts in place a range of internal control processes and procedures in order to ensure that participants and, where relevant, their clients properly manage and address the risks they pose to the CSD. CEU discloses to its participants extensive information in the respective documentation that allows participants to assess the risks associated with the products and services CEU provides. The documentation describes the activities performed by the CSD and all related obligations, rights, termination clauses, liabilities, breaches, the default and technical specifications. CEU explicitly states the risks associated with each product or service it offers.

Key participants, identified according to ESMA RTS Article 67, are managed, monitored and reported. In essence, they are subject to enhanced due diligence measures for the assessment of their risk management capabilities, that means:

- Participant settlement transaction activities (driven by volumes and values of trades settled in CEU's SSSs) are reviewed on a quarterly basis in order to generate key statistical information essential to identify and assess key participants.
- Additionally, the key participant lists are used by operational teams to map the participant causing operational incidents where relevant, further cementing CEU's view of the key participant risk exposures.

Please refer to [Principle 19](#) for details on the identification, management and monitoring of CEU's key participants.

In principle, this approach allows the CSD to derive the relevant risk metrics to support its business continuity management, recovery plan and default management procedures. In doing so, CEU ensures and obliges its key participants to have sufficient measures in place to properly manage and address the risks they pose and thereby minimise to the maximum extent possible the potential risks posed for CEU.

In addition, specifically in relation to KYC/AML, CEU has adapted its Client Due Diligence procedures to take into account the fact that it may not know the identity of the clients of its participants. For this reason, the enforcement history and exposure of CEU's participants is also subject to continuous review as part of the enhanced KYC programme. To further reduce risks of this type, there are enhanced KYC controls around the use of omnibus accounts and controls around the opening of additional accounts for existing participants.

CEU discloses to its participants extensive information in the respective documentation that allows them to assess the risks associated with the products and services CEU provides. CEU's product documentation, and, in particular, the Client Handbook and Product Guides, provide the necessary information for participants to assess the risks they face from the CSD.

Moreover, CEU participants can choose from a range of reports available to help them manage and contain the risks they pose to CEU's SSSs. Reporting profiles can be set up that are tailored to their own business requirements. Participants are asked to specify which reports they want to receive, respectively to retrieve, and via which communications media.

CEU has established two [User Committees](#) composed of issuers and participants, with the mandate to advise the management body on key arrangements that impact CEU's 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 CEU bears from other entities

CEU regularly assesses identified material risks it bears from other entities and that can potentially impact the smooth running of business services and the soundness and stability of the financial markets and system as a whole. CEU ensures that appropriate countermeasures are in place to adequately address these risks. Measures include the management of material risks related to:

- (i) Availability risk borne from reliance and connectivity to Swift, IT systems and applications for the provision of essential core business services
- (ii) Service deficiency risks borne from operational interdependencies of the company's critical outsourcing and third-party governed services, CSD market links and supplier network providers
- (iii) Operational risks that may be posed by CEU key participants as well as credit risks related to participants in default

The identification and management of operational risk is further described under [Principle 17, key consideration 1](#).

With regard to critical entities (for example critical providers of services such as Swift), CEU has defined and implemented a critical service provider governance framework procedure based on the CPMI IOSCO FMI assessment methodology. For more details, please refer to [Principle 17, key consideration 7](#).

In addition, the identification of risks is based on the risk inventory list and assigned to at least one of Clearstream's risk clusters. Depending on the risk cluster, the risk assessment will take place from the second to the fourth quarter of the year. Clearstream Risk Management assesses the materiality of the Group's risk clusters by determining their potential impact on the entity's required economic capital. If the impact is valued greater than 2.5% of the economic capital, the respective risk cluster is classified as material. In terms of financial risk, each risk item is first assessed for materiality before the exposures of the material risk items are quantified. With regard to business and operational risk, the risk items (in the form of scenarios) are first quantified according to the applicable risk assessment procedures. Consequently, the materiality evaluation per risk item is implicitly determined by linked scenarios. CEU also performs risk-wide stress tests, which incorporate the interaction of all material risk types.

Material risks associated with products and services provided by CEU

In line with Article 34 (5) of CSDR, CEU discloses to all participants information that allows them to assess the risks associated with the products and services provided. CEU explicitly states the risks associated with each product or service it offers. The CSD's product documentation and, in particular, the Client Handbooks and Product Guides provide participants and (indirectly) their respective clients with information necessary to assess the risks they face when contracting with CEU. Thus, participants can perform their own risk assessments and handle the risk the CSD poses to them.

Material risks posed by CEU to other entities

CEU's interconnectedness to other FMIs (for example, stock exchanges, CCPs) makes substitution difficult, thereby increasing its interdependencies and subsequent potential operational and financial risks that could be posed to others.

As a result, CEU addresses the risks arising from interdependencies with other entities via crisis management arrangements outlining different scenarios of disruptions potentially caused by such interdependencies. These procedures also include alert escalation mechanisms, joint key crisis contact lists and joint contingency procedures.

Additionally, a business impact assessment (BIA) is performed on the core CSD functions at business unit level of the business lines in order to identify the critical functions and accordingly define unit recovery plans to support the business continuity and incident and crisis management measures that can assure CEU can adequately address the potential risk exposures identified from internal and external interdependencies and interconnectedness.

Moreover, when a participant is identified as a "key participant", due diligence is complemented by additional questions to assess the key participant's potential interdependencies on third-party providers for critical services.

All relevant data and information are collected, assessed and reported by the company's Risk Management team. The general risk management framework processes and procedures on which CEU relies for (i) assessing the effectiveness and (ii) reviewing risk management systems and tools, as described under [key consideration 1](#), are also applicable to risks related to interdependencies.

Clearstream Risk Management reports to CEU's EB, the Audit Committee and to the Risk Committee on a quarterly basis and to the SB at least on a yearly basis regarding the overall risk exposure profile of CEU. In those reports, the responsible EB members are informed of any material risks, their assessment and possible immediate countermeasures. The risk reports include and focus specifically on the VaR figures and the utilisation of the risk bearing capacity, potential issues, specific risk topics, as well as stress test results (risk-type specific, risk-wide, and reverse stress tests), and credit concentration assessment. In the event of a material impact from a new risk or the development of an existing risk, the Risk Management team may issue an ad hoc report to the relevant recipients.

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.

Scenarios that may prevent CEU from providing critical operations and services

CEU has identified different idiosyncratic and systemic scenarios, which could potentially prevent it from being able to provide its critical operations and services as going concern. The scenarios are based on plausible near-default events taking into account the requirements of the Annex to DR 2017/390, particularly points 6 and 7. In total, CEU has identified multiple stress scenarios, which are classified into following categories:

1. Different idiosyncratic scenarios affecting CEU's operational capacity as well as its capital and liquidity profile
2. Different market-wide scenarios affecting mainly CEU's liquidity and capital profile
3. A combination of idiosyncratic and market-wide scenarios to derive a larger stress magnitude, based on which the effectiveness of appropriate mitigating tools is tested accordingly

Recovery and orderly wind-down plans

CEU distinguishes between requirements for a recovery plan (mitigating a near-default situation), a restructuring and wind-down plan (ensuring a solvent wind-down) and a resolution plan (insolvent wind-down).

The recovery plan as well as the restructuring and wind-down plan are drawn up and maintained by CEU. Their purpose is to set out available tools of CEU to overcome severe financial and operational shocks that could potentially undermine CEU's viability and the sustainability of its business. Ultimately, the plans aim at ensuring the continuity of CEU's critical operations and services, also preventing significant adverse effects on the financial system. The resolution plan, on the other hand, is owned and drawn up by the National Resolution Authority (NRA) with the objective to resolve CEU in an orderly manner in case the strategies under the recovery plan or the restructuring and wind-down plan are not sufficient to prevent the failure of CEU. In concrete terms this means that CEU can no longer meet its obligations as they fall due or is at immediate and evident risk of not being able to do so ("failing-or-likely-to-fail" situation according to BRRD). CEU provides continuous support to the NRA for the preparation and maintenance of the resolution plan.

As aforementioned, the recovery, restructuring and wind-down plans outline the critical operations and services of CEU, which were identified and assessed in accordance with the requirements stipulated in EBA/Op/2015/ 05 and the Commission Delegated Regulation (EU) 2016/778. A function was classified as “critical”, when its discontinuance is likely to lead to a disruption of services that are essential to the real economy or financial stability in one or more Member States and when that specific function cannot be adequately substituted, that means other market participants are not able or willing to take over the functions provided by CEU in an adequate timeframe.

The recovery plan includes eight scenarios which assess whether CEU’s critical operations and services are affected as a going concern. The selected scenarios stand for severe but plausible near-default situations covering a full range of stresses, both CEU-specific (idiosyncratic) and market-wide (systemic). In general, the scenarios simulate the stress on CEU’s liquidity, capital, profitability and operational capacity. Furthermore, they test the adequacy of various recovery measures available to CEU, each with an execution plan identifying key processes and potential barriers to implementation.

CEU has identified a number of viable recovery options and evaluated them towards their applicability in times of stress. These options aim at helping CEU to restore its financial and operational viability in stress situations. They are grouped in recovery options covering the aspects of capital, liquidity, risk positions, and operational capacity.

The recovery plan as well as the restructuring and wind-down plan are reviewed and updated by Clearstream Risk Management at least annually to ensure their continuous improvement. The plans are subject to approval by CEU’s Executive Board before being submitted to the regulators.

The review and update process is initiated in one of the following cases:

- Regular annual review
- Significant changes in the legal or organisational structure of Clearstream
- Significant changes of the business model or the business activities of Clearstream
- Significant changes with respect to the financial or the risk situations, that have essential effects on the recovery plans
- Other important reasons that may apply

Principle 4: Credit risk

An FMI should effectively measure, monitor, and manage its credit exposure 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 largest participants and their affiliates that would potentially cause the largest aggregate credit exposures to the CCP in extreme but plausible market conditions. All other CCPs should maintain, at a minimum, total financial resources sufficient to cover the default of the one participant and its affiliates that would potentially cause the largest aggregate credit exposures to the CCP in extreme but plausible market conditions.

Key consideration 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.

CEU's framework to manage its credit exposures to its participants and the credit risks related to all of its business activities that give rise to credit risk (see below for details) is composed of the Clearstream Credit Strategy, the Credit Policy and the Credit Handbook. The credit strategy articulates the high-level core credit principles for the maintenance of a robust credit risk framework in order to maintain credit decisions that are determined according to well-defined and objective credit granting criteria. The said principles are designed to ensure the following:

- Credit exposures to individual participants and participant groups are mostly secured through the use of collateral and other equivalent financial resources
- Intra-day and overnight credit risk is identified, measured, monitored, and managed
- Collateral and other equivalent financial resources used to fully cover corresponding credit exposures are measured, monitored, and managed
- Potential residual credit exposures are identified, measured, monitored and managed
- Reimbursement procedures along with sanctioning rates are maintained, to discourage overnight credit exposures
- Controls exist to maintain the reporting of credit exposures in accordance with regulatory requirements
- Information on aspects of credit risk measurement, monitoring, and management are regularly disclosed to the market

CEU is exposed to credit risk arising from a number of different sources, but mainly from settlement and custody activities. Credit appetite is defined as CEU's non-binding tolerance for accepting credit risk. It is approved by the company's Executive Board, taking into account CEU's business strategy, its role as an operator of a securities settlement system (SSS), as well as the target risk profile on its credit portfolio. Credit appetite is expressed numerically as the maximum amount of all credit limits available to participants and counterparties, plus a predefined threshold.

Key elements of CEU's framework for managing credit risk include monitoring of credit limits, collateral, internal credit ratings and credit control, as well as stress testing.

The governing principles of the framework for managing credit risk are determined by CEU's Executive Board. The Board members review and approve the credit strategy on an annual basis. The Executive Board also assumes responsibility for ensuring that CEU's credit activities are executed within the said framework. In accordance with Article 59 (3) (a) of CSDR, the documents forming the company's credit risk framework has been filed with the relevant competent authorities.

Key consideration 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.

Credit risk may arise from settlement activities (mainly due to cash financing of these activities), custody (generally related to asset servicing activities) and treasury operations.

Credit risk arising from settlement activities

For settlement activities, credit risk arises when CEU grants intraday credit (cash loans) to its participants. The purpose of cash loans is to facilitate the settlement of securities transactions against payment. Credit lines are offered intraday via unconfirmed funds facilities (UCFs) and technical overdraft facilities (TOFs). The size of these credit lines is determined according to the trading activity and credit worthiness (or internal rating, respectively) of the participant, as well as the availability of appropriate collateral.

TOFs and UCFs for CEU participants are governed by CEU's Credit Terms and Conditions (CTCs) and General Terms and Conditions (GTCs). They are mostly granted on a secured basis and are fully collateralised. Unsecured credit limits may be granted to counterparties with strong credit standing where zero risk weight is applied by Regulation (EU) No 575/2013 with specific approval by CEU's Executive Board.

The company's rules with respect to the granting of intra-day credit facilities to participants set out a "waterfall principle" that applies to the allocation of the proceeds after the enforcement of the collateral is extended to secure the borrower's exposure under the CTCs.

Furthermore, CEU has in place effective reimbursement procedures of intra-day credit. To discourage overnight credit, CEU applies sanctioning rates to all overnight exposures, regardless of their root cause. These rates serve as an effective deterrent. CEU extends credit exclusively to participants who meet its creditworthiness standards. Credit lines remain uncommitted and can be revoked at any time.

Credit risk arising from UCFs

CEU grants UCFs which are intra-day credit facilities designed to facilitate the settlement of securities transactions, to provision participant foreign-exchange (FX) trades, and to withdraw income proceeds. UCFs enable participants to purchase securities or settle FX trades based on an anticipated receipt of funds from either a pre-advice, a sale of securities over the Bridge with Euroclear Bank or a sale over a domestic market link.

Credit risk arising from TOFs

TOFs are intra-day credit facilities which are used to facilitate the settlement of securities transactions. TOFs enable participants to borrow funds to purchase securities and provision participant FX trades.

Measuring and monitoring of credit exposures

As part of their measuring and monitoring responsibilities, Deutsche Börse Group's Credit Management team ensures the following:

- Credit exposures to individual participants and participant groups are monitored in order to be fully secured through the use of collateral and other equivalent financial resources.
- Intra-day and overnight credit risk is measured, monitored and managed.
- Collateral and other equivalent financial resources used to fully cover corresponding credit exposures are measured, monitored and managed.
- Potential residual credit exposures are measured, monitored and managed.
- Reimbursement procedures along with sanctioning rates are maintained, to discourage overnight credit exposures.
- Controls exist to maintain the reporting of credit exposures in accordance with regulatory requirements.

In addition, CEU uses the following tools to control identified sources of credit risk and undue credit risk concentration: the Exposure Management & Collateral reporting tool (EMC2) and the DvP Model 1 settlement system, which ensures simultaneous settlement of securities and funds transfers on a gross (trade-by-trade) basis. These tools allow CEU to aggregate and measure exposures. The risk management system is updated at regular intervals and provides a consolidated view of credit exposures arising from securities settlement-related credit exposures, calculated close to real time. The system also allows the generation of automatic and on-demand reports used in the process of measurement and monitoring.

Model 1 DvP system

Clearstream operates a Model 1 DvP system, ensuring simultaneous settlement of securities and funds transfers on a gross (trade-by-trade) basis. Funds and securities transfers process within the same (settlement) system. When participants give instructions to deliver or receive securities against payment, each securities transfer links to the specific payment. Accordingly, participant transactions settle by simultaneous book-entry debits and credits in their respective accounts. Book entries effected after completion of a processing run settle in such a way as to optimise settlement while remaining within pre-defined limits. As the Model 1 DvP system ensures true delivery versus payment, failure to settle does not result in the unwinding of the concerned settlement instruction.

Key consideration 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.

To fully cover exposures to each participant, CEU applies a conservative approach to credit granting and to its collateral eligibility criteria. The company mitigates credit risk on counterparties by granting credit mostly on a fully collateralised basis. Unsecured credit limits may be exceptionally granted to

counterparties with strong credit standing where zero risk weight is applied by Regulation (EU) No 575/2013 with specific approval by CEU's Executive Board. The company accepts securities as collateral and applies conservative haircuts (please also refer to [Principle 5](#)). Through the application of sound collateral eligibility criteria, conservative haircut treatment in the valuation of collateral, and active monitoring for credit deterioration (at the individual participant level and on participant group level), CEU maintains and holds sufficient resources to offset both current and potential future exposure.

Credit limits on settlement of securities transactions

Credit limits are granted only to creditworthy participants which are subject to annual credit assessments. CEU grants credit:

- For specific, well-defined purposes (e.g. settlement of securities transactions)
- Only on an intra-day basis
- Within the limits of the participant's credit facilities
- To the extent that there is sufficient collateral available to secure the participant's obligation (unless credit limit is unsecured)

Credit limits are granted within the said scope to individual participants but monitored at an institutional, participant group and country level. Processes are in place to ensure prompt identification, accurate assessment, proper approval, and consistent monitoring and reporting of credit risk.

When granting credit with respect to the facilitation of the settlement of securities transactions, collateral is pledged on participants' accounts opened with CEU. In order to mitigate market and liquidity risk on collateral, a haircut is applied to the calculation of the collateral with respect to the valuation of securities. The purpose of the haircuts is to offset the potential loss of value (including liquidation costs) that may result from adverse price moves over the liquidation period (that is, the period between the default of the counterparty and the actual sale of the collateral). For details, please refer to [Principle 5](#).

Securities prices are automatically collected, on a daily basis, from several recognised external information providers. Where no price is available by eligible information providers or by other market infrastructures (e.g. depositories) the price of a security will be the issue price. Where a price does not list on a stock exchange, acceptance of such security is determined according to the market maker's price. For equity instruments, the issue price is required at the initial setup of the security. CEU will apply additional haircuts to the latest available price if no new price becomes available. For periods beyond two days, a haircut of 100% will be applied.

Haircuts are set taking into account the criteria listed in Articles 13 (3) and 14 (2) of DR 2017/390 such as issuer type, term to maturity, credit risk, the country of issuance, and rating of the underlying assets. Additional measures are applied to mitigate, among others, concentration and correlation ("wrong-way") risks. These measures provide an important cushion against the risk of "contagion" under situations of market stress, which is relevant for CEU given that its clientele is naturally concentrated towards financial institutions.

Placement and repo limits for Treasury operations

CEU invests residual participant cash balances as part of its Treasury activities while maintaining sufficient liquidity to meet payment and settlement obligations. Investments are carried out within the applicable counterparty, maturity, investment and nostro limits.

Available cash is primarily invested through secured reverse repos and FX swaps. Reverse repos may be executed on a bilateral or triparty basis. Remaining cash may be placed with Deutsche Bundesbank (the German central bank) or held overnight with Cash Correspondent Banks, subject to the applicable limits.

Reverse repo transactions are collateralised in accordance with the Treasury Investment Policy. Term transactions are marked to market daily, and margin calls are initiated where required. Eligible collateral may be reused to generate liquidity where necessary.

The Treasury Investment Policy establishes minimum collateral eligibility criteria, including external credit rating, remaining maturity, coupon type, issuer type, minimum issue or programme size, and concentration limits. For CEU, collateral must generally be rated at least AA— by S&P or Fitch, or Aa3 by Moody's. The issue rating is used where available; otherwise, the issuer rating may be applied. Where multiple ratings are available, the lowest rating is decisive.

CEU monitors compliance with the applicable collateral concentration limits, including limits by country of risk and issuer type, as well as collateral composition by external credit rating. These measures support the prudent management of counterparty, collateral and liquidity risks arising from Treasury operations.

Key consideration 4

A CCP should cover its current and potential future exposures to each participant fully with a high degree of confidence using margin and other prefunded financial resources (see [Principle 5](#) on collateral and [Principle 6](#) on margin). 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 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 for 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 for the CCP in extreme but plausible market conditions. In all cases, a CCP should document its supporting rationale for, and should have appropriate governance arrangements relating to, the amount of total financial resources it maintains.

Not applicable to CEU.

Key consideration 5

A CCP should determine the amount and regularly test the sufficiency of its total financial resources available in the event of a default or multiple defaults in extreme but plausible market conditions through rigorous stress testing. A CCP should have clear procedures to report the results of its stress tests to appropriate decision makers at the CCP and to use these results to evaluate the adequacy of and adjust its total financial resources. Stress tests should be performed daily using standard and predetermined parameters and assumptions. On at least a monthly basis, a CCP should perform a comprehensive and thorough analysis of stress testing scenarios, models, and underlying parameters and assumptions used to ensure they are appropriate for determining the CCP's required level of default protection in light of current and evolving market conditions. A CCP should perform this analysis of stress testing more frequently when the products cleared or markets served display high volatility, become less liquid, or when the size or concentration of positions held by a CCP's participants increases significantly. A full validation of a CCP's risk-management model should be performed at least annually.

Not applicable to CEU.

Key consideration 6

In conducting stress testing, a CCP should consider the effect of a wide range of relevant stress scenarios in terms of both defaulters' positions and possible price changes in liquidation periods. 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.

Not applicable to CEU.

Key consideration 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.

The company's Credit Terms and Conditions (CTCs) provide that further to the enforcement of the first-ranking-security interest granted over the assets held in pledged accounts in favour of CEU, the latter shall apply any amount of proceeds of such enforcement to the payment of the borrower secured obligations.

Potentially uncovered credit losses may materialise when, in the event of a liquidation process being triggered, either (i) collateral and other equivalent financial resources (pursuant to Article 15 of DR 2017/390) are insufficient to cover credit exposures or (ii) no collateral is available to cover credit exposures.

Allocation of potentially uncovered credit losses (as per Article 25 (2) (a) of DR 2017/390) follows the procedures as defined in the Clearstream Liquidation Framework: If at the end of the liquidation process, (i) all the collateral of the defaulting participant has been liquidated, and (ii) the outstanding exposure has not been fully covered by the corrective measures, and (iii) there is no other recourse to cover the remaining exposure, then the uncovered exposure will lead to the materialisation of a loss for CEU. There is no mutualisation of the loss with other participants.

Additionally, CEU has a recovery plan to ensure the continuity of its critical functions if its capital, liquidity or operational capacity are adversely affected. As such, should operational or credit losses reach an amount that affects the capital situation of CEU significantly and threatens the continuity of its critical functions, CEU has numerous recovery options at its disposal to restore the capital situation and ensure its going concern, as outlined in [Principle 3, key consideration 4](#).

For details on replenishment of financial resources, please refer to [Principle 7, key consideration 10](#).

Principle 5: Collateral

An FMI that requires collateral to manage its or its participants' credit exposure should accept collateral with low credit, liquidity, and market risks. An FMI should also set and enforce appropriately conservative haircuts and concentration limits.

Key consideration 1

An FMI should generally limit the assets it (routinely) accepts as collateral to those with low credit, liquidity, and market risks.

The general principles under which CEU considers financial assets acceptable for the collateralisation of credit limits are defined in the Clearstream credit strategy and documented in the Clearstream Credit Policy. Both the Policy and the Strategy are reviewed and approved annually by the Executive Board of CEU.

Within the scope of the Credit Policy, "collateral" means any financial security, in any form, that is held by CEU to mitigate credit risk and that would be liquidated or otherwise used in the event of a counterparty defaulting. The term "acceptable collateral" is defined in the Policy as financial securities that fulfil certain common standards, also called "collateral eligibility criteria". These are outlined in the following paragraphs:

- CEU accepts collateral according to the conditions specified in Articles 9, 10 (1) (Tier 1a) and 10 (2) (Tier 1b) of the Commission Delegated Regulation (EU) 2017/390 of 11 November 2016 supplementing Regulation (EU) No 909/2014 (hereinafter "DR 2017/390"). As such, only collateral in the form of debt instruments, transferable securities and money market instruments issued by governments, certain public authorities and issuers with low credit risk (rated BBB– or above), low market and low liquidity risk may qualify subject to specific conditions ensuring that it can be liquidated within one day.
- Other collateral that does not meet the definition of highly liquid collateral with minimal credit and market risk may also be accepted to the extent that CEU has access to routine credit with its central banks that accept such collateral ("highly liquid collateral"). Such securities are only accepted if the criteria stipulated in Article 11 (1) (Tier 2) of DR 2017/390 are met.
- Other types of collateral meeting the requirements stipulated in Article 11 (2) (Tier 3) of DR 2017/390 that are not eligible with the central banks may still be accepted if CEU holds other qualifying liquid resources (QLRs) to cover the time required to liquidate such collateral, which should not be longer than five days.

By applying these collateral eligibility criteria, CEU ensures it does not take any unacceptable credit risk without sufficient collateral in place, nor any unacceptable liquidity risk by ensuring it has access to sufficient QLRs.

Key consideration 2

An FMI should establish prudent valuation practices and develop haircuts that are regularly tested and take into account stressed market conditions.

CEU has a fully automated collateral valuation system in place to set collateral value based on up-to-date market or evaluated prices and based on haircuts which take into account the criteria such as the instrument type, credit risk associated with the financial instrument, issuer type and country of the issuer, the maturity of the asset, its price volatility and liquidity, as well as the denomination currency.

Securities for which only old or no market price data are available are excluded from collateral use.

When collateral is considered eligible at the relevant central bank, CEU applies a central bank floor rule to ensure that the haircuts applied are not lower than the haircuts applied by the central bank to that type of collateral. Stressed market conditions are taken into account using the price volatility risk factor of the collateral valuation system; haircuts are assigned accordingly. Regular haircut back testing is conducted in order to assess the robustness of the collateral haircuts.

CEU's collateral management system appropriately covers its core activities as a custodian and securities settlement system (SSS), all by allowing it to accommodate potential changes in collateral management practices and procedures. For details on the system's functionalities, please refer to [key consideration 6](#).

Securities recorded in CEU's collateral management system are reevaluated on an ongoing basis against the valuation matrix for changes in the value of risk factors, or changes in parameters within the matrix. Any change in the valuation matrix, or in either risk factors or parameters will automatically trigger a recalculation of the haircut applied to the collateral valuation of securities. These collateral valuation and provision processes are embedded in CEU's SSS and do not require any manual intervention.

In order to mitigate the market and liquidity risks on securities used as collateral, CEU applies a haircut in the calculation of the security collateral value (SCV). Generally, haircuts aim at covering the potential loss of value of the collateral security due to adverse price moves over the liquidation period (i.e. the period between the default of the counterparty and the actual sale of the collateral), as well as costs incurred in the liquidation of the asset. Haircuts are expressed as percentage and their amount reflect the characteristics of the security and not the participant's creditworthiness.

Key consideration 3

In order to reduce the need for procyclical adjustments, an FMI should establish stable and conservative haircuts that are calibrated to include periods of stressed market conditions, to the extent practicable and prudent.

In accordance with Article 13 (6) of DR 2017/390, collateral haircuts are calculated in a conservative manner to limit pro-cyclicality as far as possible. The CEU system which calculates the collateral haircut is based on a set of different risk categories thus helping to limit the effects of pro-cyclicality that could potentially arise from a single risk category. In line with Article 13.3 of DR 2017/390, the haircuts are determined taking into account the relevant criteria, including the asset's historical and hypothetical future price volatility in stressed market conditions. In addition, calculation takes into consideration the five-days period as a maximum time for liquidation.

To comply with Article 13 (5) of DR 2017/390, no collateral value is assigned to securities provided by an entity belonging to the same group as the borrower. CEU does not grant collateral value to correlated entities and negates the collateral value from correlated securities.

The annual review of the collateral policies and procedures is another measure to limit the effects of pro-cyclicality. If collateral haircuts are deemed too low as a result of ensuing macro-economic developments, CEU can increase the haircuts if necessary. CEU's internal credit rating, which is also used to rate the collateral issuer, helps to balance any pro-cyclicality that may arise from external rating agencies' ratings.

CEU's policies and procedures on collateral haircut determination take into account the fact that collateral may need to be liquidated under stressed market conditions. In addition, stressed market conditions are considered using the price volatility risk factor.

Key consideration 4

An FMI should avoid concentrated holdings of certain assets where this would significantly impair the ability to liquidate such assets quickly without significant adverse price effects.

A concentration of credit risk refers to a credit exposure with the potential to produce losses large enough to threaten CEU's financial condition. An unduly high concentration of credit risk has the potential to cause material losses which could significantly weaken the company's competitive position in the market and/or lead to a credit ratings downgrade, resulting in a loss of participant confidence. In the course of its credit granting activities, CEU might be indirectly exposed to concentration risks in its collateral pool. This risk may materialise as the potential loss which CEU may suffer during the default management process, due to an insufficient diversification of this pool.

Therefore, CEU actively monitors concentration and correlation risks in its collateral pool. Collateral concentration limits are monitored at both the CEU level and participant (client institutions) level. Collateral concentrations are monitored across multiple concentration criteria and limit types, such as issuer, country, wrong way risk, instrument type, settlement currency, instrument's credit rating, ECB eligibility, liquidity and price volatility.

Participant breaches to any of the said concentration limits are monitored, analyzed and reported on a daily basis. Risk mitigation measures may be taken to remediate a specific breach. Collateral concentration limits and procedures are subject to regular review, at least on an annual basis. More frequent reviews may be conducted in case of deteriorating market conditions or where material changes demand such a review.

Key consideration 5

An FMI that accepts cross-border collateral should mitigate the risks associated with its use and ensure that the collateral can be used in a timely manner.

The legal risks that arise through the use and acceptance of cross-border collateral at CEU relate primarily to conflicts of laws with respect to the creation, perfection, and enforcement of such collateral. The legal framework for the creation, perfection and enforceability of collateral as well as the conflict of law rule is defined under German Law – including but not limited to sections 1204 et seqq. of Bürgerliches Gesetzbuch (BGB, the German Civil Law Code); section 17a of Depotgesetz (DepotG, German Securities Deposit Act) following the implementation of the Financial Collateral Directive 2002/47/EC of 6 June 2002.

The standard TOF and UCF contracts contain rules on the enforcement of pledged securities without any notice according to section 1245 BGB. Thus, collateral can be sold after an event of default has occurred. As per Article 207 (3) of Regulation (EU) No 575/2013, Articles 43 (2) and 38 (13) of DR (EU) 2017/390, CEU has to perform regular assessments covering the financial instruments received by CEU as collateral to ensure the validity and enforceability of CEU's collateral arrangements in certain jurisdictions. As per Article 38 (13) of DR (EU) 2017/390, CEU takes all necessary steps in advance to establish the enforceability of its claim to financial instruments provided as collateral. The majority of CEU's participants are located in Germany; the remainder of the participants are based in another EU Member State. The validity, enforceability and recognition of the pledge governed by German law as set out in number XXXII of CEU's GTCs apply. Furthermore, CEU's collateral arrangements are designed in such a way as to ensure the best possible effectiveness and enforceability of the pledge. For this purpose, the collateral arrangements include, in particular, provisions on the granting of a first-ranking pledge, the agreement that any pledge of collateral under the arrangement shall be governed by German law and that the *lex situs* with respect to the collateral covered by the pledge shall be German law. Also, the pledge remains in full force and effect until full payment and performance of all collateralised obligations of the pledger, and remains binding also on successors and assignees of the pledger (provided that the pledger may not assign or otherwise transfer the rights and obligations under the collateral arrangement without the prior written consent of CEU). Moreover, the pledger is obliged, upon the request of CEU, to produce any documents or certificates, to perform any acts or take any steps that can reasonably be required by CEU in enforcing its pledge in accordance with the terms of the collateral arrangement.

Additionally, the documents mentioned in [Principle 1](#) set out provisions to mitigate above identified risks. According to the GTCs, all securities held by a participant at CEU, for which the participant has notified CEU of its ownership or unrestricted power of disposal pursuant to section 12 (4) or section 13 of DepotG, are pledged in CEU's favour to secure the entire present or future obligations that the participant has, or may subsequently have, towards CEU in consequence of any services provided by CEU to the participant. CEU has the right to debit the participant's cash account with fees, interest and expenses which accrue when CEU acts on behalf of the participant or in its presumed interest. In addition, the CSD is authorised to sell any collateral securities to cover a debit balance without any prior notice.

CEU ensures that cross-border collateral can be used in a timely manner through the following measures:

- Requiring a first-ranking pledge on the securities pledged as collateral, which is deposited in CEU's system
- Adhering to a strict policy of selection of its network of depository institutions, including the performance of regular reviews (see [Principle 16](#) for details)
- Maintaining updated default management and collateral realisation procedures (please refer to [Principle 13](#) for more information)
- Monitoring the concentration of collateral per currency

It is therefore widely accepted that the use and acceptance of cross-border collateral at CEU, whilst subjecting CEU to legal risk, does not carry any additional risk with respect to operational and market risk.

Key consideration 6

An FMI should use a collateral management system that is well-designed and operationally flexible.

CEU's collateral management system (NCMS) is well-designed and equipped with an easy-to-use user interface by the company's IT department which offers full on-site support and maintenance. The collateral management function is sufficiently staffed to ensure maintenance or adaptation of the collateral eligibility parameters even in stressed market conditions. The fully automated collateral management system comprises the following main functionalities:

- Automatic collateral haircut calculation
- Flexible maintenance of haircut parameters
- Reporting functionality allowing for detailed analysis of collateral pool
- Automatic exclusion of correlated collateral
- Maintenance function for classification purposes

The design of CEU's collateral management system allows for flexible maintenance of haircut parameters. Thus, changes in a collateral haircut due to changes in the value of one of the risk parameters are reflected and applied within CEU's settlement system via the Asset Reevaluation Manager (ARM) function. Furthermore, the system provides a flexible collateral percentage override function, for example for negating collateral value from securities that are issued by issuers that are facing financial or legal troubles. This is accompanied by the flexible collateral-tier-override function and flexible query reporting functions.

Principle 6: Margin

A CCP should cover its credit exposures to its participants for all products through an effective margin system that is risk-based and regularly reviewed.

Not applicable to CEU.

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, intra-day 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 consideration 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.

CEU has established a robust framework to manage its liquidity risks evidenced by the following set of internal policies and procedures:

- Investment policy
- Liquidity Management Guideline, Liquidity Contingency Funding Plan (LCFP) and a Qualifying Liquid Resource (QLR) Handbook
- Internal liquidity adequacy assessment process (ILAAP) report and ILAAP Guideline
- Liquidity Risk Policy
- Liquidity Stress Testing Guideline
- Set of operational procedures including an intra-day liquidity controls procedure and other procedures detailing all treasury processes
- Recovery plan including the liquidity options to stabilise CEU's liquidity situation

The above policies are reviewed at least annually, and any material changes are approved by CEU's Executive Board (EB). It is ensured that they are in line with the liquidity risk appetite as defined in Clearstream's risk strategy.

CEU's target for its liquidity management is the ability to manage its varying cash positions to have sufficient liquidity available in all currencies for a timely provision of settlement and payment services as they fall due, and to have in place measures to deal with unexpected disruptions to its cash flows.

Due to the nature of its business, CEU does not have any significant long-term obligations and does not require long-term funding. Thus, CEU's liquidity requirements are mainly intra-day and overnight.

CEU achieves its liquidity management objectives through permanent measurement, monitoring and management of its liquidity requirements and liquid resources. For this purpose, the company has in place a range of ex-ante and ex-post measures addressing liquidity risk, including intra-day liquidity risks, for each currency of the SSS for which CEU acts as settlement agent. Ex-ante measures include permanent liquidity buffers in main currencies, committed and uncommitted secured/unsecured liquidity facilities, real-time monitoring of expected cash flows etc., while ex-post measures include escalation procedures and regular stress testing.

From a normative perspective, CEU is required to maintain its liquidity coverage ratio (LCR) above the 100% regulatory requirement. Early warning indicators including an escalation procedure are in place. The LCR is calculated and monitored daily.

CEU's intra-day objective is to execute payments and settlement as they fall due. To determine the amount of liquid resources required on an ongoing basis in each relevant currency, Clearstream Risk Management runs a wide range of stress scenarios (see [key consideration 9](#) on stress testing). The level of required liquidity shall be the highest liquidity exposure identified in the various scenarios of stress.

Key consideration 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 intra-day liquidity.

To meet its liquidity management objectives set in the Liquidity Management Guideline, CEU has implemented effective operational and analytical tools. All relevant sources of liquidity risk are considered for the measurement, monitoring, and management of CEU's intra-day liquidity management, including its relations to the participants of the SSS and linked FMIs or other entities that may pose liquidity risk to its intra-day liquidity flows.

CEU's Credit department approves credit limits based on the various roles of its counterparts and considers the size of the total exposure on the applicant and all its affiliates. The monitoring process is described in further detail in [Principle 4](#).

The company has defined intra-day liquidity management processes, timelines and thresholds for management escalation in case of non-receipt of funds along with a crisis management system alerting the appropriate level of management depending on the seriousness of incidents.

CEU's Liquidity Contingency Funding Plan states the roles and responsibilities when facing a crisis event where day-to-day liquidity generation measures would not be sufficient to cover a liquidity shortage in one or several currencies. The liquidity issue would be escalated to CEU's EB which can decide in view of the liquidity crisis event to activate exceptional liquidity generation measures.

To monitor its actual cash balances held with its cash correspondent banks and central banks, CEU captures credit and debit advice by its agents and intermediaries and compiles the current actual available intra-day cash balances in all currencies on a near to real-time basis. The same applies to the matching of CEU's expected flows against incoming and outgoing funds.

CEU has specific intra-day operational processes and procedures to identify, measure and monitor intra-day liquidity needs. See [key consideration 1](#) for details.

To meet its intra-day objectives, CEU has in place intra-day funding sources. To determine the amount of liquid resources required on an on-going basis in each relevant currency, CEU runs a wide range of stress scenarios (see [key consideration 9](#) on stress testing), including stress tests implying participant defaults and idiosyncratic and/or market disruption elements.

According to the European Central Securities Depositories Regulation (CSDR), CEU also measures and monitors its own qualifying liquid resources on a currency basis.

Key consideration 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 intra-day 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.

CEU maintains qualifying liquid resources to meet its payment and settlement obligations, including under stressed conditions. These resources comprise cash held at Deutsche Bundesbank (the German central bank), committed multicurrency foreign-exchange (FX) facilities and other eligible liquid resources maintained in accordance with CSDR. Residual participant cash balances are managed separately and are invested or held within the applicable counterparty, maturity, investment and nostro limits.

CEU invests its own resources in accordance with its Treasury Investment Policy, including in eligible high-quality liquid assets. Uninvested own resources may be maintained at Deutsche Bundesbank and kept available as contingent liquidity resources. Eligible securities may also be mobilised to generate liquidity, subject to the applicable operational and regulatory arrangements.

CEU also maintains committed multicurrency FX facilities and regularly tests the operational capacity of the relevant liquidity providers in accordance with its facility-testing framework.

Available cash is managed through secured reverse repos, FX swaps, deposits with Deutsche Bundesbank and, where necessary, overnight balances with Cash Correspondent Banks, subject to the applicable limits. Treasury executes these transactions while preserving sufficient liquidity to meet payment and settlement obligations.

CEU defines a minimum amount of QLR (see [key consideration 5](#)) needed to cover the liquidity impact resulting from a possible default of the two participants and their respective affiliates that would generate the largest aggregate intra-day payment obligation for CEU in extreme but plausible market conditions.

To test the sufficiency of its liquid resources to be used as a source of backstop liquidity, CEU designed a set of liquidity stress scenarios that are in line with the requirements set out in CSDR and MaRisk. Thus, CEU calculates forward-looking liquidity stress tests (including reverse stress tests), considering a number of extreme but plausible stress scenarios. One of those scenarios is the above-mentioned default of the two participants generating the largest aggregate payment obligation for CEU under stressed market conditions (Cover 2 + market stress). The stress tests are calculated for CEU (on single-entity level) and for Clearstream (on group level⁶).

Key consideration 4

A CCP should maintain sufficient liquid resources in all relevant currencies to settle securities-related payments, make required variation margin payments, and meet other payment obligations on time 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 to the CCP in extreme but plausible market conditions. In addition, a CCP that is involved in activities with a more-complex risk profile or that is systemically important in multiple

⁶ The Clearstream group includes the credit institutions Clearstream Europe AG and Clearstream Banking S.A.

jurisdictions should consider maintaining additional liquidity resources sufficient to cover a wider range of potential stress scenarios that should include, but not be limited to, the default of the two participants and their affiliates that would generate the largest aggregate payment obligation to the CCP in extreme but plausible market conditions.

Not applicable to CEU.

Key consideration 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.

CEU's available QLRs are composed of its own funds (cash and securities), central bank facility with Deutsche Bundesbank and a range of committed liquidity facilities with creditworthy financial institutions.

CEU has routine credit access at Deutsche Bundesbank and is able to pledge its ECB-eligible securities from its investment portfolio to generate intra-day liquidity in EUR whenever it would be required.

The minimum amount of CEU's available QLRs shall at any time at least be sufficient to manage the risk to which it would be exposed following the default of at least two participants including its parent undertakings and subsidiaries towards which it has the highest liquidity exposures (Cover 2).

The QLRs mentioned above fulfilling the defined conditions are kept in separate accounts under the direct management of Treasury as CEU's liquidity management function and may only be used as a source of contingent funds during stress periods.

Key consideration 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.

CEU supplements its QLRs with the following additional liquidity resources (non-QLRs):

- Residual cash of CEU participants
- Intra-day credit line at CBL to the size of CEU-pledged collateral at CBL
- Uncommitted and undisclosed overdraft lines with CCBs

All of these additional liquidity sources are immediately available.

Key consideration 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.

CEU performs due diligence on committed facility providers to assess whether they have sufficient information to understand and manage the associated liquidity risks and the operational capacity to perform under their commitments. Each provider completes a Due Diligence Questionnaire covering, among other matters, its regulatory status, financial position, central-bank access, stress-testing arrangements, contingency procedures and understanding of the associated liquidity risk.

CEU assesses whether each provider meets the applicable internal and regulatory requirements, including:

- a sufficiently strong internal credit assessment based on a defined and objective methodology that does not rely exclusively on external credit ratings;
- access, directly or through an entity of the same group, to credit from the central bank issuing the relevant currency;
- settlement arrangements for the relevant currency; and
- sufficient information and operational capacity to understand, manage and perform the liquidity commitment.

The due diligence assessment supports the periodic reassessment of each provider and the decision whether to renew or extend the relevant facility.

CEU regularly tests its procedures for accessing committed liquid resources through liquidity-generation tests. The results are documented and reported through the relevant management process.

Key consideration 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.

CEU maintains accounts with Deutsche Bundesbank and uses the related central-bank payment, settlement and liquidity services, where practical, to support its liquidity-risk management.

Cash held at Deutsche Bundesbank is directly accessible to CEU and can be transferred through TARGET Services. CEU's main cash account supports central-bank operations and is used to fund its other TARGET accounts. Liquidity transfers may be executed through SAP S4P or, where required, directly through TARGET Services, subject to the applicable operational procedures and approval controls.

CEU has access to the Eurosystem standing facilities, subject to the applicable eligibility, collateral and operational requirements:

- the marginal lending facility, which provides overnight central-bank liquidity against eligible collateral; and
- the deposit facility, which enables CEU to place overnight cash with the central bank.

CEU also maintains uninvested own funds forming part of its qualifying liquid resources in a dedicated account at Deutsche Bundesbank under the direct management of the liquidity management function. These funds are segregated from participant funds and are directly accessible for use as contingent liquidity resources during stress periods, following the relevant internal decision.

Key consideration 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.

To determine the amount and regularly test the sufficiency of CEU's liquid resources, Clearstream Risk Management performs a number of forward-looking liquidity stress tests (including reverse stress tests) on a regular basis. These liquidity stress tests are conducted at the level of CEU itself as well as on the superordinate level of Clearstream Holding AG.

Within a dedicated liquidity stress testing framework, Clearstream clearly defines the objectives of conducting the tests, describes the different scenarios to be calculated (including the underlying parameter calibration and assumptions), sets out the relevant management reporting lines, regulates the ongoing and effective review of the stress testing processes, and ensures that a procedure for follow-up actions based on stress test results is in place.

The liquidity stress tests conducted at CEU level have been designed in line with the requirements set out in the CSDR, while taking MaRisk requirements into account. CSDR ensures that systemically important securities infrastructures are subject to common EU rules. It has mandated the European Banking Authority (EBA) to develop regulatory technical standards (RTSs), adopted by the Commission as DR 2017/390, which specify the details of the frameworks and tools for monitoring, measuring and management, reporting and public disclosure of the liquidity risks, including those that occur intra-day. The key requirements for liquidity stress testing are described in Articles 35 (5), 36 (6) and 36 (7) of the DR 2017/390.

CEU's liquidity stress tests consider all entities and products that may pose a material liquidity risk to the company. Moreover, the tests are calculated on relevant currency level where the liquidity exposures are tested against CEU's qualifying liquid resources (QLRs). They cover a multiday period and are tailored to CEU's liquidity risk profile using a wide range of scenarios, considering idiosyncratic and market stress factors as well as combinations thereof. Such stress factors include, among others, the default of the two participants that would generate the largest aggregate payment obligation for CEU (Cover 2), a multiple default event, the temporary inability of a liquidity provider to provide liquidity, a

default of a Treasury counterparty, a general economic slowdown (including shifts in market factors) and a change in the institution's reputation. The stress test results show the potential impact that a stress event might have on the liquid resources in each relevant currency. Exposures towards entities that play multiple roles (for example, both as treasury counterparty and as participant of CEU) are aggregated daily and across all roles to ensure that second-round effects are adequately reflected in the stress simulation.

The results of the different liquidity stress tests are reported to appropriate decision makers within CEU such as the Credit and Financial Risk Committee, and the Executive Board. Based on the results, Risk Management may recommend taking measures concerning CEU's liquid resources.

The stress test assumptions and parameters are reviewed and updated systematically by Clearstream Risk Management at least on an annual basis. Adverse market developments, changes within CEU's business model as well as changes within relevant regulatory requirements can lead to an ad hoc review.

Key consideration 10

An FMI should establish explicit rules and procedures that enable the FMI to effect same-day and, where appropriate, intra-day 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.

Same-day settlement and management of liquidity shortfalls

Given the short-term nature of obligations arising from CEU's settlement activities, its liquidity requirements are predominantly intra-day and overnight.

CEU has established procedures to monitor actual and expected liquidity flows and to identify and address potential liquidity shortfalls, including those arising from individual or combined participant defaults, correspondent-bank outages and market-wide liquidity disruptions. Liquidity positions are monitored by entity, currency and account. Where a potential shortfall is identified, Treasury takes appropriate mitigating actions to support the timely settlement of payment obligations.

CEU may generate same-day liquidity through available cash, nostro transfers, bilateral or triparty repo transactions, committed FX swap facilities and central-bank liquidity arrangements. In a participant-default scenario, CEU may also liquidate the collateral of the defaulting participant in accordance with the Default Management Process.

Where necessary, CEU may apply intraday liquidity-saving measures, including reducing or cancelling applicable credit facilities and prioritising critical payments. These measures are intended to preserve available liquidity, control outflows and minimise disruption to same-day settlement.

Treasury transactions and the related payment and repayment flows are recorded in CEU's trade entry system and monitored through the intraday liquidity management process. Following the applicable validation and release controls, these flows are reflected in CEU's liquidity position.

Replenishment of liquidity resources

CEU's Liquidity Contingency Funding Plan establishes standard and exceptional liquidity-generation measures that may be activated according to the nature and severity of the shortfall in liquidity. The measures are not applied in a fixed order, and their selection takes account of their availability and potential impact on other liquidity sources.

Liquidity resources used during a stress event are monitored together with the related repayment flows. CEU may continue to apply available liquidity-generation and liquidity-saving measures over the duration of the stress event to maintain sufficient liquidity and support the continued operation of its critical functions.

For the specific process governing the replenishment of liquidity resources employed during a stress event, reference should be made to the applicable liquidity contingency and recovery arrangements.

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 intra-day or in real time.

Key consideration 1

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

CEU operates two different securities settlement systems (SSS):

- "CASCADE" for settlement of instructions via the T2S platform, provided by the Eurosystem; and
- "Creation", provided by CEU's sister company CBL.

Through these two SSSs, CEU offers multiple settlement services:

4. T2S settlement against central bank money payment in EUR and DKK (if both parties maintain a T2 Dedicated Cash Account/DCA) for collective safe custody (CSC) and non-collective safe custody T2S-eligible (NCSC-T) securities;
5. Creation settlement against payment in commercial bank money for non-collective safe custody (NCSC; referred to as "6-series" settlement) securities as well as T2S settlement against payment in non-T2S eligible currencies;
6. Free of payment settlement in CASCADE/T2S and Creation; and
7. Settlement in domestic markets outside T2S using selected direct CSD links (as defined in [Principle 1](#)), referred to as "external settlement".

In accordance with Article 39 (2) and (3) of CSDR, CEU's rules for the SSSs used define and disclose the moments of entry, irrevocability and finality of transfer orders in accordance with Articles 3 and 5 of SFD (please also refer to [Principle 1](#)) for each type of transaction settling via CASCADE/T2S, Creation or externally via a CSD link.

Settlement finality is – for both CEU's SSSs – defined in numbers V, XXIV and XXV of [CEU's GTCs](#). Additionally, the rules and procedures are defined in [CEU's Client Handbook](#): Chapter 1.5 "Services for collective safe custody (incl. NCSC-T)", section "Settlement" provides information about the processing of settlement instructions, in particular the rules determining the ability of a participant to revoke or amend its instructions and the moments in time when instructions become irrevocable, binding and unconditional. The GTCs are binding upon all participants and CEU. Both the GTCs and Client Handbook are published on the CEU website.

The term "instruction" is used to refer to a "transfer order" within the meaning of Article 2 (i) of SFD, which is defined as "any instruction by a participant to place at the disposal of a recipient an amount of money by means of a book entry on the accounts of a credit institution, a central bank, a central counterparty or a settlement agent, or any instruction which results in the assumption or discharge of a payment obligation as defined by the rules of the system."

For "external" settlement, CEU uses various links via its sister company CBL to foreign CSDs outside T2S, that is, such securities transactions do not settle within a CEU SSS. Further details about settlement finality is provided in the "External instructions" section below.

CASCADE/T2S: Moments of entry, irrevocability and finality of instructions

A transfer order for payment and delivery transactions, issued to CEU for settlement in T2S is considered as entered into the CEU system when the T2S validation rules applied on the T2S platform are met.

A transfer order is irrevocable, as soon as it is indicated as “*matched*” by T2S. With this binding booking the transfer order will then be processed in T2S (Settlement).

As soon as the transfer orders are irrevocable as described above and with the binding matching in the relevant accounts, the transfer orders will be processed in T2S for settlement to become final.

Any matched instruction that has not been settled or was only unilaterally cancelled will remain in the system for further reprocessing attempts until such instruction is either successfully settled, cancellation requests were received from both counterparties (bilateral cancellation) or when matched transactions are cancelled by T2S (under certain conditions, T2S will automatically cancel matched instructions 60 days after the intended settlement day of the settlement instruction).

Finality is reached when instructions have settled in T2S and the associated re-registering has taken place in the custody ledger (section 14 of DepotG).

The binding booking in T2S is achieved:

- for against payment transactions in a T2S-eligible currency: when the transfer of title of a security in T2S as well as the respective cash payment in T2 have been executed, that is, once the securities are booked in the T2S accounts and the cash is booked on the T2 accounts (DCA) of the CEU participants;
- for against payment transactions in a non-T2S-eligible currency: when the confirmation of cash transfer is received from CBL and when the transfer of title of a security in T2S has been executed;
- for free of payment transactions: when the transfer of title of a security in T2S has been executed.

Final instructions are reported to the participants as settled via the communication means agreed for CEU's settlement services (such as Xact Web Portal or Swift statements).

Creation: Moments of entry, irrevocability and finality of instructions

For settlement in Creation, a transfer order for payment and delivery transactions is considered as entered into the CEU system as soon as the Creation validation rules are met.

The transfer or payment order issued to CEU for settlement is irrevocable as soon as it is indicated as matched by Creation. The transfer order will then be processed in Creation for settlement. Any matched instruction that has not been settled or was only unilaterally cancelled will remain in the system for further reprocessing attempts until such instruction is either successfully settled, cancellation requests were received from both counterparties (bilateral cancellation) or matched transactions are cancelled by CEU (under certain conditions, CEU will automatically cancel matched instructions 60 days after the intended settlement day of the settlement instruction). Please refer to [key consideration 3](#) for details.

Finality of the Creation instructions is reached when those instructions have settled in Creation and the associated re-registering has taken place in the custody ledger (section 14 of DepotG).

The binding booking in Creation is achieved:

- For against payment transactions, when the transfer of a participant's claim against CEU for surrender (“Herausgabeansprüche”) of securities that CEU holds within Creation or on a fiduciary basis with a foreign depository as well as the effected cash payment have been executed, that is,

once a debit entry in the participant's securities account and a corresponding credit entry into the securities account of another participant are posted and the cash is booked via cashless money transmission to the current accounts maintained by the participants with CEU or to respective accounts of third parties authorised by them;

- For free of payment transactions, when the transfer of a participant's claim against CEU for surrender ("Herausgabeansprüche") of securities that CEU holds within Creation or on a fiduciary basis with a foreign depository in Creation has been executed.
- For transactions in a non-T2S-eligible currency, when the transfer of title of a security in T2S has been executed.

The moments of entry, irrevocability and finality of an instruction are reported to the participants via the communication means agreed for CEU's settlement services (such as Xact Web Portal or Swift statements).

Please also refer to chapter 1.5 "Services for collective safe custody (incl. NCSC-T)" of the CEU Client Handbook.

External instructions ("links" settlement) via Creation: Moments of entry, irrevocability and finality of instructions

Transactions settling with a domestic counterparty (in the context of CSD links) are considered by CEU as "external instructions".

For EU/EEA countries, the individual Market Link Guides available in the [Market Coverage](#) section of the Clearstream website provide information about the moments of entry, irrevocability and enforceability and the settlement rules as applicable for each domestic market as well as the rules governing the finality of transfers of securities and cash as defined by each depository or local issuer's SSS (that is, deliveries of securities to or from a domestic counterparty are final depending on the local market regulations and practices).

For the purpose of this section, "depository" shall refer to another CSD, an SSS operated by a CSD (that is, a linked issuer SSS) or to a financial intermediary to which CEU entrusts the safekeeping and administration of securities that CEU holds via its sister company CBL on behalf of the participants. For the avoidance of doubt, the term "depository" shall be understood as the entity with which CEU (via CBL) has its securities account for the deposit of the securities on behalf of its participants.

For domestic markets in which matching is "binding", an instruction can only be cancelled upon bilateral agreement between the parties to the trade. Any specific rules for the cancellation of unsettled transactions with domestic counterparties are published in the respective Market Link Guide.

External instructions that are irrevocable and unconditional in the domestic market – but not yet reported to the CEU participants as settled – are considered as final. Once instructions are final with the depository (or, for the avoidance of doubt, the local issuer SSS) and upon notice of credit/debit of the relevant account of CEU (via CBL) with such depository, CEU will update the participants' accounts accordingly.

Deliveries of securities to or from a domestic counterparty are final depending on local market regulations and practices. Deferral of final settlement applied as per the rules defined in the system of CEU is only experienced in case of deliveries to or from domestic counterparties as finality may depend on local market regulations or practice. For markets where such exception exists, the local market regulations and practices have been published and are accessible to CEU participants.

For links to domestic markets, CEU requests—on an annual basis—legal opinions issued by local external law firms confirming that settlement finality can be achieved in accordance with local laws and regulations, notwithstanding any insolvency procedure. For all such domestic links, CEU ensures that finality is achievable in a way that protects the activity of its participants and guarantees asset protection.

Final instructions are reported to the participants as settled via the communication means agreed for CEU's settlement services (such as Xact Web Portal or Swift statements).

Key consideration 2

An FMI should complete final settlement no later than the end of the value date, and preferably intra-day 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 processing day varies depending on the type of settlement instruction, being it in T2S, Creation or external with a domestic counterparty.

Final settlement on value date

For CASCADE/T2S settlement, T2 RTGS settlement applies.

Settlement on value date or same-day settlement can be completed in case that both counterparties fulfil their settlement obligations for processing on the intended settlement day.

It should be noted that CEU cannot influence the point in time when settlement transactions actually settle as this depends on the instructing participants' cash and/or securities resources as well as their settlement priorities (including putting instructions "on hold" to block settlement on the intended settlement date or after for reasons unknown to CEU).

For further information on the completion of final settlement, please refer to the section "Intra-day or real-time final settlement" further below.

For external settlement local market rules apply. The respective Market Link Guides provide further details on the final settlement on value date.

Intra-day or real-time final settlement

CASCADE/T2S settlement

Instructions transmitted to T2S are processed in different settlement cycles in T2S. For cash and securities settlement, T2S offers a sequential night-time processing (night-time settlement, NTS) with two cycles and up to two real-time processing cycles (real-time settlement, RTS). Cash entries which result from securities settlement or from interest and redemption payments, cross-border market and reverse claims for foreign CSC securities as well as from fees and charges are booked on the Dedicated Cash Accounts (DCA).

Settlement can take place in both NTS and RTS. T2S NTS is the first settlement cycle with final settlement on the next business day.

The settlement timing slots in T2S are according to business days: A new T2S business day starts at approximately 18:45 CET on the same calendar day that the previous T2S business day ends. Settlement in T2S starts with the NTS at approximately 20:00 CET and ends with the real-time settlement at approximately 18:00 CET the following calendar day.

After 16:00 CET, free-of-payment and delivery-versus-payment settlement for specific transactions (labelled by the participants as "BATM", short for bilaterally agreed treasury management) is still possible until 17:40 CET. Cash settlement takes place via participants' T2 DCAs when payments are made in EUR or DKK and through the CEU participants' ICSD-linked (6-series) accounts when payments are made in other currencies.

For further details, please refer to chapter 1.5 “Services for collective safe custody (incl. NCSC-T)” of the CEU Client Handbook.

Creation settlement

The settlement day in Creation consists of one main settlement processing, the real-time processing, followed by the end of day processing as described in chapter 3.4 “The settlement day” of the CBL Client Handbook applicable to the Creation settlement activity of CEU participants.

In order to detect differences or errors in the instructions submitted, matching attempts are applied as soon as the instruction has been submitted to and validated. Details on the matching process are provided in chapter 3.7 “Matching requirements” of the [CBL Client Handbook](#).

External settlement

Individual local market rules apply. Please refer to the respective [Market Link Guides](#) for details.

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.

CASCADE/T2S and Creation internal settlement

Unmatched instructions can be revoked (cancelled) anytime.

Matched internal instructions can only be bilaterally cancelled. Participants cannot cancel them unilaterally even if the requested settlement date has not been reached. If no matching cancellations are received by the requested settlement date and the instruction has not settled by the end of day processing on the requested settlement date, CEU will, in the name and on behalf of the participant, issue a renewed cancellation request for the new instruction for settlement on the next settlement date; such new cancellation request must be matched by the participant’s counterparty on the same settlement date.

In T2S, under certain conditions, T2S will automatically cancel matched instructions 60 days after the intended settlement day of the settlement instruction. In Creation, matched instructions remain valid for settlement until matching cancellations requests are received from both participants (bilateral cancellation) or when they are cancelled by CEU (under certain conditions, CEU will automatically cancel matched instructions 60 days after the intended settlement day of the settlement instruction).

Settled instructions cannot be cancelled.

For further details, please refer to the sections “Processing instructions” and “Settlement failure” in chapters 4.2 “Stock exchange trades (non-CCP stock exchange trades)” and 4.3 “OTC transactions” of the CEU Client Handbook.

External settlement

Individual local market rules apply. Please refer to the respective [Market Link Guides](#) for details.

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 minimise 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.

In line with Article 40 (1) of CSDR, cash payments related to delivery versus payment (DVP) transactions are settled in central bank money (CeBM) where available and practical. This currently applies to:

8. Securities settlement with cash (EUR and DKK) in CEU's securities settlement system (SSS) CASCADE via TARGET2-Securities (T2S) through the CEU's clients Dedicated Cash Accounts (DCAs) of a central bank. Every CEU client securities account is associated with a DCA account;
9. Settlement of Swiss securities versus CHF currency via T2S and SECOM⁷ for CEU's link to Switzerland.

For non-T2S settlement via CEU's SSS Creation, prior to opening a local/domestic market link, Clearstream Network Management assesses the availability and practicability of processing cash settlement in local currency via an account held with the local central bank. Alternatively, settlement in commercial bank money (CoBM) using a cash correspondent bank (CCB) is applied.

To support day-to-day payment activity, CEU relies primarily on:

- a direct access to T2 for payments in T2S-eligible currencies (payments in CeBM) related to the CASCADE settlement transactions;
- a large network of CCBs (payments in CoBM) related to the Creation settlement transactions.

Information about settlement-related cash processing is described within the chapters "Cash and securities accounts per transaction type", "Cash settlement through T2S", "Cash settlement of non-EUR currency", and "Cash settlement through the Swiss National Bank", "Collateral Valuation" of the [CEU Client Handbook](#), as well as the chapters "Settlement services" and "Cash Financing services" of the [CBL Client Handbook](#), published on the Clearstream website.

Cash settlement through T2S

CEU makes use of the T2S platform provided by the Eurosystem for its securities settlement. Cash payments related to DVP transactions are settled in CeBM on the T2S platform through the DCAs of CEU participants who are required to have a DCA linked to their corresponding securities account. The accounting structure (integrated model) gathers cash and securities accounts in the same technical environment. Cash settlements in T2S take place exclusively on DCAs; these cash accounts are opened in the books of a T2S participating central bank and are dedicated to the settlement of the cash leg of

⁷ For settlement of cross-border securities transactions and CCP transactions in Swiss CSC securities there exists a mutual account link (CSD link) between CEU and SIX SIS. Cross-border settlement processes are connected and synchronized on the T2S and SECOM platforms. Cash settlement in CHF is carried out for participants by SIX SIS via the Swiss National Bank (SNB). For this purpose, both parties in a securities transaction (buyer and seller) must maintain a cash account link with the SNB. The CEU participant's SNB cash account is lodged with CEU.

securities transactions initiated by CSD participants and the settlement of liquidity transfers for liquidity management purposes initiated by central bank participants. Each DCA is linked through static data to one or more RTGS accounts of the same currency held in a central bank. For the settlement of cash-related operations in T2S, the provision of liquidity to cash accounts (that is, to the DCAs) is necessary. For this purpose, T2S provides the technical means for its participants (CSDs and central banks) to transfer funds from the RTGS accounts onto the technical platform or from one T2S DCA to another. The holders of the DCAs are responsible for monitoring the balance in their DCA(s) and shall be able to issue liquidity transfer orders in T2S.

The cash settlement of securities transactions and certain corporate actions generally involves the following instruction types:

- Transfer of securities against payment: Delivery versus Payment (DvP), Receive versus Payment (RvP)
- Transfer of securities with payment: Delivery with Payment (DwP), Receive with Payment (RwP)
- Payment without transfer of securities: Payment Free of Delivery Debit (PFoD-DBIT), Payment Free of Delivery Credit (PFoD-CRDT)

These transactions can settle in T2S during night-time settlement (NTS) as well as during real-time settlement (RTS), until 16:00 CET. In both cases, cash is settled directly via a DCA linked to the respective Securities Account (SAC). The DCA can either be stated in the instruction or be set up as a default DCA at CEU.

Participants can either open their own DCA at one of the central banks participating in T2S or make use of a cash correspondent's DCA for which a respective credit line exists. Each connection between a SAC and a DCA which is to be used for cash settlement must be set up as a SAC link by CEU and authorised via a Credit Memorandum Balance (CMB) by the responsible central bank or CCB in advance.

If a transaction cannot settle due to lack of cash or credit line, T2S will reconsider it for settlement in regular intervals during the day. That means that an increase of cash or the credit line on the DCA is considered in a timely manner.

Funding

Participants in settlement of RvP, DwP or PFoD-DBIT instructions in T2S must generally ensure that there is sufficient cash or an appropriate credit line available on the DCA.

Funding of the DCA, to be used for night-time settlement (NTS) of the following T2S business day, takes place on the basis of an individual or standing instruction to CEU until 18:30 CET. The cash forecast function in CASCADE supports participants in determining how much cash needs to be reserved and takes account of the following transactions:

- Matched OTC transactions against payment;
- Stock exchange trades (CCP and non-CCP);
- Eurex® exercises;
- New issues;
- Interest and redemption payments of German government bonds.

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.

When commercial bank money settlement takes place in relation to the Creation activity, the settlement asset used is a claim on CEU itself. CEU is subject to Article 16 of CSDR and holds a limited purpose banking licence, allowing it to provide banking services in relation to settlement services only. For further information about credit and liquidity risk stemming from the use of commercial bank money for settlement in Creation see [Principles 4](#) and [7](#); details on collateral management to mitigate credit risk are given in [Principle 5](#).

With regard to CoBM cash processing on the CEU participants' multi-currency cash accounts (that is, the 6-series accounts), the CEU Client Handbook provides participants with information that is applicable to the SSS Creation (including "Financing" and "Collateral valuation" as stated in [key consideration 1](#)).

Commercial bank money settlement applies to:

1. Non-T2S eligible currencies cash settlement: For cash settlement in currencies that are not T2S-eligible and settlement outside T2S (that is, CEU's international services, "6-series accounts", using Creation), CEU settles cash payments through its own accounts. The 6-series (cash) accounts are opened with CEU and technically held on the Creation platform.
2. Cash settlement for internal, external and Bridge transactions: Creation allows for internal and external (local market) settlement processing, including the processing of transactions via the Bridge with Euroclear Bank. CEU participant accounts are associated with multi-currency cash 6-series accounts for CoBM funding needs in the relevant settlement currencies in the books of CEU. In conjunction with this requirement and in relation to internal settlement in non-EUR currencies and external settlement in all eligible currencies, CEU offers securities settlement solely against payment in CoBM through the respective local CCB, based on the cash funding and provisioning processes of the Creation platform. Cash settlements are effected by crediting and debiting the relevant cash accounts of the CEU participants.

CEU's commercial bank money activity including the respective cash settlement in most currencies other than T2S-eligible currencies is executed through the respective local CCB. For every settlement currency, a CCB (several for Euro) is appointed to handle the external payment and receipt of funds between the domestic banking system for the currency and CEU. All CEU participants have multi-currency cash accounts in the relevant settlement currencies in the books of CEU. Money settlements are affected by crediting and debiting the relevant cash accounts of the participants. CEU operates a DvP Model 1 system, thereby ensuring simultaneous final settlement of securities and cash funds transfers on a gross (transaction by transaction) basis. For all DvP transactions, the cash funds either have to be available on the participant's account or can be made available through CEU's cash financing facilities.

For external settlements in local markets outside T2S via Creation, CEU uses central bank money where feasible. Non-T2S settlement against payment takes place in CoBM (in line with Article 40 (2) of CSDR) in more than 40 currencies eligible for securities settlement for most links.

CoBM settlement adheres to the following principles:

- Cash reporting for CoBM payments is produced exclusively for the 6-series accounts.
- The availability and funding of CoBM on a 6-series account is governed by the descriptions available in the CEU Client Handbook; it is the responsibility of the CEU participant to provide adequate cash liquidity required for settlements against that account.

- For every eligible settlement currency, at least one CCB is appointed to handle external payment and receipt of funds between the domestic banking system for the currency and Creation. Details of the CCBs are provided in the [Cash Timings Matrix](#) published on the Clearstream website. With regard to CSD links, the CCB is published in each Market Link Guide, section “General information”.
- Funds are transferable intra-day depending on the cash deadlines of the respective currencies. Cash deadlines vary in accordance with the time zones of the liquidity providers of the currency. Timings are outlined in the Cash Timings Matrix.

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, capitalisation, 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. CEU settles the cash leg in its own books (see also [key consideration 5](#)).

Key consideration 4

If an FMI conducts money settlement on its own books, it should minimise and strictly control its credit and liquidity risks.

CEU has a limited banking licence that allows it to only offer banking services ancillary to core and non-banking services. All 6-series participants have cash accounts in the available settlement currencies in the books of CEU. CEU performs cash settlement by debiting and crediting the cash accounts of the participants.

CEU has a robust risk management framework that covers all key sources of risk including credit and liquidity risks. Please refer to [Principles 3, 4, 5 and 7](#).

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 intra-day, in order to enable the FMI and its participants to manage credit and liquidity risks.

Not applicable to CEU.

With regard to CASCADE/T2S settlement against payment in T2S-eligible currencies, T2S takes over the entry and the processing, validation, matching and settlement of the transmitted instructions, the administration of positions as well as the reporting of transactions and positions for the T2S securities accounts (SACs). Thereby, the settlement, that is, the exchange of securities and cash, takes place directly on the T2S platform. The cash leg of DvP settlement settles on the associated DCAs.

For the CEU-SIX SIS link, both parties in a securities transaction (buyer and seller) maintain a cash account link with the SNB. The CEU participant’s SNB cash account is lodged with CEU.

With regard to Creation, CEU settles the cash leg in its own books.

Principle 10: Physical deliveries

An FMI should clearly state its obligations with respect to the delivery of physical instruments or commodities and should identify, monitor, and manage the risks associated with such physical deliveries.

Key consideration 1

An FMI's rules should clearly state its obligations with respect to the delivery of physical instruments or commodities.

CEU's obligations and responsibilities with respect to the immobilisation and delivery of physical instruments or commodities are prescribed by German law.

As CSD subject to German law and CSDR, CEU's obligation is mainly to receive physical deliveries for immobilisation purposes in order to represent such securities as book entries. Circulation of the securities in CEU's systems is performed exclusively in book-entry format in accordance with Article 3 of CSDR.

The procedures relating to the delivery of each of the eligible classes of securities, as well as the instruction requirements and procedure for effecting physical delivery are set out in the [GTCs](#), the [Client Handbook](#) and other publications, for example, regular client announcements on the [Clearstream website](#).

The rules of the Depotgesetz (DepotG, German Securities Deposit Act) regarding the deposit are applicable to CEU.

According to the company's General Terms and Conditions (GTCs), the following securities are accepted for physical delivery into custody with CEU:

- Securities in bearer or registered form issued by German issuers and governed by German law
- Securities in bearer or registered form issued by foreign issuers and not governed by German law

For physical delivery, CEU only accepts securities in collective safe custody which are transferable and fungible in accordance with sections 1 (1) and 5 (1) of the DepotG and number XI of the GTCs.

For physical deliveries of commodities, CEU relies on bilateral agreements with issuers or agents.

With regard to individual safe custody (also referred to as jacket custody), which is regulated in section 2 of the DepotG, the custodian or, in the case of custody with a third party, CEU, must segregate the securities to be kept in safe custody from other securities holdings it keeps in safe custody (separated from its own and third persons' holdings), on the depositor's express request. In this case, CEU will hold the client's securities, bearing its identification in externally visible manner. This identification often takes place in the form of a "jacket" marked with the depositor's name. This separation preserves the depositor's sole ownership of the physical securities certificate in question and when the certificate is deposited, this ownership is not transformed into fractional co-ownership of the collective holding.

In order to facilitate participants' understanding of their obligations and procedures for effecting physical deliveries, if any, CEU maintains, in addition to the information publicly disclosed in the said governing documents, an active relationship with its participants; please refer to [Principle 23](#) for details.

Key consideration 2

An FMI should identify, monitor, and manage the risks and costs associated with the storage and delivery of physical instruments or commodities.

Risks associated with the storage and delivery of physical instruments or commodities

The main risks associated with the immobilisation, storage and delivery of physical instruments are:

- Loss of certificates during the process
- Receipt of fraudulent certificates
- Fire in Vault

CEU has implemented defined processes, procedures and controls to monitor and minimise the risks associated with the handling (storage and delivery) and the immobilisation of physical instruments or commodities.

These processes, procedures and controls comprise an operational risk scenario analysis that is updated on a regular basis. The scenarios take into account different risk categories, such as “fraudulent destruction”, “theft”, “transportation issues”, “loss”, “betrayal” or “attacks”. In addition, root causes with a validated percentage of possible issues in the different categories are established. Offenders, different types of a possible crime, possible loss or damage have been taken into account, based upon statistics of the Bundeskriminalamt (BKA, Federal Criminal Police Office), rounded out by own internal data, if applicable.

The receipt of fraudulent certificates is avoided by undertaking in-depth validation checks upon receipt, including signature checks of transfer documents and validation checks of certificates in accordance with market practice.

In addition, vault reconciliation to avoid loss of certificates, is performed by CEU, including the following:

1. Daily controls of physical security deliveries and receipts together with the corresponding orders on the CASCADE settlement platform to ensure safe receipt and proper recording of deliveries
2. Daily reconciliation of positions booked in CASCADE following the settlement of securities instructions versus holdings in Vaults Management application
3. Inventory controls to ensure that all securities deposited with CEU and recorded in the Vaults Management application are also physically deposited in the vaults. This includes a predominantly digital reconciliation process of Global Notes encompassing an electronic annual completeness check of sealed inventory and a more detailed spot-check control on a pre-defined amount of the physical inventory.

Costs associated with the storage and delivery of physical instruments or commodities

The costs associated with the immobilisation, storage and delivery of physical instruments or commodities typically include postal costs, insurance costs, physical handling and re-registration fees, as well as custody fees.

Principle 11: Central securities depositories

A CSD should have appropriate rules and procedures to help ensure the integrity of securities issues and minimise and manage the risks associated with the safekeeping and transfer of securities. A CSD should maintain securities in an immobilised 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 unauthorised creation or deletion of securities, and conduct periodic and at least daily reconciliation of securities issues it maintains.

According to the requirements set forth by Articles 26, 37 and 38 of CSDR, CEU has implemented rules, procedures and controls to safeguard the rights of the securities issuers and holders as well as the integrity of issues by preventing the unauthorised creation or deletion of securities (UCoD). These rules are described in CEU's CSDR authorisation file and are designed to comply with CSDR and the German law framework as described in [Principle 1, key consideration 1](#).

Safeguarding the rights of securities issuers and holders

Concerning the protection of the rights of the securities holders, CEU offers the possibility to its participants to choose between a segregated account structure or an omnibus account within the CEU system. Further details are described in [key consideration 5](#).

Please note that CEU as a CSD with registered seat in Frankfurt/Main, Germany, maintains accounts which are indeed opened in the participant's name. A sub-account structure permits to open clearly identifiable accounts to segregate participants' and underlying clients' assets. In the local markets linked to CEU, participant assets are held in an omnibus account in CEU's name. This account however is segregated from the proprietary assets of the local CSD and other CSD participant's assets. CEU does not hold "own" assets in local markets.

CEU does not use, for any purpose, securities that are not proprietary to it. CEU may however use securities of a participant where it has obtained that participant's prior express consent. CEU requires its participants to obtain any necessary prior consent from their clients. This corresponds to the legal requirements of Article 38 (7) of CSDR. For more information regarding the usage of securities and the rules for obtaining written consent may be seen in CEU's [GTCs](#).

Securities can be held in custody with CEU under any the following main structures:

- **Girosammelverwahrung (collective safe custody, CSC):** CSC is governed by the Depotgesetz (DepotG, German Securities Deposit Act). Currently, CEU is the only national CSD for the German market providing a CSC holding structure. Under German law, holders of securities held in CSC are granted a proprietary right to those securities (a "right in rem") being a pro rata co-ownership right in a fungible pool of securities represented by a global note or a similar number of definite securities held by CEU in its vaults in accordance with section 5 (1) DepotG. Furthermore, there are certain types of securities which can be represented in a dematerialised form via an entry in a central register (electronic securities in accordance with the eWpG) as well as Bundesanleihen (German federal government bonds) and Länderanleihen (German state bonds, that is, bonds issued by the German federal states) held by entry in the respective debt registers of the Federal

Republic or State. Equivalent rights are granted under German law for such securities which CEU holds via a cross-border CSD link with a foreign CSD based on an account relationship in accordance with section 5 (4) DepotG.

The process of admission of securities to CSC by CEU is initiated by the applicant, the issuer (or the issuing bank, that is, the lead manager acting on the issuer's behalf), which submits the request for admission to CEU. The applicant must be a credit institution and a participant of CEU. The admission and depositing of securities in CSC are described in CEU's GTCs.

CEU books a CSC balance (GS-Gutschrift) for its participants. This system enables the transfer of rights inherent to the securities by book entry. This is known as a securities transfer by book entry. The co-ownership of securities held in CSC is transferred in accordance with the principles of property law, that is, by agreement in rem and transfer. Depositories, as CEU's participants and (intermediate) custodians, as well as CEU as a CSD only provide the depositor (third-party) possession of the securities kept in custody, as required by civil law. As custodians, they are not the owners of these securities, neither in the sense of a trustee nor in the sense of a beneficial owner. When a transfer of co-ownership fractions takes place, constructive possession must move from the depositor who sells them to the depositor who buys them or to his depositories, on all levels of the custody chain. Under section 4 (1) DepotG, CEU is deemed to have explicit notice of third-party ownership of the securities that a depository, as an intermediate custodian, keeps in custody with CEU. This means that CEU is attributed with the knowledge that the securities which the depository has delivered into safe custody do not belong to the depository. This applies as long as the depository does not give CEU explicit notice that certain securities are its own positions. The particular consequence of this constructive notice of third-party ownership is that these securities owned by third parties enjoy full protection in the event of debt enforcement measures and similar acts against the depository or CEU.

- **Streifbandverwahrung (individual safe custody):** Jacket custody of fungible and non-fungible certificates, where each participant is entitled to have the individual certificates with a particular serial number at his disposal. In the case of individual safe custody (also referred to as jacket custody), which is also regulated under the DepotG, the custodian or, in the case of custody with a third party, CEU, must segregate the securities to be kept in safe custody from other securities holdings it keeps in safe custody, on the depositor's express request. The depositor in question must be identified on the outside. This identification often takes place in the form of a "jacket" marked with the depositor's name. This separation preserves the depositor's sole ownership of the physical securities certificate in question and when the certificate is deposited this ownership is not transformed into fractional co-ownership of the collective holding.
- **Wertpapierrechnung (non-collective safe custody, NCSC):** NCSC applies to fungible securities kept abroad and are not settled via the TARGET2-Securities (T2S) platform. The depository bank where the account is kept becomes the legal owner (acting as trustee) of the rights granted to it under the legal system or market practice of the country of custody. The investor, as the account holder and beneficial owner, merely has a bilateral claim against its depository for the surrender of this legal title under the law of obligations, along with the rights of a beneficial owner to issue instructions to the trustee. CEU acts as the depository (intermediary) and keeps the positions in the form of book-entry credits on a fiduciary basis, using the technical and functional infrastructure of its sister company Clearstream Banking S.A., Luxembourg, which uses custodians in various countries for custody purposes. Depositories are under an obligation to obtain what is known as a "Three-Point Declaration" from the (first) custodian outside Germany. The requirements of the "Three-Point Declaration" are explained in detail under [key consideration 4](#). It is the predominant opinion that in the event of insolvency on the part of CEU or the depository, the intermediate custodian's or the beneficial owner's rights to the surrender of these securities are eligible for separation from the debtor's assets.
- **Lagerstellenverwahrung (vaults services for third parties):** for example, insourcing of depository function from custodian banks.

For certain registered shares, CEU offers a “CASCADE registered shares service” allowing participants to either register the shares under their nominee account name or in the name of the final beneficial owner.

If the collective holding is decreased due to a loss which CEU is not responsible for, the company will apportion such loss on a pro rata basis to the participants according to the fraction each participant holds (for its underlying clients) in this collective holding at the moment that the loss occurred. CEU's liability pursuant to section 7 (2) sentence 2 DepotG and as established in the GTCs (“Liability”), shall remain unaffected.

If CEU were to become insolvent, participants' securities would not fall in the bankruptcy estate of CEU. Pursuant to section 47 of the Insolvenzordnung (InsO, German Insolvency Code), participants would be entitled to a right of segregation. If said securities are not sufficient to ensure the full restitution of the securities maintained in the account, they will be allocated between the account holders in proportion to their rights. If CEU is responsible for the loss of securities, such a participant would have a senior claim in an insolvency proceeding, according to section 32 DepotG.

Safeguarding the integrity of issues by preventing UCoD and daily reconciliation

To safeguard the integrity of issues by preventing UCoD and protecting the right of both securities holders and issuers, CEU as CSD, applies the requirements set out in Article 37 of CSDR. The company has implemented rules, procedures and controls to hold, on its own books or with another (foreign) CSD, securities that are, in number and description, equal to the number and description of the securities credited on the securities accounts it maintains for its account holders.

CEU has in place operational measures, internally and with linked CSDs, to properly safeguard, record, reconcile and report the assets deposited with it, and notify the relevant stakeholders when required. The reconciliation duties are set forth in number XIII of the GTCs which provides for the following obligations:

- Obligation for CEU to report the positions to participants on a daily basis by providing them statements of accounts as specified in its governing documents. For further details, see number XIII (2) of the GTCs.
- Obligation for participants to reconcile the said statements with their own books. Participants are solely responsible for their internal reconciliation processes.
- Obligation for participants to report back to CEU immediately any inconsistencies in any of the said statements or related information to ease any remedial actions.

Prevention of the unauthorised creation or deletion of securities

CEU has implemented rules, procedures and controls to prevent UCoD of securities:

- Authorised creation of securities positions in the CEU system is only performed upon receipt of securities to be credited to participant accounts either through a new issue distribution (issuing agent) or the settlement of a corporate action.
- Authorised removal of securities positions is generally performed upon final maturity or in the context of a corporate event.

Integrated securities provisions checks are exercised before release of a settlement instruction.

Daily reconciliations are performed to ensure the correct application of the rules to prevent UCoD of securities. The various reconciliation measures as well as the handling of differences are detailed below in the "[Periodic reconciliation of securities issues](#)" and "[Reconciliation frequency](#)" sections of this key consideration.

Periodic reconciliation of securities issues

The internal and external reconciliation procedures and controls ensure on a daily basis that rules are adhered to.

As required by Article 37 (1) of CSDR, appropriate reconciliation measures are performed automatically within CEU's systems to verify that the number of securities making up a securities issue or part of a securities issue submitted to CEU is equal to the sum of securities recorded on the securities accounts of the CEU participants of the SSS, and on owner accounts maintained by CEU. Such reconciliation measures are conducted daily. As required by Article 59.1 of RTS 2017/392, CEU ensures that these measures are performed for each securities issue recorded in all securities accounts maintained by CEU (centrally and not centrally).

The validation of securities positions covers the following key processes:

- Validation of the number of securities making up a securities issue or part of a securities issue submitted to CEU versus the total position recorded on the securities accounts of its participants and validation against a negative securities balance (that means that no negative securities balance exists on a participant account)
- Comparison of the previous end-of-day balance with all settlements processed during that day and the current end-of-day balance on CEU's books
- Usage of double-entry accounting

Automated alerts are generated when a mismatch or divergence from established rules is detected.

For settlement activities using the Eurosystem's T2S platform, the validation measures are supported through the operative processes of this platform.

Reconciliation frequency

CEU performs daily internal securities reconciliation processes that it maintains centrally. It involves those functional and non-functional processes performed on CEU's books or in its systems, respectively, ensuring the integrity of a security issue (as explained in the "[Periodic reconciliation of securities issues](#)" section of this key consideration).

CEU also maintains daily securities reconciliation processes with various external parties as required by Article 37 (2) of CSDR. The main purpose of the reconciliation is to ensure the integrity of the issue and minimise operational risk related to open differences in the respective holdings. For investment funds, the daily frequency refers to the frequency of the net asset value (NAV) calculation.

A daily reconciliation of the total holding per security issue is performed automatically by CEU's systems. Validations are performed in accordance with whether settlement data is received from T2S or Creation. The automated checks are performed at minimum once per day. Upon detection of a difference, the securities reconciliation team starts an investigation to either reconcile the item or find the root cause of the reconciliation break, and allocate it to the correct internal operational unit or to the relevant external party for investigation and correction.

In addition, daily reconciliation is performed for the following securities positions:

- Securities held or mirrored at external parties, for example, registrars or CSDs
- Securities held in CSC with the CSDs to which CEU maintains custody network links (investor-CSDs)
- Securities held in NCSC (reconciliation with CBL and its sub-custodians)

Every issuer/registrar of CASCADE-RS-eligible registered securities is provided with the overall reconciliation record by CEU on a daily basis.

Furthermore, CEU has established a reconciliation process with issuer agents as there is no contractual relationship, neither with the issuers of securities in registered form, nor with the entities maintaining the issuers' register. Hence, every day, CEU provides the issuer agents with a reconciliation file containing the total issue outstanding amount (IOA) for the securities requested for admission by the relevant issuer agents as recorded in the books of CEU. Since CEU has no relationship with fund managers or transfer agents, but with the issuer agents, and receives mark-ups and mark-downs directly from them, the daily reconciliation of the IOA issued via CEU is conducted with the issuer agent.

The issuer agent must reconcile the daily report with the information filed in the ownership register of the registrar and with the records of the transfer agent or the entity acting in this capacity. Any identified mismatch or discrepancy must be reported to CEU within the business day following the reception of the report. In addition, the issuer agent must provide all information necessary to enable CEU to ensure the integrity of the issue.

CEU performs the following control and reconciliation processes on physical inventory to ensure duly safekeeping and proper handling of physical securities:

- Daily controls of physical security deliveries and receipts together with the corresponding order in the CASCADE settlement platform, to ensure safe receipt and proper system recording of deliveries
- Daily reconciliation of positions booked in CASCADE following settlement of securities instructions versus holdings in the Vaults Management application
- Inventory controls ensuring that all securities deposited with CEU and recorded in the Vaults Management application, are also physically deposited in the vaults. This includes a predominantly digital reconciliation process of global notes encompassing an electronic annual completeness check of sealed inventory and a more detailed spot-check control on a pre-defined amount of the physical inventory.

The control processes are in scope of the annual audit performed by CEU's Internal Audit function and the external auditors, as well as on the field work (during on-site evaluation), samples of evidence are assessed for adequacy of controls and adherence to procedures.

Each remaining difference following reconciliation tasks is reported as open until it is fully resolved, that means, corrective actions have been taken, or missing movements have been booked. Once these movements have been reported or transmitted to the reconciliation application, open breaks can be reconciled and the open items authorised and closed. This is documented in CEU's internal reconciliation procedure.

According to CSDR reconciliation requirements, any reconciliation break is immediately investigated by CEU's reconciliation team and the impacted business unit(s). Both will perform all necessary measures to remedy the break without undue delay: the reconciliation team investigates the differences and may identify missing movements to solve them. However, the corrective action itself can only be confirmed as correct and be booked by the impacted CEU business unit or external party.

Where the reconciliation break reveals a UCoD, and CEU fails to solve this reconciliation break by the end of the following business day, CEU will suspend the affected securities issue from settlement until the UCoD of securities is resolved. In such cases, CEU will inform internal and external stakeholders without undue delay of the fact that settlement in the relevant securities issue is suspended. Internal and external stakeholders will also be informed without undue delay when the UCoD of securities is resolved, and settlement in the affected securities issue is resumed.

As stated in CEU's governing documents, the company makes daily statements of holdings and transactions available to participants that they have to subscribe to in line with number XIII Reconciliation of securities accounts and registers of the CEU GTCs.

The robustness of the system and the daily reconciliation processes are reviewed also by internal and external auditors on an annual basis.

Key consideration 2

A CSD should prohibit overdrafts and debit balances in securities accounts.

CSDs that have outsourced their settlement activity to T2S have no measures at hand that could prevent negative securities positions as CSDs rely on T2S provision checks and settlement rules. The CSD reflects the T2S settlement results. Negative balances might be accepted if and on accounts that operate as mirror accounts. In these cases, these accounts as well as their counterparty accounts must be included in the reconciliation process.

If the structure of an account does not allow negative securities balances, the settlement platforms also perform a "provision check" before executing a participant instruction, thereby ensuring that sufficient securities are available on the participant account to execute the delivery and preventing a debit balance. This ensures that no negative securities balances can result from the settlement process, even on an intra-day basis.

As per Article 37 (3) of CSDR, no negative securities balances are allowed on participant accounts maintained by a CSD. There is no specific article that covers the securities reconciliation of internal accounts. However, this reconciliation type is an additional check to avoid any mismatch or inconsistency that could lead to the UCoD of securities.

Key consideration 3

A CSD should maintain securities in an immobilised or dematerialised form for their transfer by book entry. Where appropriate, a CSD should provide incentives to immobilise or dematerialise securities.

The majority of today's issues (roughly 99%) is done in immobilised form. The process for admission of securities to CSC by CEU is initiated by the applicant, either the issuing bank (lead manager) or the issuer itself, that submits the request for admission together with the certificate(s) and various accompanying documents to CEU. To simplify and shorten the admission process for certificates, warrants, certain types of bearer bonds, as well as for shares and funds, CEU offers its participants the eMission service. Issuers and issuing banks (lead managers) can use an internet portal to submit to CEU the terms and conditions of issue and the basic data for new issues of securities certificates etc. In addition to government bonds, where dematerialised issuance has been possible for a long time, the dematerialised issuance became compliant with the DepotG. This was enabled through the Gesetz über elektronische Wertpapiere (eWpG, German Electronic Securities Act), which entered into force on June 10, 2021. Issuers are now able to issue securities electronically in dematerialised form. CEU is offering the D7® platform for dematerialised issuance of warrants, certificates and certain types of bonds. The eligible asset classes on this platform will be broadened. In the first years, CEU put a fee holiday for the issuance process in place to incentivise the dematerialised issuance of such securities.

Key consideration 4

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

CEU obtains (and subsequently updates as per CSDR requirements) third party legal opinions in respect of the legal protection afforded to the securities deposited with CSDs/sub-custodians in each market pursuant to local laws (in particular insolvency protection). Therefore, when appointing a CSD/sub-custodian, CEU reviews the custody risks associated with the decision to entrust the securities to the sub-custodian.

CEU assesses and reviews the custody risks associated with the decision to entrust the securities to the CSD/sub-custodian on a regular basis.

The essential points of the legal opinions are published in the "Legal arrangements" section of the Market Link Guides on the Clearstream website.

CSDs/sub-custodians are requested to provide a Three-Point Declaration in which the non-German custodian confirms the following:

- The securities positions delivered into safe custody by the depository are kept as participant positions of the depository.
- As a matter of principle, it will not assert any rights of lien or rights of retention in relation to these securities.
- Custody of the securities positions underlying the Three-Point Declaration will not be outsourced to a third party without the consent of CEU.

The Three-Point Declarations are published in the [Regulation](#) section of the Clearstream website.

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.

In order for the safe custody and settlement of securities transactions to be carried out by CEU, participants can maintain a collective account at CEU, in which the securities holdings of multiple underlying clients of the participant are booked. This level of segregation corresponds to the omnibus client segregated account (OCS) as set out in Article 38 (3) of CSDR. Alternatively, the participant may choose to set up separate deposit accounts at CEU to segregate the securities of its individual clients from the holdings of the participant and of its other clients. This level of segregation corresponds to the individual client segregated account (ICS) as set out in Article 38 (4) of CSDR. For either account type (ICS or OCS), CEU books the securities and any other fungible financial instruments received as a deposit or held in an account, separately from its own proprietary positions and off balance sheet (that is, independently of ICS or OCS).

Under German law, Section 2 DepotG provides for a separate safe custody of securities in the case of individual safe custody. Additionally, according to Section 4 (1) DepotG, participant accounts held by CEU are managed as a third-party deposit.

Please refer to CEU's [CSDR Article 38 disclosure document](#) for further details.

Participant assets are held in an omnibus account in CEU's name with the local CSD and are therefore segregated from the proprietary assets of the local CSD. CEU does not hold its own assets at the CSD level in the local market.

For assets held in NCSC via 6-series accounts on the Creation platform of CEU's sister company Clearstream Banking S.A. (CBL), a different operating model applies. In this context, CEU uses accounts directly at the CSD or indirectly via a custodian. At the CSD/custodian, CEU holds an account for its proprietary assets and an omnibus account for its participant assets.

This structure simplifies the recovery of assets for participants should CEU become insolvent. CEU participants' assets deposited with CEU are governed and protected by the provisions of the DepotG and the InsO.

As described above and in [Principle 1](#), participants depositing securities in collective safe custody with CEU benefit from a right in rem. They are co-owners in the pool of securities deposited at CEU up to the number of securities held on its securities account. Clients depositing securities in non-collective safe custody with CEU receive a pro rata claim for delivery in relation to the asset pool for the respective securities' class in the custodian's country. Under German law, in the event of bankruptcy of CEU, the company's participants would be entitled to claim their assets or equivalent assets deposited with CEU in accordance with Section 47 InsO as they have a right to segregate the securities.

The right of segregation would apply, irrespective of whether securities are booked in ICS or OCS, so that both segregation types provide a similar level of protection in the case of insolvency of CEU.

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.

Besides central safekeeping and administration of securities and settlement, CEU offers a variety of services for financial institutions across selected markets and financial instruments. The company identifies, measures, monitors and manages the risks from these activities. The following sections present information complementing the propositions provided in [Principles 3, 4, 7, 15, 16](#) and [17](#).

CEU performs cash management and FX services, as well as financing services. Comprehensive custody management includes, for example, withholding tax and general shareholder meeting services. In addition, CEU offers related information distribution including participant reporting and a comprehensive new issues service.

Credit and liquidity risks arising from CEU's additional services

Any risk deriving from credit and liquidity activities is addressed in [Principles 3, 4](#) and [7](#).

CEU considers corporate actions (including general meetings) as central safekeeping and administrative functions.

Credit and liquidity risks arising from collateral management agency services mainly relate to derived asset servicing and settlement activities; they do not differ from the risks set out in [Principles 4, 5](#) and [7](#).

For securities lending services, a dedicated legal framework is set up for and with each individual participant in addition to the provisions of CEU's GTCs.

CEU offers several foreign exchange (FX) services to its participants for the 6-series account activities, such as automatic FX services for custody proceeds, interest charges and standard monthly fees, as well as an FX service for securities settlement instructions and the case-by-case FX service.

All of CEU's additional services are delivered in accordance with the company's key risk and credit principles. A permanent monitoring process is in place to identify large participant positions which may lead to unwanted nostro balances. Also, regular daily reconciliation of cash balances and a contractual framework are in place with each of the two CCBs.

Operational risk arising from CEU's additional services

The creation of new products or services is triggered in different manners: through CEU's participants, the company's reply to market or regulatory changes or through CEU's management initiatives.

CEU has put in place a wide range of IT tools, controls and procedures to minimise the impact of sources of risks related to new or existing (enhanced) products and services to ensure the integrity of securities issues, minimise and manage the risks associated with the safekeeping and transfer of securities. Thus, IT tools support the monitoring and reduction of operational risk and ensure that CEU's technical environment remains stable (for example, by ensuring the monitoring of the infrastructure).

With regard to operational risk, CEU in particular uses IT tools and processes to manage and monitor its settlement systems. The governance and control environment includes but is not limited to IT controls: it covers, for instance, cybersecurity measures, local and physical access management, stress testing, risk quantification based on a Value-at-Risk (VaR) concept, BCM or project management processes, such as the 4-eyes principle. Key controls are detailed and documented in the "Mitigation actions and controls" section of CEU operational risk scenarios which lists information on controls and procedures (which may

also be supported by IT tools). The other control types are further detailed in internal policies and procedures used by CEU to minimise the impact of sources of operational risk.

CEU's Material Change Process (MCP)

As a general control mechanism, for material changes⁸, new business activities and strategic initiatives, Deutsche Börse Group has implemented a Material Change Process (MCP) governance framework. This framework defines rules, roles, processes and responsibilities applicable to all staff and management, as well as the principles to be applied when assessing any material change activity before, during and after their implementation (including intended updates or implementation of new business activities and services).

Within the MCP framework, a Material Change Committee (MCC) has been set up in addition to the Clearstream Risk Committee (CRC) that is chaired by an independent chairperson. The MCC is designed to ensure consistency in material change risk assessment reviews, approval processes, completeness of risk impact analysis and adequacy of risk-based measures to manage dependencies and potential risk implications of respective material changes (in accordance with the defined workflow requirements). The MCC has veto right of non-recommendation of a proposed material change by way of their advisory opinions provided for the MCC reviews.

Furthermore, the MCC assessment ensures that key factors for relevant risk types are taken into consideration, and potential capital impact is assessed. It is essential for CEU to identify those risks and modify or structure the product in such a way as to mitigate the risks in the best possible manner. Material changes including all new business activities are assessed by the MCC or CRC. The outcome of the risk management assessments shall be reported to the CRC and CEU's Executive Board by the chairperson of the CRC.

Within the MCP framework, various stakeholders are involved both at Deutsche Börse Group and legal-entity level based on a "three lines of defence" strategy. The heads of departments and sections (business owners) are responsible for informing the MCC of any plan to introduce a change activity considered a "material change". In the event that the MCC does not recommend a proposed new business activity, this may nonetheless be proposed to the relevant governing board or committee explicitly stating the conclusions of the MCC.

There are a number of interconnected risks involved in the launch of a new product. Accordingly, it is essential for Clearstream to identify those risks and modify or structure its products in such a way as to mitigate the risks in the best possible manner. Clearstream Risk Management performed 130 risk assessments and recommendations for the year 2025, of which 14 were initiated by CEU. Material changes are tracked in a centralised inventory also comprising the full list of Clearstream products and services. This inventory is periodically reviewed to ensure appropriate governance during the lifecycle of the respective products and services.

In accordance with the MCP workflow requirements, the material assessment review will be performed by the business owner responsible for CEU in collaboration with other relevant stakeholders, notably the company's Risk Management, Compliance, Information Security, Data Protection and Legal functions. The assessment review is divided in three phases: initiation, pre-launch and post-launch. "MCC review & recommendation" quality gates (QG) are used to verify that a set of required activities is performed to ensure a sound and reliable analysis of the intended material change to allow for a fact-based decision making by the Executive Board. Following the review performed by the MCC, a recommendation will be provided to CEU's Executive Board (MCC review documentation and minutes are stored in a centralised inventory for reference).

⁸ A change activity is classified as "material" where it has the potential to directly or indirectly affect the business and risk profile of one or more of the regulated Clearstream entities. In these regards, the MCP outlines a set of categories that exemplify prominent examples (not exhaustive) of activities included in scope of "material change", in particular those that have an impact on the governance, business products and processes relevant for Clearstream.

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.

CEU settles transactions that involve the settlement of two linked obligations being the delivery of securities against the payment of cash (delivery versus payment, “DvP Model 1”). Principal risk is avoided through the irrevocable, unconditional and simultaneous exchange of the securities (the delivery) and the cash value (the payment) to settle a delivery versus payment transaction. This aspect is covered by the following:

- (i) The legal framework applicable to CEU’s services and settlement activities as defined in [Principle 1](#);
- (ii) With regard to settlement via CASCADE/T2S, the [CEU Client Handbook](#) (chapter 4 “Settlement Services”) sets out the settlement mechanisms and rules applicable to and binding upon CEU and its participants in order to address the principal risk in the system.
- (iii) With regard to settlement via the Creation SSS, the information is to be found in the [CBL Client Handbook](#) (chapter 3 “Settlement Services”).
- (iv) From a technical perspective, CEU’s two SSSs CASCADE (used for settlement that is outsourced to the T2S platform provided by the Eurosystem for securities settlement of T2S-eligible instruments free of or versus payment in central bank money⁹) and Creation (used for the securities settlement instructions free of or versus payment in commercial bank money) process all instructions in real-time ensuring a simultaneous exchange of delivery and payment. Regarding T2S, a real-time interface between T2S and CEU’s SSS CASCADE ensures the exchange of settlement information as well as the consistency of the instructions in T2S and CASCADE. Securities are matched and provisioned prior to settlement to ensure the adequacy of cash and securities for settlement. The timely processing is assured by undertaking regular mitigating measures, such as system developments as soon as potential system performance issues are detected. The high level of system performance is being ensured by regular system regression testing activities.

For external settlement with domestic markets via direct or indirect CSD links through the Creation SSS, the settlement model applied may vary per market. Such information is available in the [Market Link Guides](#) on the Clearstream website. Any external receipt or delivery instruction is only released for settlement after successful provisioning of the securities or cash obligation. DvP transactions involving a domestic counterparty are final depending on the receipt of expected settlement results in accordance with local

⁹ T2S versus payment settlement comprises transactions in EUR or DKK currency central bank money (with cash settling on T2) as well as versus payment in non-T2S eligible currencies (with securities settling free of payment on the T2S platform, and cash settling in the Creation SSS).

market regulations and practices and in particular under consideration of the processing mode (batch, real time) of the relevant local market and its time zone. Upon successful validation of respective settlement results received from domestic markets, real-time processing will take place in Creation in order to reflect the full transfer of securities and cash.

The finality of instructions is further described in [Principle 8](#).

The order in which transactions are considered for provisioning and settlement is generally determined by the transaction priority (assigned by the participant or by CEU), and the settlement sequence option on the account.

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

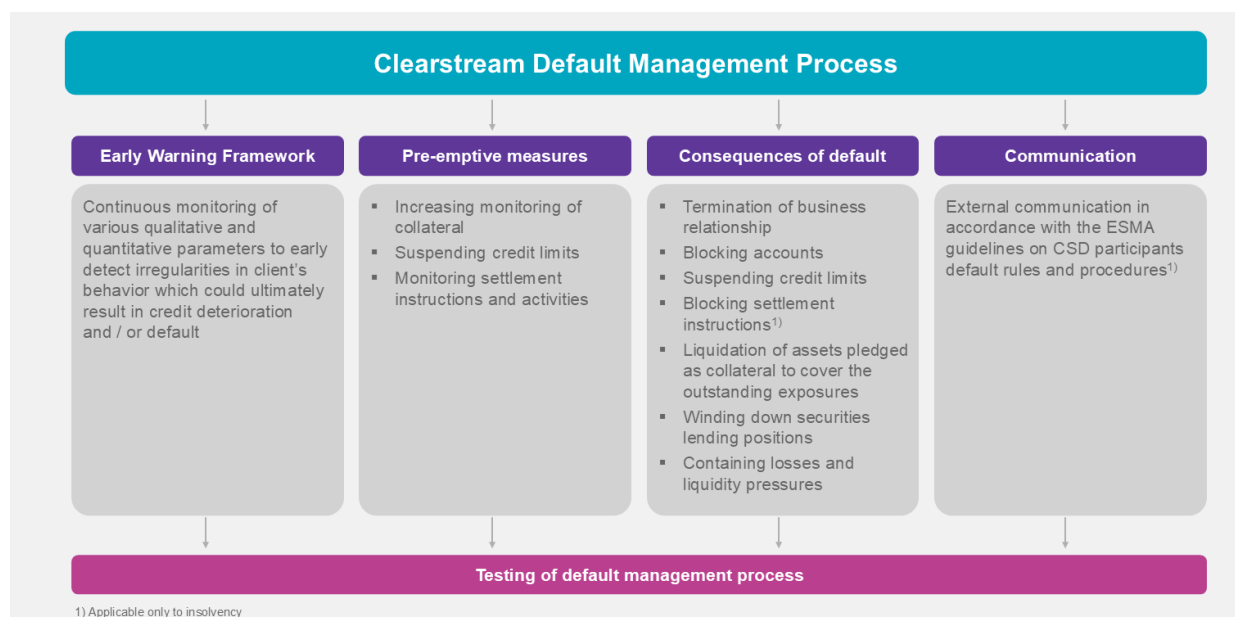
An FMI should have default rules and procedures that enable the FMI to continue to meet its obligations in the event of a participant default and that address the replenishment of resources following a default.

CEU has default management process (DMP) rules and procedures in place which define the circumstances under which a participant is considered to be in default, the measures implemented to mitigate the risks arising from a participant default and the testing activity to ensure its continuous improvement.

Referring to the products and services offered, CEU defines two types of default:

- (i) Legal default: When a participant is unable to fulfil its contractual obligations according to an agreement with CEU where insolvency proceedings, as defined in Article 2 (j) of SFD, are opened against a participant. "Insolvency proceedings" shall mean any collective measure provided for in the law of an EU Member State, or a third country, either to wind up the participant or to reorganise it, where such measure involves the suspending of, or imposing limitations on, transfers or payments.
- (ii) Contractual default: When a participant is unable or unwilling to fulfil, in a timely manner, one or more of its scheduled obligations according to an agreement with CEU.

The DMP of CEU has been implemented in accordance with this Principle and Article 41 of CSDR. The chart below describes different phases of the DMP, which consist of (i) monitoring (identifying a participant's default at an early stage and taking preliminary measures in order to eliminate/reduce the exposures), (ii) taking corrective measures (liquidation of defaulting participant's pledged collateral in order to cover the outstanding exposure) and (iii) communicating, as per ESMA guidelines, the competent authority and the defaulting participant of the actions to be taken or taken by the CSD following the default and any other persons of the actions taken following the default.



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.

The Clearstream Default Management team (CDM) is the owner of the DMP. The process is initiated and coordinated by CDM, which regularly reviews, tests and amends the process, where necessary, in order to be well prepared to act if needed. In case of a participant default CDM would initiate the DMP. Upon approval of default, the DMP foresees the suspension of the credit limits (if not already implemented as a pre-emptive measure) and the liquidation of the defaulting participant's collateral for the purpose of covering the outstanding exposures (if any). Liquidation of collateral is a corrective measure in the process. The key objectives of liquidation are to (i) minimise the losses for CEU, (ii) limit disruptions to the market by ensuring a smooth collateral liquidation and a timely completion of settlement even under stressed market conditions and as a result avoid impact on the normal settlement activity of non-defaulting CEU participants, as well as (iii) sell collateral in a prudent and orderly manner.

CEU's settlement system offers its participants various options to segregate proprietary assets and underlying clients' assets in accordance with Article 38 of CSDR. Only participants' proprietary assets pledged as collateral are subject to liquidation in case of default. The underlying clients' assets are segregated and cannot be pledged or be subject to the other security interests permitted by CEU's GTCs. Therefore, underlying clients' assets are not subject to liquidation or off-setting in case of a participant default (if not specially agreed otherwise).

Upon default of a CEU participant, there are two types of treatment for the underlying clients' assets:

- (i) In general, should a CEU participant default contractually, this participant will be able to continue its operations at CEU once the outstanding exposure of CEU, on the given participant, has been covered in accordance with the rules and procedures of the DMP. As such, the defaulting participant will also be able to continue the operations of its underlying clients as its assets remain on the accounts opened with CEU. However, CEU could decide on a case-by-case basis to terminate the relationship in accordance with the GTCs and its Client Access and Acceptance Policy.
- (ii) Should a CEU participant default legally, CEU would follow the instructions of the appointed administrator in order to transfer the remaining proprietary assets of the defaulted participant as well as the assets of its underlying clients to the dedicated accounts opened by the insolvency administrator. Should an underlying client wish to open a direct account with CEU, CEU would apply the standard due diligence under the participant acceptance criteria and decide whether an underlying client meets the criteria to be accepted as a new CEU participant.

With regard to a participant's underlying client transactions, CEU applies the settlement finality rules, provided the provisioning rules are respected. Should a participant of CEU default, the DMP would be activated, and the accounts of the defaulting participant would be blocked. Under the settlement finality rules, CEU would allow manual release of the relevant pending transactions.

CEU's GTCs and its uncommitted intra-day Technical Overdraft Facility (iTOF) agreement govern the right of pledge over participants' proprietary assets and their enforcement of those assets in case of a participant's default. Based on this, CEU's DMP defines the operational processes which enable the company to promptly access the above-mentioned pledged assets in case of a participant's default and liquidate them in order to cover any potential outstanding exposures of the defaulted participant.

Additional financial resources that can be used for avoiding liquidity pressures or covering potential liquidity gaps are defined in [Principle 7](#), [key consideration 10](#). In addition, the Clearstream Recovery Plan states that financial resources are to be used for recovering from a major potential loss.

In compliance with the ESMA guidelines on CSD participant default rules and procedures, CEU communicates a participant's default and/or the measures taken following a default to all relevant stakeholders. CEU's default management procedures define the communication path in case of a partici-

pany's default to the relevant internal and external stakeholders. The communication of default to the competent and relevant authorities of CEU is part of the communication plan. In order to inform the non-defaulting participants of the actions taken following a participant's default, CEU will publish a press release on its website as well as an alert on Xact Web Portal.

All default management processes and procedures are reviewed, tested, updated and approved by CEU's Executive Board at least annually in order to ensure their quality and functionality.

Key consideration 3

An FMI should publicly disclose key aspects of its default rules and procedures.

CEU publishes an overview of its main default management rules on the [Clearstream 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.

CDM conducts the default management testing in order to ensure a continuous improvement of the DMP and the best possible level of preparation for a crisis situation, which can be triggered either by a participant default or a market crisis. In addition to the regular maintenance of the DMP, CDM undertakes the default management testing following any substantial changes to CEU's default rules and procedures or upon request from its competent authority. In accordance with the ESMA guidelines and depending on the type of test, CDM can invite different participants. These can be CEU participants, relevant FMIs and any other entities, as appropriate, for the securities settlement system it operates. The competent authority may also request to take part in such tests. CDM tests the default management process also to ensure that all relevant stakeholders are familiar with their roles and responsibilities in the DMP. Additionally, the objective of default management testing is to provide training and guidance to CEU personnel on how the default rules and procedures should be implemented.

CDM also discloses on Clearstream's website at least a summary of the result of the performed tests and the contemplated changes to its default rules and procedures, if any. Additionally, CEU offers participants the opportunity to be involved in the Clearstream default management framework by going through the company's default rules and procedures as well as the testing activity with the Clearstream Default Management unit.

Principle 14: Segregation and portability

A CCP should have rules and procedures that enable the segregation and portability of positions of a participant's customers and the collateral provided to the CCP with respect to those positions.

Not applicable to CEU.

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 materialise. 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.

For CEU, business risk reflects the sensitivity to macroeconomic evolution and vulnerability to event risk arising from external threats, such as changes in the competitive, macroeconomic, regulatory or political environment or internal weaknesses (including erroneous strategic management decisions). It comprises, for instance, threats from competition, a negative economic environment and other aspects, which lead to revenues that are lower than projected or costs that are higher than projected.

Revenue risk arises if the competitive environment deteriorates as a result of the demand situation on the market, or a change in this situation; for example, due to an inability to sell the services, changes in participant requirements, missed trends, a change in business areas, overpricing, or a lack of production efficiency.

Major cost drivers for cost risk are, for instance, labor, hard- and software or external providers. Moreover, CEU has direct and indirect dependencies on earnings before interest, tax, depreciation and amortisation (EBITDA) like interest rates, the gross domestic product, interest or foreign-exchange rates which could result in risk from macroeconomics. Besides the obligation to fulfil all current regulatory requirements, the risk of changing laws may additionally impact CEU in a negative manner.

Overall, business risk is the loss (including losses arising from missed opportunities) arising from strategic decisions and/or their implementation, or from the inability to adapt to external factors. Earnings at Risk (EaR) are calculated using a Value-at-Risk (VaR) model and are based on the variance-covariance approach using a historical time series of profit and loss figures. The model uses a historical time series of more than 15 years. The confidence level is of 99.9% in the economic perspective of the internal capital adequacy assessment process (ICAAP) over a specified time horizon of one year. The methodology is based on quarterly relative deviations – positive as well as negative— between budgeted and actual profit and loss figures.

Further, CEU uses a scenario-based approach under CSDR to assess the effect on revenue and cost drivers by estimating potential loss scenarios. Revenue risk could arise, for example, when the competitive environment deteriorates because of reduced market demand. Drivers of revenue risk include the inability to sell services, changes in client requirements, missed trends, or a change in business areas. The drivers for cost risk include, for example, labor market changes or changes to pricing from hardware. An expert panel for each scenario estimates the effects of these drivers.

For CEU, the framework to manage and control business risk comprises several instruments including an early warning system based on key risk indicators (KRIs).

Details on responsibilities, process and procedures with regard to risk management are documented in Clearstream's Business Risk Handbooks (ICAAP and CSDR). Both are reviewed annually and updated on an ad hoc basis.

Furthermore, as an additional level of assessment, Clearstream Risk Management performs stress testing. The objective of the business risk stress test is to identify current and relevant threats for CEU in order to derive the potential impacts of these events to the company's revenue and cost situation.

In general, the top three business risk scenarios are eligible for stress testing, along with a potential fourth "root cause" scenario (e.g. related to geopolitical risk). Therefore, the stress test storyline takes into account a plausible combination of these top scenarios, covering the key business risk drivers. It is assumed that the selected scenarios will occur at the same time. They are selected based on the three highest maximum losses, as well as other economic/business factors important to CEU's business strategy implementation. The potential fourth scenario is an example of such a factor, providing a root cause for the stress test storyline.

In order to ensure completeness and the timely update of the business risk stress testing framework, CEU regularly monitors the main business risk stress test drivers, analysing the information received by different organisational areas.

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.

Liquid net assets funded by own funds

CEU's own funds are used to fund CEU's investment portfolio. Liquid own funds are composed by cash and bonds with a maximum time to maturity per transaction of five years, as described in the Clearstream Treasury Investment Policy. These assets are EUR or USD denominated. Only highly liquid financial instruments with minimal market and credit risk, and hence minimal adverse price effect, where public update of the prices is available, are eligible. The high quality of the assets ensures that in times of stress same-day monetisation may be achieved by either using the ECB marginal lending facility. CEU currently has a number of committed FX swap facilities to convert into a number of currencies including EUR and USD.

Capital requirements under CSDR

In order to be compliant with Article 6 "Capital requirements for business risk" of DR (EU) 2017/390, CEU applies the following measures.

For the scenario-based business risk model used under CSDR for relevant business risks, a scenario analysis method is used, that is, a structured form of assessing current business risks based on experts' knowledge, macroeconomic input data and external research. Using the said scenario analysis, CEU achieves several objectives:

- Documenting and assessing business risk and major potential events
- Establishing a sound basis for risk management, by determining likelihood and effect of potential generic events
- Allowing for a follow-up on the success of implemented measures
- Including the macroeconomic and regulatory environment as well as internal factors

In order to effectively identify, monitor and manage general business risks, scenario analysis and parametrisation are carried out by experts of CEU's first line of defence and of the Clearstream Risk Management team with an oversight of senior management. Senior managers are involved throughout the process and confirm the completeness, accuracy, relevance, timeliness and reliability of coverage.

The capital requirements of a CSD for business risk shall be whichever of the following is higher:

- 25% of the CSD's annual gross operational expenses
- Estimated amount resulting from the application of the scenario analysis, minus whichever of the following is the lowest:
 - Net income after tax of the last audited financial year
 - Expected net income after tax for the current financial year
 - Expected net income after tax for the previous financial year where audited results are not yet available

CEU has developed business risk-specific key risk indicators (KRIs) which are reported within the quarterly risk reporting. The metrics give an overview of the components that are also used as input data for the Earnings at Risk (EaR) business risk model. They may trigger an ad hoc review if considered necessary. KRIs are reviewed at least annually in collaboration with subject matter experts. The KRIs are monitored on a monthly and a quarterly basis. The purpose of this underlying early warning system is to determine if an ad hoc review of a particular risk component is required and to outline the required reporting to the executive management in case of a trigger event (yellow and red warning lights).

When a breach occurs, the relevant business units shall investigate the related detailed information and especially the root cause(s) of the breach and estimate/calculate the potential impact of the breach. In addition, if deemed necessary and possible, the respective business area can develop and propose a remediation plan to compensate the impact of the breach.

When investigating the root cause(s), the business units shall examine if the breach was the result of a specific event. If the cause/threat is new, that is, it has not been seen or recorded before, an ad hoc business review shall be proposed to the executive management. It is the responsibility of the respective business area to ensure further development/alignment and introduction of mitigating actions. Typically, mitigation actions (for instance, increase of fees or reduction of certain costs) to compensate the impact materialising business risks have to be approved by the responsible executive management.

Moreover, a list of descriptions of mitigating factors is collected for all the scenarios. Estimates are provided net of effects of any mitigating controls and/or actions in place. The aim of the mitigating measures and controls is to reduce the frequency of occurrences. The extent of this reduction is difficult to quantify and is not quantified in the scenario-based risk analysis.

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.

CEU distinguishes between requirements for a recovery plan (mitigating a near-default situation), a restructuring and wind-down plan (ensuring solvent wind-down) and a resolution plan (insolvent wind-down).

The recovery and restructuring and wind-down plans are drawn up and maintained by CEU. Their purpose is to set out available tools of CEU to overcome severe financial and operational shocks that could potentially undermine the viability of CEU and sustainability of its business. Ultimately, the plans aim at ensuring the continuity of CEU's critical services and operations, also preventing significant adverse effects on the financial system.

At present, the recovery capability of CEU is considered to be given. A suitable number of viable recovery options has been identified for the case CEU is exposed to severe stress. The range of identified recovery options ensures that CEU can raise sufficient capital or funding to withstand severe stress affecting its capital and liquidity profile. In addition, there is a range of recovery measures aimed at restoring the company's operational capacity or strengthening the risk profile.

Operational capability has also been proven to be stable, even in crisis situations. This is the result of robust and efficient crisis management processes and procedures as well as detailed business contingency measures, which are partially also reflected in the recovery plan.

Both risk and financial profiles of CEU prove to be robust and only an extreme event would trigger a near-default situation. As aforementioned, CEU has a number of recovery options, which would be implemented as an appropriate response to severe stress. In addition, CEU has adequate crisis and default management procedures to deal with anomalies and emerging crisis situations. These procedures are regularly tested to ensure their effectiveness and that all relevant stakeholders are familiar with their roles and responsibilities. Hence, CEU is able to respond very quickly to a crisis event and implement the necessary mitigating tools in a timely manner.

The recovery plan is reviewed at least annually and approved by the Executive Board of CEU as described in [Principle 3, key consideration 4](#).

In the restructuring and wind-down plan, several tools are identified as being applicable in restructuring and wind-down scenarios. The scenarios are differentiated on the basis of the criteria and requirements stipulated by CSDR and considering the applicable tools accordingly. These tools vary in their applicability and feasibility depending on the scenario.

The restructuring and wind down plan of CEU defines a restructuring and wind-down timeline based on the relevant scenario and the applicable tools. Accordingly, the necessary amount of capital is derived to ensure that critical operations and services can be continued during the restructuring or wind-down period. Currently, CEU is subject to a restructuring or wind-down period of eight months.

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.

CEU's investment portfolio is composed of issuers whose bonds have a remaining life to maturity below five years. These assets are exclusively ECB-eligible HQLA Level 1 assets denominated in Euros (CEU's equity is only in EUR currency). They are kept unencumbered on a separate account under the direct management of CEU's Treasury team as the company's liquidity management function. The assets may only be used as a source of contingent funds during stress periods. They are directly transferrable to Deutsche Bundesbank to generate intra-day liquidity via CEU's credit line.

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.

CEU maintains recovery and recapitalisation plans, which include a range of recovery strategies under severe stress scenarios, including situations in which equity falls below the recovery threshold or minimum regulatory requirements.

The viability of both recovery plan and recapitalisation plan is ensured through an annual maintenance and update cycle. The updates incorporate input from subject matter experts, enhancing the comprehensiveness and effectiveness of the plans. Following completion of the annual review, both plans are submitted to CEU's Executive Board for approval. Moreover, the plans are shared with the relevant supervisory authorities, who evaluate the plans' compliance and feasibility and provide their assessment, which is considered in the ongoing improvement of the plans. To ensure operational effectiveness, the plans are internally tested for the evaluation of governance processes in place. The testing results as well as any lessons learned, either from tests or real-case scenarios are taken into account to make necessary enhancements to verify plans' readiness.

Principle 16: Custody and investment risks

An FMI should safeguard its own and its participants' assets and minimise 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 participants' assets at supervised and regulated entities that have robust accounting practices, safekeeping procedures, and internal controls that fully protect these assets.

All CSDs and agent banks appointed by CEU in domestic markets are contractually required to obtain and maintain all necessary permits, licences and consents or authorisations required by applicable law(s) to enable them to fulfil their obligations under the agreement. CEU ensures that the CSDs and agent banks have robust accounting practices, safekeeping procedures and internal controls through a set of assessment measures described below.

In its **direct link** model, CEU holds its own and its participants' assets in accounts opened directly at a local CSD. In these cases, CEU operates its own account and performs both settlement and custody activities together with the local CSD. The role of the CSD/agent bank is reduced to a power of attorney which can be revoked with immediate effect. Furthermore, CEU has established **directly operated links**, where local CSDs enable settlement services and appointed local partners (Agents) provide custody services in a number of domestic markets.

Both link types qualify as CSD links. For each link arrangement, CEU assesses all elements relevant to asset protection to ensure full compliance with its obligations towards its participants. This includes evaluating the enforceability of contractual arrangements with the local CSD or appointed agent, as well as ensuring the protection of the assets—particularly in the event of the insolvency of the CSD or the agent bank.

How CEU assesses local CSDs and agent banks

The Clearstream Network Management (NM) function is responsible for the establishment, ongoing maintenance, and oversight of relationships and services with CEU's network of CSDs, central banks and agent banks. The team also assesses the risks resulting from the relationship with the CSDs. As part of this mandate, NM conducts continuous assessments of the risks arising from these counterparties, including operational, legal, and financial risks, to ensure that such arrangements remain compliant with CEU's regulatory obligations and risk management framework.

Each market linked to CEU is supervised by a dedicated Clearstream Network Manager who provides comprehensive, "end-to-end" oversight of all market infrastructures, CSDs and agent banks relevant to that market, ensuring that the services received are reliable, that counterparties meet CEU's standards, and that all associated risks are duly monitored, escalated, and mitigated in accordance with CEU's policies and the applicable international standards.

Relationship management tasks include the following:

- Monitoring and maintenance of legal documentation
- Policies and guidelines (for example relating to risk management and contractual arrangements)
- Process definitions
- CSD/agent bank and market review process
- Management of statistical reporting and business targets
- KPI reporting, analysis and action planning
- Issue management
- Incident management
- Benchmark development and maintenance
- Monitoring and communication of market changes internally across impacted departments and externally towards participants
- Annual credit review (by Credit department on behalf of NM) for non-EEA CSDs

Through these measures, the NM team, who is located in Luxembourg, Prague and Singapore, ensures that local CSDs and agent banks linked to CEU have in place robust accounting practices, safekeeping procedures and internal controls. The CSDs and agent banks are assessed by NM as part of the selection process during the setup of a new market link and on an annual basis for existing links.

Furthermore, CEU ranks its linked CSDs and agent banks on the basis of MIS data collected by its NM and Operations teams. The rankings are complemented by periodic depository quality assessments for CSDs and agent banks across the network.

Cash correspondent banks (CCBs), in the case of the 6-series account activities, are subject to similar obligations compared to those applicable to CSDs and agent banks as described above and in the following sections.

Selection process via requests for proposal/information (RfP/RfI)

When CEU establishes a new market link, Network Management (NM) conducts a comprehensive Request for Proposal (RfP) / Request for Information (RfI) process to ensure that the selected central securities depository (CSD) or agent bank operates in a manner that adequately safeguards CEU and its participants from custody and investment risks. The assessment framework includes:

- a detailed review of the candidate's operational processes,
- a legal and compliance assessment of the proposed infrastructure, and
- an evaluation of the intermediary's credit standing.

CEU evaluates candidate CSDs/agent banks based on their responses to the RfP/RfI questionnaires and supporting documentation. The selection criteria include, inter alia:

- **Operational efficiency**, including settlement deadlines, turnaround times, and process resilience
- **Creditworthiness**, including capitalisation, asset quality, governance and management competence, risk profile, earnings capacity, and liquidity

- **Compliance standing**, including corporate structure, ownership, shareholder composition, and market capitalisation
- **Adherence to AML/CFT requirements**, specifically compliance with regulations addressing money laundering and terrorist financing
- **Proposed credit lines**
- **Fee structure and pricing transparency**
- **Connectivity and technical capabilities**, including Swift compatibility and compliance with straight-through processing (STP) and ISO 15022/20022 standards
- **Market presence and systemic relevance**, including the intermediary's market share and participation in relevant local market forums

Following the evaluation of RfP/RfI responses, CEU shortlists candidates. Due diligence visits (DDVs) may be conducted on the finalist(s). Based on the documentation received and the results of the DDVs, NM forms a comprehensive view of the risks associated with establishing the new link or appointing the intermediary. CEU may, where deemed necessary, conduct additional verification by contacting clients of the candidate institution.

Final approval of the selected CSD or agent bank is granted by CEU's Executive Board.

Once a market link has been established, CEU performs annual reviews to verify the intermediary's continued compliance with the provisions of the link agreement. These reviews rely on a defined set of tools and control measures, the most significant of which are outlined in the subsequent sections.

Link arrangement review questionnaires

The link arrangement review questionnaires are sent out to each CSD. These questionnaires intend to verify the CSDs' compliance to all key regulatory points of CSDR. It has been based on this regulation and is commonly used by all CSDs in the countries covered by CSDR. For CSDs not covered by CSDR, a more extensive questionnaire is used.

Due diligence inspections including DDVs

Due diligence inspections consist of any verification deemed appropriate in order to ascertain that the CSD/agent bank fulfils its obligations under the legal agreement pursuant to the professional standards of a securities custodian. Hence, the inspections are based on the AFME industry standard questionnaire and an appendix with a set of additional questions that are specific to CEU as CSDR regulated entity, for indirect and operated links. These questionnaires cover aspects such as, among others:

- (i) Legal and regulatory frameworks
- (ii) Security and insurance coverage
- (iii) Operational processes and reconciliation items
- (iv) Business continuity management
- (v) AML measures
- (vi) Recent and forthcoming market changes

This assessment allows CEU to monitor and manage any additional risks resulting from the use of an agent bank and to verify that the link and the agent bank meet the regulatory requirements set out in CSDR. Like the link arrangement reviews, DDVs provide CEU's NM team with additional information on the respective markets since the Network Managers also use them to discuss subjects such as regulatory changes, market developments, fee renegotiations or potential business developments (for example the inclusion of a new asset class on the link).

Depending on the link structure, DDVs may additionally include a review, among others, of the agent or CSD operations site or vaults if applicable, as well as meetings with regulators or market infrastructures. DDV reports and accompanying material are subject to internal and external audit reviews. As part of the annual CSDR review and evaluation process, CEU shares the outcome of the DDVs with the regulators.

Service reviews

In addition to the annual due diligence inspections, CEU conducts service reviews on its various CSDs/agent banks. These service reviews are organised on an ad hoc basis, sometimes in combination with an annual DDV, and may be established on a recurring, periodic basis if required. Generally, service reviews focus on a specific set of issues or topics whereas DDVs are rather an overall assessment of the CSD/agent bank and the respective market.

External legal opinions

CEU requests legal opinions on its custody network links from external legal counsels that take into account the requirements of CSDR (as defined in [Principle 1](#)). They are considered an independent and neutral confirmation of key legal requirements in respect to the market served. They confirm the foreign depositories' abilities to perform, as required under the respective link agreements, without the risk of being superseded by local regulations or practices.

Regarding the scope of the opinions, please refer to [Principle 1](#).

The opinions further aim at confirming the relevant and competent regulators of the respective CSDs/agent banks. They are subject to annual renewal at CEU's expense and in accordance with the agreement made with the respective legal counsel.

Officer's certificates on internal control system

In these certificates, agent banks confirm that an effective internal control system is in place for the securities, that respective controls are reviewed at least annually by their external auditors and that during the preceding year, no such review has revealed any material deficiencies or made any material objections other than those already notified to CEU, as the case may be.

Further documentation

In addition to the above assessment measures to verify its linked CSDs'/agent banks' compliance with contractual, legal and regulatory requirements on an annual basis, CEU requests a documentation of their business continuity management and asks for completion of an AML questionnaire.

Key consideration 2

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

CEU ensures that participants' assets are protected and can be accessed promptly whenever required. Securities held on behalf of participants are maintained in dedicated accounts opened by CEU in its own name at the relevant local CSDs. These accounts are clearly flagged as client accounts to ensure strict segregation from CEU's proprietary positions.

For assets held in local markets via linked CSDs or agent banks, prompt access is further supported through the established 6-series account structure, which provides a clear and transparent view of client holdings and enables continuous oversight of safekeeping arrangements.

To protect both participant and proprietary assets, CEU's participation agreements with the local CSD and agent banks explicitly state that no lien, pledge, or right of retention may be applied to the assets held. This safeguard is reinforced by independent legal opinions, as referenced under [key consideration 1](#).

In the event of a participant default, CEU immediately blocks all accounts containing pledged collateral to prevent any unauthorised movements. Should a liquidation be required, pledged assets are segregated and managed in accordance with established default procedures to enable timely and orderly realisation.

CEU also maintains its own securities in separate proprietary accounts at the local CSDs, ensuring that it has direct and unrestricted access to these assets whenever needed.

To maintain continuous and reliable access, both for client holdings and for its own, CEU monitors the operational performance and legal compliance of its linked CSDs and agent banks through defined oversight processes and contractual standards.

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.

CEU achieves optimal reduction of exposure to linked CSDs and agent banks by holding assets under custody directly with the respective CSD. Currently, the vast majority of securities are held under this structure.

CEU also maintains a link to CBL for non-T2S securities. CBL, in turn, applies the same controls as CEU applies to direct links.

Elements regarding the monitoring of the exposure vis-à-vis CSDs and/or agent banks and CCBs (in the case of the 6-series account activities) are described in further detail in [key consideration 1](#) as well as in [Principles 4](#) and [7](#).

CEU's measures to understand its exposures to its intermediaries/ custodians

CEU's procedure on CSD Links and agent bank risk management outlines the activities, documentation and stakeholders involved in identifying, assessing, controlling and monitoring risks for CEU and its participants—both during the setup of a market link and on a periodic basis thereafter. CEU identifies three main categories of risks when assessing new or existing CSD Links: (i) financial risk, (ii) operational risk, and (iii) business risk.

For CEU, all links are direct or direct-operated, which means CEU's accounts are held directly with the respective CSD, significantly minimizing CEU's custody risk.

In accordance with ESMA RTS, if Agents are involved (e.g., in operationally supported models), such entities must be credit institutions as defined by CRR or third-country financial institutions subject to equivalent prudential rules. Intermediaries must also comply with CEU's operational, reconciliation, account segregation and risk management requirements.

CEU's measures to evaluate and manage its exposures to its intermediaries/custodians

CEU achieves optimal reduction of exposures to CSDs and potential intermediaries by holding assets under custody directly with the respective CSD. As a result of CEU's operational model, CEU maintains dedicated accounts directly at CSD level (see [key consideration 1](#) for additional details on link types). This direct-holding structure materially reduces custody and credit exposures.

Elements related to the monitoring of exposures vis-à-vis CSDs and, where applicable, agent banks or central credit banks, are further described in [key consideration 1](#) as well as in [Principles 4](#) and [7](#).

Assets placed with central banks are subject to limited or no concentration limits, as such institutions are considered risk-free depositories for their respective currencies and eligible financial instruments. For CEU, no concentration limits apply to cash held at the central bank of issue, nor to securities (assets and collateral) held at the central bank of issue. Agent banks and central credit banks are included in CEU's aggregated credit risk monitoring. Further details on exposure monitoring and collateral concentration limits are provided in [Principles 4](#) and [7](#).

To avoid excessive reliance on any individual financial institution, CEU monitors and controls concentration limits on an intra-day basis. Alerts are triggered whenever predefined thresholds are approached. The sufficiency of these limits—per currency and on a consolidated basis—is evaluated through ex-post stress tests, and their accuracy is confirmed through liquidity stress-testing.

CEU reviews its policies and procedures regarding applicable concentration limits for liquidity providers annually, or sooner if a material change occurs that may affect CEU's risk exposure to a specific financial institution.

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.

CEU's investment strategy

CEU's investment strategy has two main objectives: in the first place, the company aims at the minimisation of credit and market risks by managing its own funds and participant cash in order to ensure capital preservation. The second major objective is CEU's access to liquidity to always ensure the company's ability to satisfy payment obligations in a timely manner. The investment strategy forms part of CEU's liquidity risk management strategy and is described in detail in [Principle 7](#). Further information is available in CEU's [Pillar III disclosure report](#) on the Clearstream website.

Risk characteristics of CEU's investments

CEU does not engage in proprietary trading activities and does not maintain a trading book.

Investments in securities as part of the investment or short-term portfolios are only high-quality liquid assets (HQLA) against high-quality obligors. These are purchased by using the "buy and hold" strategy and are recognised in CEU's banking book. They always remain unencumbered and available for an immediate sale or monetisation if required. CEU's Investment Policy defines limits for securities purchase transactions.

CEU's Treasury team invests in highly liquid financial instruments with minimal market and credit risk. To minimise counterparty default risk, placements may only be executed with counterparties of adequate creditworthiness. Credit quality is expressed through an internal rating assigned by the Credit department and described in the Credit Policy.¹⁰ The policy requires that 90% of available funds are placed on a secured basis, that means, (i) deposited with central banks, or (ii) through arrangements that ensure the collateralisation of cash with highly liquid assets, or (iii) HQLA securities that can be monetised on an intra-day basis.

If no access to a central bank's deposit facility has been granted or if no other alternative secured instrument is available, Treasury places uninvested funds among several commercial institutions to avoid concentration risk.

¹⁰ Accordingly, placements may only be executed (i) with counterparties with a minimum internal rating of "D" which corresponds to an external rating of BBB+/BBB (Fitch/S&P) or Baa1/Baa2 (Moody's), or (ii) with counterparties exceptionally approved by CBL's/CEU's Executive Board.

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.

Identification of operational risk

Operational risk is generally defined as the risk of losses resulting from people, systems, inadequate/failed internal processes or from external events. More specifically, CEU has adopted a definition that is in line with Basel definitions of operational risk which is the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by CEU.

CEU established appropriate systems, policies, procedures and controls which are described within the adopted risk management framework. The company applies a five-step process for risk management, described in [Principle 3](#). Risk identification involves, to the most complete extent possible, all operational risk issues relevant to CEU, as well as risk drivers. Risks may arise as a result of internal activities or external factors. The risk examination must be performed with regard to existing or new processes, when concluding new business or entering new service areas. The identification can be reactive, following an operational risk event, but it should also be pro-active, based on regular reviews of processes in order to identify weak areas, or based on scenarios taking into consideration all potential sources of issues.

Operational risk contains the following 17 risk clusters: compliance risk, contagion risk, corporate tax risk, custody risk, data integrity risk, information security risk, information technology risk, legal risk, model risk, operational project risk, people risk, physical security risk, process risk, product tax risk, risk management risk, secondary reputational risk, and third-party risk.

The risk taxonomy of operational risk on four levels supports CEU to identify and categorise (potential) risks and allows the company to link appropriate risk management activities.

IT tools support the identification, assessment, monitoring and management of operational risks and ensure the technical environment of CEU remains stable (for example, ensure processing and monitoring of the infrastructure). With regard to operational risk, CEU is, in particular, using IT tools and processes to manage and monitor its systems to minimise operational risks for the settlement systems.

Furthermore, CEU has in place a wide range of various controls set up with the aim to minimise the impact of sources of operational risk. The control environment includes IT controls themselves but also covers several other types of controls (cybersecurity, logical access management, physical access management, stress testing, risk capital quantification (Value at Risk), BCM, project management process, 4-eyes principle, etc.). Some of these controls are detailed and documented in the "Mitigation actions and controls" section of CEU's operational scenarios which lists information on controls and procedures (which may also be supported by IT tools). The other control types are further detailed in the policies and procedures used by CEU to minimise operational risk.

After the risk identification step, the risks are notified to Clearstream Risk Management in the **notification stage**. All risks are centrally recorded. All organisational units and individual employees must timely notify Risk Management on risks which they have identified and evaluated. Depending on the materiality, two forms of notification can be distinguished: periodic and ad hoc.

The next stage is the **assessment**: All operational risk events or potential new risk developments are assessed qualitatively or in financial terms. The assessment of an incident or a potential risk development aims at quantifying the risk in financial terms using the VaR methodology and comparing the result with the available risk cover. It takes into account mitigation measures currently in place.

After the assessment, the stage of **treatment** follows. The most adequate treatment is applied to the identified risk in order to mitigate them or actively control/manage them. In general, mitigation encompasses the following: risk avoidance, risk reduction, risk transfer and intentional risk acceptance. All organisational units and employees must perform risk control, implement mitigating action, and monitor these actions according to the established processes.

The last stage of the process is the **monitoring and reporting** of the identified risks to the Executive Board (EB). The EB is at least on a quarterly basis and in addition on ad hoc basis – if required – and consistently informed about material risks and the related risk control measures.

CEU employs several policies, processes and controls that are designed to ensure that operational procedures are implemented appropriately:

- Risk strategy and risk appetite
- Operational Risk Handbook (incl. documentations): The objective of the Handbook is to give a comprehensive description of the processes and methodologies that constitute CEU's operational risk model from an economic perspective.
- Operational Risk Procedure: This Procedure describes the approach and major instruments applied within the process of managing operational risk on a high level. Furthermore, CEU has established a segregation of duties and follows the "three lines of defence" governance concept for operational risk management (the business functions as first line, the Risk Management function as second line and Internal Audit as third line).
- Reviews: CEU also conducts reviews of its risk management framework to identify the necessity or possibilities for amendments and improvements. This is performed at least once a year in the context of the Internal Capital Adequacy Assessment Process (ICAAP).

Change management and project management policies

CEU follows a stringent project management process which consists of three steps:

- Project planning and initiation: This includes the creation of a project charter, a project management plan, and other key project management deliverables.
- Project monitoring control and reporting: This describes the series of activities involved in managing a project against its approved project plans, managing scope and costs, managing relationships with suppliers to the project, managing stakeholders and communications, risks, issues and dependencies, project change, configuration management and quality, as well as reporting performance.
- Project closure: This describes the series of activities involved in closing a project appropriately, inclusive lessons learnt.

A dedicated Market Member Readiness (MMR) team is involved in projects from their initial set up. Their task includes the review of the Business Requirements Analysis (BRA) to identify any impacts on participants and other market participants, with the objective to communicate these as early as possible and ensure the readiness of these external shareholders. This avoids the risk of participants and other external stakeholders not being able to perform their business activities with CEU.

Software change management takes place according to a defined and documented process. The purpose of this process is to control changes to the application software in an organised manner by implementing approved changes with minimal disruption. Its scope covers the full life cycle of changes, including the correction of software incidents, requests for software change, approval of the change, development activities to realise the change, the initiation of software configuration management activities, testing activities and approval to launch the change in production environment. The standards mentioned above and used by CEU stipulate minimum requirements for availability and service continuity management.

As per CEU's processes, an acceptance, being functional and/or technical, is always mandatory for any change or fix in order to guarantee that the change functions correctly in a replica of the live environment, performs in the manner that was expected, does not cause degradation of other systems, and meets the needs of the business. This is complemented by:

A system and technical acceptance test: System performs as per technical requirements; no negative impact on other systems; performance check. This can involve testing with external parties, such as depositories.

A business acceptance test: Development is according to business requirements.

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

CEU has adopted a two-tier board structure and is therefore currently managed by an executive board (EB) which is supervised by a supervisory board (SB). Please refer to [Principle 2](#) for a detailed description of CEU's governance structure. Effective and efficient risk management is vital to protect CEU's interests and it enables CEU to achieve its corporate goals and safeguards its continued existence.

CEU's EB approves the company's risk strategy and risk appetite. The Risk Committee and Supervisory Board receive them for acknowledgement.

The EB of CEU is ultimately responsible for the company's risk strategy and appetite. The risk appetite defines the type and level of risks the organisation is willing to accept in pursuit of its strategic objectives and business plan. The Board ensures that the risk strategy is integrated into the business activities throughout CEU and that adequate measures are in place to implement the strategies, policies and procedures. The EB holds the responsibility to determine and communicate the risk appetite and that the risk management framework is adapted accordingly.

CEU's EB has the ultimate responsibility to ensure a strong risk management culture. This includes the ultimate responsibility for risk management, including operational risk and the determination of an appropriate level of aggregate risk tolerance and capacity. The Board also establishes a risk management framework that is consistent with the risk tolerance and capacity.

The EB is timely and consistently informed about material risks and the related risk control measures. Reporting is an essential part of risk management and is designed to give the EB and SB timely and accurate information about the risks that CEU has encountered. All relevant data and information are collected, assessed and prepared by Clearstream Risk Management.

The risk management framework of CEU, as stated in the Operational Risk Handbook, aims at ensuring that all threats, causes of loss and potential disruptions are properly identified as soon as possible, centrally recorded, assessed (that is, quantified in financial terms to the largest possible extent), reported in a timely manner and consistently, together with suitable recommendations to the EB, and controlled.

The risk management framework is constantly challenged by internal auditors, external auditors and regulators. In addition, to ensure that operational risk management approaches and systems are up to date, employees in the Risk Management function are members of different associations of risk management professionals that are engaged in the further development of respective operational risk topics. They regularly check for and take part in risk management conferences or seminars in this area.

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.

From a business perspective, CEU's operational reliability objectives are documented within a large set of key performance indicators (KPIs) that allow a quantifiable and qualitative view of service delivery provided by Business Operations. Such KPIs deliver information on effectiveness, efficiency, degree of automation, turnaround times, operational quality and operational risks for business processes. The operational reliability objectives are, among others:

- Automate processes and operate in STP mode wherever possible, that is, in the areas of income, corporate actions, tax, reconciliation
- Reduce operational errors to a minimum in all areas
- Provide competitive deadlines
- Reduce reversals to a minimum
- Set up new participant accounts as soon as possible
- Meet the recovery time objective (RTO) of two hours for time critical systems
- Provide self-explanatory documentation to decrease number of calls to Client Services

The above-mentioned KPIs are both of qualitative and quantitative nature and can be classified in three different categories with focus on:

- Quality and risk aspects
- Capacity and volume aspects
- Process efficiency aspects

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.

All of CEU's reliability objectives stated in [key consideration 3](#) aim at delivering services to participants at the highest level possible while ensuring a robust service resilience. This also includes the operation of systems at defined service levels.

CEU ensures continuously highest levels of system availability for its core systems (occasional down-times are scheduled on weekends for essential system maintenance). The Creation and CASCADE platforms are designed to cope with settlement volume peaks 50% greater than the average daily activity. Higher peaks can be directly handled by assigning further infrastructure capacity.

CEU has set up a monitoring of volumes in business and IT. Volume information is collected on a daily basis. This is supported by the monitoring of KPIs and deadlines, as defined in the service level agreements. In the event of a deviation or sudden surge in capacity requirements due to increasing volumes (changes in the market environment), an immediate analysis is performed and additional capacity is activated via on-demand arrangements with infrastructure providers to ensure system performance. Permanent changes follow the IT change management process (see [key consideration 1](#) for details), which includes impact assessments and, if necessary, subsequent stress tests.

CEU uses KPIs to monitor the capacity of its systems to ensure that a capacity buffer (also known as "headroom") is maintained. The following key internal indicators are used to monitor the CSD's IT system performance: system availability, external deadlines and load/resource consumption. Each month, a capacity management report including volume trends analysis is produced. If one or more of the said indicators fall below specific thresholds, CEU will take appropriate actions to improve or upgrade its systems in order to maintain the capacity buffer.

From a control perspective, during each application audit, KPIs and latest capacity management reports are reviewed and compared with the latest incidents reports. The capacity management process itself is also part of the audit plan.

Thanks to a comprehensive change and release management process, IT systems go through a structured development and testing process before being put into production. Robust tests are also performed throughout the lifetime of the IT systems, for example, whenever material changes are implemented to a system or when a system has suffered a major operational disruption, as applicable on the basis of the underneath root cause.

CEU practices a BCM risk mitigation and avoidance strategy by identifying and assessing the risks and taking preventive precautionary measures to address and mitigate adverse effects in infrastructure or data centre services in the form of developing and upholding business continuity and disaster recovery procedures. By maintaining a dual data centre strategy and keeping all key components redundant and identical between the two data centres for Clearstream-hosted applications, it is warranted that mainframe servers operated under full sysplex, enterprises disk storage systems and the tape library infrastructure including peripheral hardware such as storage area network and network components are always fully operational in both locations. This is perpetuated by continuously employing both data centres with running production and test workloads. Running production workloads in both locations will always fully allocate and demand the underlying infrastructure in its entirety for both data centre locations.

Business volume is monitored throughout the day and during night-time batch operations. Systems are equipped with additional headroom of unallocated reserved resources to accommodate to higher workloads, should it be necessary due to a large increase in business volume.

Business Operations has a high level of process automation and capabilities to address significant, short-notice increases of settlement volumes with limited impact on Business Operations. Key mitigation actions will be limited to resource measures like extended working hours or temporary allocation of resources from non-impacted business areas to impacted areas.

Key consideration 5

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

Physical security

CEU's physical security objectives are defined in the ICT Risk Management Framework and the Data Center and Physical Protection Guideline.

Physical security is a high priority for CEU due to continuously changing global security risks and threats. CEU has developed an integral risk management process to proactively and reactively protect the company, its employees and values from internal and external attacks and threats: Analysts continuously assess the security situation at our locations and on business trips, while maintaining in close contact with national and international authorities (Bundeskriminalamt, the German Federal Criminal Police Office, Bundesamt für Verfassungsschutz, the German Federal Office for the Protection of the Constitution etc.), security service providers, and security departments of other companies. Multi-level security processes and controls ensure physical security at CEU locations. Physical access to buildings and values is continuously monitored and based on the access principle of "least privilege" (need-to-have basis).

Physical Security designs and executes a risk management approach to prevent financial, human, regulatory and reputational loss events emerging from natural and human-made hazards, crime, civil unrest, terrorism etc. The strategic objectives of the operating model are:

- Availability and integrity of physical locations and other assets, including staff
- Physical access to legal entity premises only to authenticated staff, suppliers, and visitors
- Confidential information on physical assets is provided on a "need to know" principle and securely destroyed when disposed

To safeguard the strategic objectives for physical assets, Physical Security is additionally applying the following operational objectives in its risk management process:

- Prediction: forecasting of physical security threats before developing to imminent risks to legal entities
- Prevention: early mitigation of physical security risks before causing financial, human, regulatory and reputational loss events
- Detection: physical security measures that identify threats and vulnerabilities
- Response: physical security measures, that deter, deny, delay, and defend risks when they occur

ICT risk management

The ICT Risk Management Framework is a foundational element of CEU's control environment and is designed to provide reasonable assurance over the adequacy and operating effectiveness of ICT controls. It establishes a hierarchy of documents and end-to-end traceability from requirements to implementation and ongoing monitoring to achieve and maintain an adequate state of cyber resilience within the approved risk appetite:

- Level 1 – ICT Risk Management Policy: binding ruleset to manage and oversee ICT risks, including roles and responsibilities and the principles for digital and operational resilience, approved by the EB and reviewed at least annually
- Level 2 – ICT Risk Guidelines: define what must be achieved by specifying organisational, process, and control requirements, including the target level
- Level 3 – Procedures: define how requirements are executed to ensure consistent, compliant operations across the organisation
- Supporting documents: processes, standards, and work instructions that operationalise and evidence of control execution

The ICT risk management approach at Clearstream uses the European Digital Operational Resilience Act (DORA), supporting technical standards and respective terminology as a conceptual foundation. In addition, the ICT risk management framework, including but not limited to the minimum requirements stipulated in this policy, is based on ISO 2700X. The policy is based on the essential principles of the following (non-exhaustive) regulations, such as the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04), GDPR (Art. 32), the Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines, CSDR (incl. REFIT – Regulation (EU) 2023/2845), EMIR, Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG, German Act on the Protection of Trade Secrets) and the Minimum Requirements for Risk Management (MaRisk).

The framework is aligned with the Group Risk Management Policy and Taxonomy; ICT risks are managed as a subset of operational risk, using standardised classifications (e.g., impact levels) to support consistent identification, assessment, reporting, and treatment. The framework interfaces with further key corporate documents, including the Operational Risk Procedure and Handbook, the Group-wide Incident and Crisis Management Guideline, the Business Continuity Management Policy, the ICT Risk Management Policy, the Compliance Policy, the Data Protection Policy, and the Material Change Process Policy. Policies and guidelines are formally governed, version-controlled and reviewed on a defined cycle, subject to EB approval.

Roles and responsibilities are structured in line with the “three lines of defence (LoD)” model for effective management of ICT and adequate control mechanisms:

- **1st LoD** operates ICT, implements and maintains controls, executes security processes, and manages day-to-day ICT risks within the approved risk appetite.
- **2nd LoD (including the CISO, the ICT Risk Officer and Risk Management)** sets ICT risk requirements, oversees effectiveness, challenges risk and controls self-assessments, reviews security aspects of new initiatives and material changes, monitors threat intelligence and significant vulnerabilities, and reports at least quarterly on the ICT risk posture to the EB and relevant committees.
- **3rd LoD (Internal Audit)** provides independent, objective assurance through risk-based and event-driven audits on the adequacy and effectiveness of risk management, controls, and governance processes.

The EB and senior management are responsible for establishing the “tone at the top” regarding the importance of cyber resilience and information security, internal control environment including compliance with internal policies and external regulatory requirements. In addition, the EB approves the cyber resilience strategy and ensures that the strategy is regularly reviewed and updated according to CEU’s threat landscape.

The ICT Risk Control Function, with the support of relevant internal stakeholders, is responsible for defining the cyber resilience strategy and overseeing its execution from a second line perspective. It ensures that the cyber resilience objectives are properly defined and communicated, both internally and, when relevant, to third parties, and that compliance is reviewed, monitored and ensured. The CISO/CICTRO reports, on a quarterly basis, on the company’s security posture to the EB, the SB via the Risk Committee.

The Clearstream Risk Committee (CRC) is a committee with escalating authority, advises the EB on CEU’s overall current and future cyber risk appetite, risk tolerance and the remittance of information security and cyber resilience related risks.

The Digital Security Committee (DSC) consists of members of the Chief Information Officer (CIO) department of Deutsche Börse Group. It has been established to steer and shape the Group’s security. Regular activities include reviewing latest developments of the threat landscape and Deutsche Börse Group’s cyber resilience, steering priorities and supporting informed decision-making on investments.

IS risk management

The IS risk assessment is a component of the comprehensive Information Risk Management (IRM) framework documented in Deutsche Börse Group’s IRM guideline. The key purpose of the IRM framework is to provide a holistic view on risks affecting Clearstream’s information assets, to enable the effective treatment of these risks in a targeted and consistent manner as well as to report on these risks to the management and other stakeholders. The IRM is designed to consistently identify, analyse, evaluate, treat, monitor, review, report and communicate in line with internal and external (for example, regulatory or legislative) requirements.

The CISO/CICTRO reports to the EB and supports the colleagues in business, IT, and especially CEU information owners, to adequately protect their information and corresponding facilities from significant loss and to be compliant with legislative, regulatory, and contractual requirements.

Other security aspects

In relation to ICT and security risks trainings, all employees, including key function holders and executive management, receive the following periodical mandatory online training sessions covering, for example, the following:

- Risk awareness and culture
- ICT security
- Acceptable use
- Data leakage prevention
- Individual data processing

Tailored training for the Board is carried out on a regular basis.

Security tools are in place and cover, among others, access control, intrusion prevention and detection, denial of service, vulnerability scanning (for identifying potential vulnerabilities on IT applications and underlying IT infrastructure), events logging and monitoring etc.

The Cyber Emergency Response Team (CERT) is in charge of analysing pro-actively potential impacts of major cyber incidents and determining a regularly updated picture of cyber situational awareness. The CERT is also in charge of managing information security events and incidents.

Tests are performed, for instance, before the implementation of new processes and tools, regular penetration tests are performed ensuring the effectiveness of the controls in place.

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.

CEU's Business Continuity Management

Objectives of CEU's business continuity plan

CEU strives to provide products and services with utmost reliability. It thus gives the highest importance to the resilience of its business to safeguard it against incidents and disasters, as the unavailability of core processes and resources poses a substantial risk for the company and potential systemic risk to the markets. Therefore, CEU aims to satisfy itself and the markets of its ability to continue to operate under adverse conditions or in the face of unexpected events or disasters.

To achieve that, CEU leverage on business continuity solutions to address the loss of significant numbers of staff in one location, also considering solutions such as dispersed operations and business transfers.

CEU's Business Continuity Management System (BCMS) policy stipulates that in case of business interruption, operations must be resumed within appropriate time scales in order to:

- Safeguard CEU from significant losses, maintain revenue generation and shareholder value
- Maintain participant confidence, market stability and liquidity and minimise systemic risk
- Maintain management control, fulfil contractual obligations and regulatory compliance

The policy further defines that the processes, indispensable for the critical daily operations, are classified as mission-critical and must be resumed within a recovery time objective (RTO) of two hours.

In accordance with the policy, business continuity plans (BCPs) define the processes and resources including systems and the associated RTOs, thereby observing the RTO of two hours for mission-critical functions. Further RTO classes are defined for functions to be recovered within 24 hours, up to one week or more than one week.

The BCPs address the impact of unavailability of systems, workspace, staff and suppliers in order to ensure the continuity and rapid resumption of the critical operations in case of major or wide-scale scenarios.

Design of CEU's business continuity plans

BCPs are a collection of information, guidelines and procedures that specify how critical services, processes and resources will be reinstated to a predetermined minimum business continuity level within

pre-defined timescales after a business disruption, an incident or crisis affecting one or several of the key resources. CEU's BCPs are compiled, developed and maintained by the relevant organisational units for use in the event of a business disruption, an incident or a crisis to maintain the continuity of critical operations and reviewed regularly.

Mission-critical processes as defined above must be resumed within an RTO of two hours. Each unit responsible for a mission-critical CEU process must establish, implement, develop and maintain a BCP to cover its time-critical business activities, associated business recovery requirements and business recovery action plan.

The BCM framework, and associated BCPs, are designed to be as comprehensive as possible. Events which would lead to the unavailability of key resources (for example, workspace, IT systems, staff, suppliers) fall within the scope of the Clearstream BCM framework. BCPs deal with the direct effects of an event (workspace unavailability, staff unavailability etc.) rather than specific root causes leading to any disruption (for instance, natural disaster, pandemic situations, physical attacks, intrusions, terroristic attacks) as all these events would ultimately lead to the unavailability of facilities, staff, suppliers or technical equipment.

Interface to ICT Response and Recovery and Digital Operational Resilience Testing

Information and Communication Technology (ICT) is a fundamental resource for the effective and efficient operation of CEU's critical activities. Therefore, a dedicated interface for ICT Response and Recovery has been established to ensure timely service restoration.

ICT Response and Recovery plans are established by the respective teams operating the different technology clusters. These plans document the procedures for ICT-related infrastructure recovery and service continuity following significant ICT incidents.

Clearstream has established an IT resilience coordination and testing programme. This programme incorporates various IT security requirements and testing approaches to evaluate key resilience measures. A central element of this programme is the disaster recovery test, which simulates a data centre failure by isolating it from the network. During the test, all systems are recovered in the secondary data centre to validate its capacity to handle the full processing load independently. Participants, CSDs and/or agent banks as well as critical service providers are invited to participate in these tests.

Interface to Incident & Crisis Management

An Incident and Crisis Management process is in place to facilitate the coordinated and rapid reaction to an incident/crisis in a controlled and effective manner, aiming to contain and resolve incidents, minimise business and market impact and return swiftly to normal business activities.

Incident managers are appointed as single points of contact in their respective business areas to support in case of incidents and disruptions. This also ensures the proper escalation up to the Executive Board and Executive Committee levels.

An alert system is used to classify incidents and disruptions according to colour codes based on business impact. The system ensures an adequate response to incidents and crises, including the potential activation of business continuity plans and timely notification of relevant internal and external parties, including:

- Communication to participants
- Communication with external suppliers, other FMIs
- Communication to the market, as applicable
- Communication to regulators, as applicable

Secondary site

Business and IT operations

Clearstream's business operations are distributed across several processing global sites, including Luxembourg, Frankfurt, Cork, Singapore and Prague. Geographical distance between the mentioned operational hubs ensures diversity in terms of risk profile among processing sites and enables risk mitigation. Processing sites are fully equipped in terms of capabilities, functionalities, staffing arrangements and operational at any time, to ensure that the required RTO can be met in case of incident or crisis.

In addition, in Luxembourg, Cork and Frankfurt, backup facilities provide alternative dedicated office space for Clearstream mission-critical units in the event their normal office location would become unavailable. Like the main processing sites, the backup locations are fully equipped in terms of capabilities, functionalities, staffing arrangements and operational at any time, to ensure that the required RTO can be met in case of an incident or crisis.

Data centres (DCs)

The systems architecture is designed to ensure high availability requirements. The systems infrastructure is duplicated between two distant data centres. Components such as network communications, servers and storage are running in parallel in the two centres. Core systems are clustered and load-balanced between the two centres to allow quick take-over in case of failure. Production data is synchronously mirrored in real-time between the two centres, ensuring the preservation, online availability and integrity of transaction data following a disruption without data loss. In addition, data can be restored from off-line data back-ups which are taken at different intervals during the production cycle and are duplicated on libraries located in both data centres.

Failover mechanisms ensure that no data is lost. In the event of one component becoming unavailable, the "remaining" data centre can cover workloads on a normal level. Data centre capacities and normal load usage are designed and dimensioned to handle full-load operations alone.

To further enhance the high availability, a progressive migration to Cloud services is ongoing. Regulatory compliance is fully ensured and aligned with supervisory authorities. Both in-region and out-of-region failover capabilities are in scope of the design and applied as required.

Review and testing

BCP testing

The implemented business continuity solutions are regularly tested to ensure effectiveness and functional effectiveness. Tests provide assurance that a real incident could be successfully managed and provide awareness and training to staff members involved in the execution of activities.

Clearstream has adopted a comprehensive BCM testing framework based on key principles and with ambitious BCM testing objectives in order to simulate real-life situations, in terms of definition of scope and scenarios, and to be comprehensive, in terms of coverage of critical resources, procedures and plans.

The test objectives are based on the following criteria:

- Functional effectiveness: validate that arrangements are technically functioning
- Execution ability: ensure that staff are familiar and knowledgeable in the execution of plans and procedures
- Recovery time: confirm that plans and procedures can be executed within the defined recovery time objective

BCPs are tested on a regular basis, at least annually, either announced or unannounced to the participants to provide best possible assurance of the BCM preparedness.

As BCP tests are conducted during normal business hours, in the live production environment to be as close as possible to real life, participants, external suppliers and other FMIs are always indirectly participating in the BCM tests.

Examples of tests which are conducted:

- Workspace unavailability tests: simulate the loss of one building or location and require the relocation of staff to the secondary site or activation of business transfer plans to other Clearstream locations
- Staff unavailability tests: simulate the loss of all staff in one location and require the transfer of activities to staff of units in other Clearstream locations

The Incident & Crisis Management process is also tested as part of major/large-scale tests to ensure effectiveness of the end-to-end communication and recovery process.

Test results are consolidated as part of BCM test reports which are provided to key stakeholders.

Review and continuous improvement

CEU annually checks the business continuity preparedness of the linked FMIs (agent banks) by collecting information on their business continuity policies, planning and infrastructure including descriptions of the incident and crisis management, training, awareness, testing and pandemic preparedness. The business continuity and disaster recovery plans of the CSDs and/or agent banks are also reviewed as part of the due diligence process.

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 CEU's own operations

Potential risks caused by key participants are mainly related to operational problems of the key participants themselves and have no direct and significant impact on CEU. Nevertheless, this may pose risks to their counterparts and subsequently pose risks to CEU's settlement systems' efficiency. To appropriately identify, monitor, manage and report on the key participants' risks, CEU has implemented a key participant procedure that primarily focuses on:

- Identification of key participants and their related material dependencies
- Periodic enhanced key participant due diligence reviews (which assess key participants' risk control and management capacities to address and manage fraud, cyber, information security, business continuity, disaster recovery, infrastructure technology and application system risk elements)
- Monitoring potential key participant operational risk exposures and assuring appropriate mitigation measures

- Ensuring that CEU's key participants (as well as their underlying clients) have sufficient measures in place to properly manage and address the risks they pose to CEU (incl. CEU's key participants) and to thereby minimise to the maximum extent possible the potential risks posed to the CSD, other participants and, thus, the market as a whole

Additional measures include:

- Clear and stringent criteria to become a CEU participant; please refer to the [Becoming a Clearstream client](#) section – in particular, the Client Access and Acceptance Policy – on www.clearstream.com.
- Continuous monitoring of system usage and the global settlement efficiency level
- Detailed Market Link Guides documenting the established rules for participants, market practice across the Clearstream network and instruction specifications as well as potential risks (see the [Market Coverage](#) section of the Clearstream website)
- Choice between CEU proprietary connectivity or Swift
- Participant training support
- Clear and timely client announcements for system changes that affect participants
- Periodic enhanced due diligence on identified key participants

Risks posed by CEU to others

The CSD's interconnectedness to other FMIs (for example, stock exchanges and CCPs) makes substitution difficult, thereby increasing its interdependencies and subsequent potential operational and financial risks that could be posed to others.

Risk mitigating measures include due diligence reviews performed on the CSD by its participants and service providers to assess their risk and regulatory control framework capacities put in place to manage all related risks. A major element of these reviews is that CEU shares relevant information with other entities that allow them to adequately assess the risks posed to them by CEU.

Furthermore, CEU has implemented many layers of precaution and protection of its processes and services (regular tests of BCPs) and operates a comprehensive risk management framework built on established standards and best practices.

On an annual basis, Clearstream Risk Management publishes the [Pillar III disclosure report](#) on the company's current risk situation.

Outsourcing of critical operations

For the provision of products and services to its participants, CEU uses a system of mainly intra-Group outsourcing agreements to work effectively and efficiently. All entities within the Group are subject to the same requirements on reliability and contingency. The service delivery between two Clearstream entities is subject to a framework agreement and a formal service definition agreement (SDS). The latter also defines qualitative requirements (for example, service features, quality and performance standards and escalation mechanisms). The SDSs also contain KPIs to measure the quality of the respective service.

Any outsourcing is to be based on an initial analysis of the proposed outsourcing (including a pre-assessment, initial outsourcing risk assessment) ensuring compliance with at least current standards as well as fulfilling all legal obligations (that is, being compliant with existing regulation, ensuring banking secrecy, data protection requirements etc.).

Outsourced services and documentation are constantly monitored, and a regular risk assessment is done according to the Outsourcing Policy. The Outsourcing Coordinator, as part of the Central Outsourcing Management, discusses the initial score of the risk assessment with the other second line of defence functions, which are Compliance, Risk Management, ICT Risk Management, Data Protection, Business Continuity Management and Internal Audit (as third line of defence). After the review of each participant the Outsourcing Coordinator informs CEU's Executive Board of the results.

Apart from the Central Outsourcing Management, Clearstream Risk Management might in regular reviews identify several operational and business risks that could arise from service providers, as well as from other FMIs. The outsourced services are included in an appropriate manner in the operational risk management framework.

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.

Participation criteria and requirements

In accordance with Article 33 (1) CSDR, CEU's admission and participation criteria are publicly disclosed in the [Becoming a Clearstream client](#) section of its website. The criteria fulfil the requirements of the regulation to be transparent, objective, and non-discriminatory so as to ensure fair and open access to CEU with due regard to risks to financial stability and the orderliness of markets. The criteria are described in detail in CEU's [Client and Access Acceptance Policy](#) (CAAP) that can be found in said section of the company's website.

Participation criteria that restrict access are permitted only to the extent that their objective is to justifiably control a specified risk for CEU: pursuant to Article 33 (3) CSDR, CEU denies access only where duly justified based on a comprehensive risk assessment. Article 89 DR 2017/392 stipulates the criteria and risks on which basis CEU may refuse access to a requesting party such as a participant or another CSD¹¹.

Accordingly, CEU shall only consider legal risk (as defined by Article 89 (2) DR 2017/392), financial risk (as defined by Article 89 (7) DR 2017/392) and operational risk (as defined by Article 89 (11) DR 2017/392) when conducting the risk assessment. In addition, requirements from rules on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and financial sanctions are taken into account.

The regulatory requirements under CSDR and DR 2017/392 mentioned above are applicable to CEU following its authorisation pursuant to Article 16 CSDR on 21 January 2020.

Access to CEU and its settlement services is limited to participants as defined by Directive 98/26/EC but with the possibility of Member States of the European Union to designate further participants pursuant to Article 2 (f) Directive 98/26/EC. CEU considers access requests by applicants who are regulated financial institutions (credit institutions and investment firms), sovereign and supranational institutions (public authorities), and CCPs (trading venues have access rights to allow the trade feed generally to become settled via a CSD). CEU may however accept unregulated entities (other than sovereign and supranational institutions) as eligible for the limited purpose of receiving collateral from participants in the securities settlement system (SSS). Pursuant to the CAAP, CEU has defined criteria for persons who are prohibited from participating in the SSS (for example, natural persons, residents of any country that is subject of a "call to action" by the Financial Action Task Force (FATF), participation by persons causing CEU to breach any law, order, sanction or regulation). Lastly, CEU does not foresee indirect participation.

¹¹ Slightly different rules may apply for deciding on a request for access by an issuer, a CCP or a trading venue.

CEU's admission process

CEU ensures that the applicants are validly incorporated and existing under the relevant jurisdiction of incorporation and have the capacity to enter into agreements with CEU and to perform the activities provided therein.

In this respect, CEU requests from its participants to be provided with the documents listed in the [Becoming a Clearstream client](#) section of its website, in particular the [Client Application Form](#) and the [Account Application Form](#), along with other relevant [account opening forms](#), according to the required type of account. Details of account opening requirements and account maintenance procedures are provided in the chapter on client accounts in the [Client Handbook](#). For clients onboarded via the Clearstream Onboarding Tool, the information and document submission process is managed directly through integrated digital workflows which replace the conventional forms referenced above.

Applicants are required to confirm that they have read CEU's governing documents as available on the company's website, that they acknowledge such documents as amended from time to time, and that they accept to be bound by the terms and conditions set out in these governing documents. These documents shall also apply to all subsequent accounts to be opened upon an applicant's request.

In addition, applicants have to specify the connectivity media to use and the CEU facilities and services to which they want to subscribe. The respective application forms can be provided upon request and are available from the [Clearstream website](#).

CEU reserves the right to request additional information in relation to an applicant's institution as may be required under the applicable money laundering rules.

Applications from financial institutions are reviewed by CEU's credit and compliance departments and will be submitted to the company's Executive Board for final approval.

Clearstream will notify applicants in writing whether they have been accepted. The new participants then receive by standard mail the necessary information for using a CEU account. This includes the account number, passwords (where applicable) and relevant CEU publications.

CEU reserves the right not to accept an application.

Key consideration 2

An FMI's participation requirements 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.

Justification and rationale of participation criteria

CEU's participation criteria are geared towards avoiding undue legal, financial and operational risk for the safety and efficiency of the SSS CEU operates.

When assessing legal risks, CEU will take into account in particular the following criteria:

- Compliance with the legal requirements for participation in the SSS, including any required legal opinions or legal arrangements;
- Assurance with the rules on the confidentiality of the information provided through the SSS;

- Where a party is established in a third country, either of the following:
 - (i) Party is subject to a regulatory and supervisory framework comparable to the regulatory and supervisory framework that would be applicable to a party if it were established in the European Union;
 - (ii) Rules of the CSD concerning settlement finality referred to in Article 39 CSDR are not enforceable in the jurisdiction of a party.

When assessing financial risks following a request for access by a party, CEU will take into account whether said party holds sufficient financial resources to fulfil its contractual obligations towards CEU. The company will also assess the financial resources of the party in order to ensure that it has the capacity to contribute to a sustainable level of settlement efficiency. As to the financial conditions of a potential new participant, the applicant's credit standing is reviewed taking into account various qualitative and quantitative factors such as operating environment, liquidity, capitalisation, asset quality, profitability, financial support by the parent etc.

When assessing operational risks following a request for access, the following criteria are relevant:

- Operational capacity to participate in the SSS, including connectivity, communication and cyber risk considerations;
- Compliance with the risk management rules;
- Existence of business continuity policies or disaster recovery plans;
- Potential changes of its operations and risk management procedures in order to ensure the smooth functioning of the SSS.

As long as the applicant is meeting the criteria defined above, and once the application forms are validated internally, CEU's participants will have in principle access to the full range of services offered by CEU, under the specific terms of each service, subject to credit, operational and legal risk assessments that in some cases are product-specific. For example, a credit vote is given to assess the financial risk involved with a party requesting access and specific assessments are being regularly made for the granting of credit limits for participant relationship.

CEU cannot have relations with indirect participants. Indirect participants would be the underlying client of a participant of CEU whose contractual relation with and contractual obligations to is unique to the CEU participant. Such parties would therefore only benefit from the services CEU offers through CEU's participants, their own custodians, under the same terms. CEU endeavours to identify the participants' clients responsible for a significant proportion of transactions processed by the company and the participants' clients whose transactions, based on their volumes and values, are significant relative to the respective participants' risk management capacity.

CEU considers the risk that an actual or prospective participant may represent and ensures that applicants and participants meet appropriate legal, financial and operational requirements to allow them to fulfil their obligations.

Least restrictive access

The implementation of the above-mentioned access criteria are also geared towards having the least-restrictive impact on access that circumstances permit: (i) a non-regulated party may be granted access for the limited purpose of receiving collateral from participants (ii) enhanced legal, financial operational risk assessment are applied for certain products and a party may therefore be denied access to certain products only, while access to the SSS is generally granted. Additional risk assessments are performed when existing participants seek access to higher risk products. This is typically the case when an existing participant requests the opening of an additional account for a specific purpose. The whole relation will be considered in the decision to open or not such account. Such review process will trigger the review of the level of access restriction for the services offered, and the different requirements that may be imposed, or lifted, on the participant.

Essential required information on CEU's products and services is publicly available in [CEU's Client Handbook](#). The [Client Handbook for clients using the OneClearstream service](#) is also available on the company's website. For the 6-series activities, clients should refer to the [CBL Client Handbook](#).

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.

Monitoring compliance

CEU has the obligation to ensure that the documents, data and information regarding a business relationship are kept up to date at all times. According to section 10 (1) no. 5 Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz – GwG, German Anti-Money Laundering Act), CEU must continuously monitor the business relationship and the transactions carried out within this relationship. In scope of the ongoing monitoring CEU must ensure that the relevant documents, data or information are updated at appropriate intervals considering the level of money-laundering and terrorist financing risk. Therefore, a periodic review cycle applies to all participant relationships and accounts, and a prescribed set of documents are collected on an ongoing basis according to the Guideline on the Prevention of Money Laundering & Terrorist Financing. See also [Principle 19](#) for details on participant assessment measures and tools. The frequency of the review cycle depends on the risk classification of the participant.

Suspension and orderly exit

The termination of business relationship is stipulated in number VIII of the [GTCs](#) of CEU in line with regulatory requirements. Possible suspension of services to the participant is covered by numbers VI, XXII and XXVIII of the GTCs.

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

CEU has contractual relationships covering the delivery of its products and services, in particular settlement and custody services, uniquely with its direct participants. It therefore maintains only direct participation arrangements. CEU neither opens accounts for, nor recognises any indirect or tiered participants. Hence, no material risks to CEU can arise due to the absence of any tiered participation arrangements.

CEU owes a duty of redelivery or restitution of assets deposited by a direct participant uniquely to that participant or to its legal successor even if CEU is aware that its direct participant owes generally corresponding duties to its clients and that its direct participants routinely deposit securities which are ultimately owed to other intermediary firms and to investors.

CEU's direct participants are obliged under CEU's GTCs to segregate securities deposited for their own account (proprietary assets) from securities deposited on behalf of third parties (client assets). One of the key provisions of the arrangements governing the deposit of client assets is that each participant account opened in CEU's system must be allocated by its direct participant to one of three categories: (i) proprietary, (ii) client – segregated, or (iii) client – omnibus. Please refer to [Principle 11](#) for more details on the account categories.

On specific occasions, CEU has a right to collect information on its participant's clients as defined by number IV of the GTCs. CEU may request declarations and representations from a participant's client as to the purpose of an intended transaction and compliance with legal regulations.

CEU gathers information relating to assets deposited in client accounts through four primary mechanisms:

- Participant onboarding process;
- Opening of additional accounts of existing direct participants;
- Regular KYC reviews;
- Periodic key participant due diligence reviews.

The process is conducted by CEU's first line of defence and reviewed by the Compliance team. In the case of client segregated accounts, CEU seeks to identify the party to whom its direct participant owes the securities deposited on the account and records this information in its KYC file.

In the case of any direct participant depositing assets on client accounts whether in segregated or in omnibus form, CEU collects information relating to the regulatory, business and control arrangements that its direct participant has in place in order to service or to support third party business. CEU also obtains information on the geography, products and type of client that its direct participant supports through any client accounts held with CEU. CEU aims at updating this information on an annual basis.

CEU evaluates its risks arising from client accounts, in particular with regard to AML obligations and sanctions regulations. CEU's compliance risk assessment identifies the conduct of its direct participants' clients as a significant component of its overall operational risk. These risks are mitigated in the following manner:

- Upon onboarding and during regular KYC review, the competence and the capacity of participants depositing client assets are assessed, including the regulatory capacity of the direct participant to accept client assets and, in the case of omnibus accounts, to commingle them. That assessment includes a determination of whether the direct participant is AML regulated in a jurisdiction applying standards equivalent to those that apply in Germany. New client accounts – whether of existing or of new participants – are subject to the prior review of CEU's compliance officers and the approval of the Executive Board.
- To monitor client data and transactions, Deutsche Börse Group, including CEU, implemented a Group-wide sanctions screening system based on industry leading technology. Two times per day, the systems receive updates of sanctions lists to screen client and transaction data against the most recent available lists.
- The sanctions screening systems screen relevant information such as counterparties, issuers, securities, transaction data (settlement and payment instructions, corporate actions etc.), free-format messages and other against EU, U.S., UN and other applicable sanctions lists as well as internal lists.
- Further checks are performed via adverse media and politically exposed persons lists at the point of onboarding, during regular KYC reviews and regularly throughout CEU's relationship to its participants.
- A procedure defines roles and responsibilities of Compliance teams for 1st and 2nd level review of alerts created by the screening tool. Sanctions hits and related issues will be resolved in accordance with CEU's compliance policies and applicable laws and regulations. Risk mitigation measures may include the blocking of transactions, segregation of assets into dedicated sundry accounts and notification to the authorities.
- CEU implemented several quality assurance measures to ensure the effectiveness and efficiency of the sanctions screening systems such as Swift sanctions testing services, participation in a peer assessment, alert sampling activities, an independent audit function and others.
- CEU's screening strategy aims to ensure that the identity of such investor does not expose it to undue compliance risk.

In cases where the identity of the underlying client or information relating to the direct participant's client franchise in general triggers heightened AML, sanctions or related risk concerns, CEU may employ a number of specific mitigation strategies including requiring the direct participant to disclose additional information (including where not previously known, the identity of the underlying client or the beneficial owner), blocking the securities entitlements and disclosure to CEU's regulators, foreign authorities or CEU's sub-depositories or paying/transfer agents involved in the custody or administration of specific securities. CEU's contractual right to pursue and to enforce such mitigation strategies is derived from its GTCs.

Lastly, in respect of credit risk for CEU's credit business, the company does not permit assets deposited on client (as opposed to proprietary) accounts to be pledged as collateral to secure credit facilities enjoyed by its direct participants.

Risks to CEU

The principal risks, in particular from undisclosed beneficial owners, result from potential violations of regulations relating to the prevention of money laundering and terrorist financing, and in particular financial sanctions. Therefore, CEU continuously monitors all of its participants' transactions, including those resulting from underlying clients, with an IT-based compliance monitoring tool, which is supplemented in justified individual cases by manual checks. If the review identifies irregularities, CEU will obtain further clarification as it deems necessary. CEU may cease or temporarily suspend execution of a participant's instructions or the provision of other services (such as collection and payment of interest, dividends, repayments of capital or other amounts owed by the issuer to the participant), without notifying the participant in advance, if:

- Executing the instruction or providing another service violates applicable legal regulations relating to the prevention of money laundering and terrorist financing or financial sanctions (for example, of the UN, EU or U.S.A.);
- Executing the instruction or providing another service would, as a result of legal regulations relating to the prevention of money laundering and terrorist financing or financial sanctions, materially jeopardise the proper provision of CEU's services to its participants or, as a result of such requirements, put CEU's or its participants' assets at significant risk; or
- CEU's participant has not or has not yet provided the declarations and representations that CEU may request.

Key consideration 2

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

As a CSD, CEU is under the obligation to:

- Identify, monitor and manage the operational risks it faces from key participants and ensure that the key participants duly meet the CSD's operational requirements
- Identify, on an ongoing basis, material dependencies between a CEU participant and its clients that might affect CEU, and are responsible for a significant proportion of transactions processed through CEU's SSS or whose transactions, based on their volumes and values, are significant relative to the risk management capacity of the CEU participant

CEU's key participants and related material dependencies (underlying clients who constitute 10% or more of their settlement transaction activity) are identified as follows:

- Identification is driven by volumes and values of the transactional trades settled in CEU's SSS in accordance with the key participant regulatory requirements set out by CSDR;
- Identified key participants and material dependencies are requested to disclose to CEU their underlying clients who constitute 10% or more of their overall settlement transaction activity;
- Once identified as a CEU key participant, this status is held for twelve months;
- An annual recertification of the key participant status is performed.

In addition, CEU made its key participants aware of enhanced due diligence measures applicable to them (including their material dependencies) and of remediation measures to be assured on their side based on the key participant enhanced due diligence reviews performed. Further information is given in [key consideration 3](#).

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.

Where a client account is segregated, CEU's direct participant is required to disclose to CEU the identity of its underlying client, that is, the party for which the securities were deposited. The account name may or may not incorporate this disclosure at the discretion of CEU's direct participant.

Where a client account is opened in omnibus form, CEU's direct participant commingles the assets of several of its underlying clients. CEU requires that no single interest in a client omnibus account should exceed 25% of the total value of assets deposited on that account over time as represented by its direct participant. When a single interest does exceed that threshold, CEU requires its direct account holding participant to segregate the corresponding assets onto a client segregated account.

In line with CSDR, CEU's key participant procedure (see [key consideration 2](#)) ensures the identification on an ongoing basis of material dependencies between CEU participants and their clients that might affect it. This procedure also covers the performance of monitoring analyses and management of the operational risks that CEU's key participants may pose to its operations.

Analysis reviews

Clearstream's Risk Management function runs a process to identify CEU's key participants and related material dependencies in the SSS on an ongoing basis. Respective reports are assembled at the end of each quarter and cover settlement activities of the preceding six months. The identification process and the resulting reports are based on the following factors:

- Participants' transaction volumes and values
- Material dependencies between participants and the participants' clients, where the clients are known to CEU and that might affect CEU
- Their potential impact on other participants and CEU's SSS as a whole in the event of an operational problem affecting the smooth provision of services by CEU

In addition to the above reports, Risk Management may run ad hoc reports under stressed market conditions or on exceptional events (for instance, when a financial crisis occurs, high volatility is observed or geopolitical changes are expected).

Analysis to identify potential material dependencies of indirect participants is performed at the level of all participants of CEU, that means, by taking into account all settled volumes and values for all participants. Thus, CEU can also identify (i) participants' clients responsible for a significant proportion of transactions processed by CEU, and (ii) participants' clients whose transactions, based on their volumes and values, are significant relative to the respective participants' risk management capacity:

Upon identification of a key participant with material dependencies, Clearstream's Risk Management sends out a formal notification letter to the participants identified as CEU's key participants to duly inform them of their new status as CEU key participant as well as to request them to disclose their underlying clients (material dependencies). This disclosure targets primarily clients that represent a threshold of at least 10% or more of the overall volume/value of transactions processed by the legal entity. In this case, the identified CEU key participant is requested to provide details on those clients and confirm that appropriate measures have been imposed on them to ensure that (potential) operational risk related to the key participant's clients is adequately managed. In addition, an enhanced key participant due diligence review will be carried out.

Key participants' operational risk exposures (that means, operational incidents, issues, risk loss history and events) are reviewed for the purpose of assessing the evolutions in the CEU key participants' risk profiles. In this regard, measures are currently ongoing to create a dedicated CEU key participant operational risk scenario. The purpose is to ensure CEU derives a concise view of its key participants risk profile and can assure relevant mitigation measures to manage the key participant operational risks.

In addition, reconciliation breaks caused by CEU key participants are closely monitored. In the event of reconciliation breaks identified for CEU key participants, a potential provisioning allocation may be required.

Key consideration 4

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

As explained above no tiered participation arrangements are permissible at CEU. However, all participants are reviewed on a periodic basis (KYC review). Periodicity of these reviews depends on the risk classification of the participant:

High risk → review cycle: one year

Medium risk → review cycle: three years

Low risk → review cycle: five years

In addition, ad hoc reviews are performed, and mitigating measures are taken when and where appropriate. As an example, when it is detected that assets deposited by a direct participant and held in an omnibus account might expose CEU to the violation of financial sanctions, CEU can transfer the securities to a separate securities account opened for such participant. Such detection also leads to an ad hoc review of the participant and its arrangements for compliance with regulations in the area of financial sanctions.

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

CEU establishes links ("CSD Links") with one or more FMIs in accordance with the principles set out in CSDR, such as Article 48 of CSDR and Chapter XII of RTS 2017/392 (as defined under [Principle 1](#)). The identification, monitoring and management of the risks arising from a CSD link is addressed, in particular, by Article 48 (1) of CSDR, which requires all CSDs, before establishing a CSD link and on an ongoing basis, to cover "all potential sources of risk for themselves and for their participants arising from the CSD link and take appropriate measures to mitigate them".

Accordingly, CEU maintains implemented processes to identify, monitor and manage all potential sources of risk arising from new market links. These processes are embedded in its internal procedures, such as the Network Management Procedure, described in further detail below.

Initial assessment of (potential) link arrangements

Before opening a CSD link, CEU conducts a general assessment of the prospective link that is presented for assessment to the Clearstream Material Change Working Group (MCWG). This working group will then either make a positive recommendation or decline the proposal to develop this link. If the MCWG approves to move ahead with the link development, a full risk assessment process is coordinated by Network Management with input from various departments, for instance, Credit, Treasury and Operations.

During this full risk assessment, aspects like the following are covered:

- (i) Criteria on securities registration, ownership restrictions, reporting obligations and disclosure requirements
- (ii) Market assessment including legal (legal opinion), tax and regulatory issues as well as risks related to the market infrastructure (CSDs, stock exchanges, CCPs) and operational risks (use of Swift, business continuity)
- (iii) All appointed agents are subject to CEU's due diligence framework, which assesses their anti-money laundering controls, operational readiness, good reputation and financial soundness, as well as their ability to support CEU's settlement and asset servicing activities.

Ultimately, CEU's Executive Board is responsible for the approval of every new or enhanced link setup and/or appointment of a CSD/agent bank. If the risk assessment identifies significant weaknesses resulting from major risks in the local market that cannot be adequately mitigated and/or should no agent meet CEU's criteria, no link will be established with the market.

Network Management ensures that the relevant competent authorities of CEU in charge of its supervision are informed of the intention to establish a new CSD Link in line with CSDR. Accordingly, the new CSD Link is notified three months prior to the targeted implementation date and generally after the approval of the Executive Board.

Ongoing assessment of (existing) link arrangements

Risks from existing CSD Links are assessed through CEU 's continuous oversight of market developments in the areas of procedures, practices, regulations or other infrastructure related developments.

In addition to the annual due diligence visits (DDVs), CEU may choose to visit the receiving CSDs/agent banks at any time to review the relationship and ascertain that all governing documents remain relevant to the activities and regulations of the market.

Contractual documentation consisting of the legal main agreement and the operational agreements (service level agreement, SLA) are monitored on an ongoing basis. The main agreement is renewed in case of legal or regulatory changes, the SLA is renewed in case of new or enhanced processes.

The link arrangement and the legal framework are reviewed at least annually in accordance with Article 84 (1), par. (i) of RTS 2017/392.

CEU monitors the performance of its network of receiving CSDs and agent banks through a structured set of oversight and review processes. In line with the due diligence and ongoing monitoring obligations set out in Article 48 of CSDR, supplemented by the related Regulatory Technical Standards in DR (EU) 2017/392, CEU's Network Management (NM) function performs periodic assessments of each CSD link.

As part of CEU's due diligence framework, internal operations teams are requested on an annual basis to review and assess the quality of services received from each provider. The outcome of these internal assessments may be shared with the relevant CSD or agent operating the link.

CEU also maintains an incident reporting database to record and track deviations from expected procedures. These incident records, together with the results of the internal operational assessments, feed into the scheduled service reviews performed by the NM team.

In addition, CEU conducts ongoing monitoring of the creditworthiness of its network of receiving CSDs and agent banks. This credit assessment is performed by CEU's Credit department and complements CEU's CSDR-aligned due diligence framework.

Risks deriving from existing links are part of the annual risk review conducted in the frame of the DDVs. These are managed by NM in coordination with the Clearstream Risk Management function. Management of risks on links includes the following potential tasks:

- (i) Updates to contractual arrangements with existing linked CSDs and agent banks to emphasise their responsibility in relation to any risks identified
- (ii) Establishment of action plans with the linked CSDs and agent banks and subsequent follow-up to ensure any agreed actions are being undertaken. Such follow-up may be conducted via regular meetings/calls and results in a subsequent update of action plans showing the progress of each action.
- (iii) Ad hoc testing with CSDs and agent banks to ensure operating effectiveness of processes and related controls
- (iv) Change of agent bank
- (v) Creation and maintenance of internal procedures and processes to document the actions to be taken as part of the risk management of the linked CSDs and/or agent banks

In the event of any operational, legal, creditworthiness or regulatory changes or changes that affect the appointed linked CSDs and/or agent banks, the risk profile of every link is reviewed in the light of the relevant CPMI IOSCO Principles, among others.

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.

All types of links are contractually documented between CEU and the CSD and/or the agent bank and generally include the following:

The Link Agreement

For the description on the legal aspects of the CSD Links, please refer to [Principle 1](#). The CSD Links are governed by contractual arrangements subject to the law and rules of the receiving CSD.

- For **direct links**, the terms and conditions are set out in the CSD's rules, which are drafted in the form of standardised general terms and conditions governed by the law of the jurisdiction in which the receiving CSD is established.
- For **direct links operated by a local agent**, which contractual framework is composed by (i) the receiving CSD rules and (ii) the account operator agreement setting out the rights and obligations of the agent operating CEU's account with the receiving CSD. These contractual documents are generally governed by the laws chosen by and applicable to the receiving CSD and/or the agent.

Furthermore, the Link Agreement with the receiving CSD and/or agent bank identifies and clarifies:

- Eligible instruments and authorised parties
- Defined terms and procedures for settlement, safekeeping/recording and administration
- Required insurance coverage
- Establishing the receiving CSD's and/or agent bank's standard of care
- Liability of the receiving CSD and/or agent bank towards CEU
- Representation and warranties and confidentiality requirements
- Incorporation of service level agreement (SLA)

The legal opinion

Details on the legal opinions and their scope are available under [Principle 1](#).

The SLA

This document sets forth the expected action, reaction, deadline and communication format for each individual operational process. It specifies the operational procedures to follow including:

- Authorised instructions and deadlines with regard to settlement and asset servicing
- Expected actions and contingency action plans
- Reporting structures related to reconciliation, position management, exceptions with their resolution and inquiries
- Notification of market information related to custody operations

At the level of CEU's own books and records, CEU ensures full segregation between the accounts and financial instruments of its participants. Each participant's assets are held in separate accounts and remain fully segregated from CEU's own proprietary assets. CEU's platform allows, at all times, clear identification and separation of positions belonging to different participants.

At the level of the receiving CSD, CEU maintains a direct account in its own name. In accordance with MiFID II client asset protection requirements, CEU ensures that its proprietary assets are strictly segregated from the assets held for its clients in the books of the receiving CSD. This segregation is achieved through dedicated account structures at the receiving CSD that clearly differentiate CEU's own holdings from the securities held for the benefit of CEU's participants. As a result, the receiving CSD's legal and operational framework provides an enforceable and robust basis for the protection of client assets, thereby supporting the sound functioning of the link arrangement.

Further information on market practice for each of CEU's domestic links is available in comprehensive Market Profiles and Market Link Guides in the [Market Coverage](#) section of the Clearstream website.

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.

CEU performs an annual, structured credit assessment of each appointed depository and agent. This assessment follows a formal methodology based on a fixed evaluation grid and includes a detailed analysis of audited financial statements, liquidity and capital indicators, management structure, external credit ratings, operational performance, and the quality and safety of assets held. CEU applies its internal credit risk framework to derive an internal credit rating, supported by documented scorecards, analyst assessments, and management approval. The resulting internal rating forms the basis for setting and reviewing exposure limits and monitoring requirements.

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.

Provisional transfers of securities are not part of CEU's service offering. CEU processes securities movements only once finality has been achieved in the local market of the issuer CSD. Until finality is confirmed, securities received via a linked CSD or agent bank remain blocked and cannot be re-transferred or used for onward settlement. This prevents any credit or liquidity exposure that could arise from an unwinding of the underlying transaction.

In exceptional cases where a local market operates on the basis of provisional settlement and no alternative process exists, CEU applies additional controls, including:

- (i) Mandatory blocking of the securities pending finality,
- (ii) Close monitoring of the settlement status with the issuing CSD or agent bank, and
- (iii) Prior communication to participants through formal market documentation.

Any such cases are documented and subject to internal risk assessment and approval.

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.

CEU respects a strict procedure when setting up new links. This procedure includes, but is not limited to, risk, compliance and credit reviews, as well as external legal advice (legal opinion) and a strong contractual framework. Each step of the setup of a new link is reported and approved by senior management committees such as MCWG, CRC and CEU's Executive Board.

Please see [key considerations 1, 2 and 3](#) for more details.

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.

When establishing a link with an issuer CSD, CEU may use one of the following link models:

- **1. Direct link with an issuer CSD**
CEU may establish a direct connection with an issuer CSD. In such arrangements, CEU must comply with the terms and conditions of the issuer CSD, including the liability standards defined under the issuer CSD's applicable laws and regulations (see [Principle 2](#)).
- **2. Direct link supported by an intermediary providing ancillary services**
CEU may appoint an intermediary to deliver additional operational or administrative services that support the functioning of a direct link.

The intermediary's responsibilities and liability standards are defined in the applicable agency agreement. As a standard requirement, CEU requires the intermediary to assume liability for any loss, damage, or cost resulting from its negligence. CEU's framework for selecting, monitoring, and overseeing such intermediaries is described in [Principle 16, key consideration 1](#).

Annual review of issuer/receiving CSDs and agent banks

CEU reviews its issuer and receiving CSDs, as well as its agent banks (intermediaries supporting the operation of a link), at least on an annual basis. The review covers the following areas:

Creditworthiness

- AFME questionnaire and supporting documentation: The assessment of agent banks is based on the AFME questionnaire and related documentation. The analysis follows a fixed evaluation grid that is consistently applied to all agent banks.
- CSD Link Review Questionnaire: CSDs are assessed using the CSD Link Review Questionnaire. As with agent banks, CEU applies a fixed evaluation grid to ensure a consistent approach across all CSDs.

Contractual framework

CEU reviews the contractual arrangements in place with each CSD and agent bank to ensure they remain robust, up to date, and aligned with CEU's requirements.

Service level performance

Clearstream Operations evaluates the performance of each CSD and agent bank against the service levels defined in the applicable SLA.

If any issues, deficiencies, or service weaknesses are detected, CEU ensures close monitoring and follow-up until the CSD or agent bank has returned to the agreed level of service performance.

Key consideration 7

Before entering into a link with another CCP, a CCP should identify and manage the potential spillover 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 to CEU.

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 fulfil its obligations to its own participants at any time.

Not applicable to CEU.

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 to CEU.

Principle 21: Efficiency and effectiveness

An FMI should be efficient and effective in meeting the requirements of its participants and the markets it serves.

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.

To ensure that Clearstream Europe AG (CEU) meets the needs of its participants and the markets it serves, the company has adopted an active approach towards its participants by structuring their input in a number of ways. These include a series of industry surveys, organised senior executive sessions, specific participant validation during the product/service development cycle and one-to-one participant sessions during due diligence visits.

Furthermore, CEU works closely with the members of the User Committees established according to the EU Central Securities Depositories Regulation (CSDR). The committees shall advise CEU's Executive Board (EB) on key arrangements that impact its participants, including the products and services it offers to its participants via the securities settlement systems (SSSs) CASCADE and Creation as well as on service level. Please refer to [Principle 2, key consideration 7](#) for details.

CEU's product management teams engage with participants in order to determine which new products and services require development either in response to the changing market environment or in order to respond to specific participant needs. In addition, CEU assesses its product portfolio inventory and monitors competition on an ongoing basis. Thus, the company can anticipate participant needs. Getting in contact with the participants and obtaining their voice on the development of CEU's offering is an integral part of the company's product teams' activities. New products and services are announced to participants well in advance (in principle six months prior to implementation) to allow participants to thoroughly test new releases with a technical and/or operational impact.

Clearstream's Network Management team ensures that the services provided by the CSDs and agent banks appointed by CEU are continuously meeting Clearstream's and Clearstream participants' expectations. To this end, the team has set up key risk, and key performance, indicators to monitor Clearstream's intermediaries/custodians. In this respect, key risk indicators are monitored and reported regularly, and any deviations are tackled without delay.

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.

CEU's business strategy (referring to objectives and goals) is set out in detail in [Principle 2, key consideration 1](#). It is reviewed on a continuous basis and adapted according to the business conditions the company faces over time. Being part of Deutsche Börse Group, CEU's strategic goals have been guided by the Group-wide "Horizon 2026" strategy throughout 2025. From 2026 onward, CEU transitions to the new Group-wide "Leading the Transformation" strategy for 2026–2028 with a focus on driving structural growth, advancing market transformation themes, and strengthening its operating model. This will be underpinned by ensuring regulatory compliance and fostering effectiveness in sales and client services through innovation and operational excellence.

Furthermore, CEU defines its service levels and consequent goals and objectives in depository service level agreements (SLAs). These agreements reflect market standards and are the basis for operational procedures and publications of applicable operational processes to CEU participants. Minimum service levels are highly variable according to the market rules and time zones for the securities eligible for deposit and delivery within the CEU systems.

CEU's risk strategy is aligned to its business strategy and its goals of continuously developing new services, enhancing the efficiency of its operations and reducing overall processing costs. The risk strategy defines the risk appetite as a risk limitation, which protects and ensures continuity of operations. CEU's risk appetite framework constitutes the tools and concepts that are used to manage risks. The aim is to be able to monitor risks continuously and thereby manage risks according to the risk appetite. See [Principle 3](#) for details.

Key consideration 3

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

CEU has engaged in and works on the basis of a continuous improvement process and has established a very strict service level measurement discipline. The company measures KPIs including operational and service level indicators. These are regularly reported to CEU's EB – the most significant ones also to the User Committees – and constitute the basis for the continuous improvement of the service. The tools used for continuous improvement are the following:

- (i) Forum for structured, systematic and creative solution identification, including a post-claim analysis and identification of appropriate measures;
- (ii) Key performance indicators (KPIs): quantified, objective view on service delivery of operations and outsourced business activities, for example on effectiveness, efficiency, operational quality, and operational risk;
- (iii) Key risk indicators (KRIs): early warning system for operational risk, periodically collected and analyzed to observe the trend and, if necessary, initiate mitigating measures;
- (iv) KPI engine: data warehouse, linked to major production systems, enabling standard and ad hoc reporting and detailed data analysis;
- (v) Report on the performance of the settlement system and committed service level targets.

By applying the above tools, a systematic process is set up to ensure a comprehensive detection of quality deficits, leading to their resolution.

KPIs have been defined to measure adherence to the SLA specifications. CEU measures operational KPI straight-through processing target rates to ensure the monitoring of participant instruction processing at the highest possible system standard. The KPIs quantify different dimensions of the operational service delivery, mainly quality (for example error rates, degree of automation and turnaround times) including risk elements and capacity utilisation.

Some IT operations KPIs are also defined to measure business application's availability, response time and adherence to contracted internal and external deadlines. If the KPIs are risk-related, they are the basis for key risk indicators (KRIs), which are monitored by Risk Management on a monthly basis. In a continuous process, KPIs and KRIs are measured, analysed and reported to management. At least yearly, target reviews ensure adoption towards a changed market environment, participant demands or a changing internal focus.

Furthermore, CEU strives to provide products and services with utmost reliability. Thus, the company gives the highest importance to the resilience of its business aiming to safeguard it against incidents and disasters, as the unavailability of core processes and resources represents a substantial risk for CEU and potential systemic risk to the markets as a whole. Therefore, CEU aims to satisfy itself and the markets of its ability to continue to operate under adverse conditions or in the face of unexpected events or disasters. In case of business interruption, operations must be resumed within appropriate time scales primarily in order to:

Safeguard CEU from significant losses, maintain revenue generation and shareholder value;

Maintain participant confidence, market stability and liquidity and minimise systemic risk;

Maintain management control, fulfil contractual obligations and regulatory compliance.

The functions which are indispensable for the critical daily operations in view of the above objectives are called mission-critical and are designed and implemented in such a way that they can be resumed within a recovery time objective (RTO) of two hours following a disruptive incident, crisis or disaster. The RTO is the time period following a disruptive incident within which products, services or activities must be resumed or resources must be recovered.

In order to minimise the impact of unavailability of key resources, that is, information (electronic or other), IT systems and networks, workspace and facilities, staff and suppliers, CEU has implemented and maintains effective and efficient business continuity management (BCM) plans in line with its needs and regulatory requirements. The BCM plans specify how services, processes and resources will be reinstated to a predetermined level within pre-defined time scales after an incident or disaster. Thereby the RTO for mission-critical processes must be observed. The resilience and disaster tolerance of critical processes and resources is commensurate with the business impact and the prevailing risks.

BCM plans are tested or exercised regularly in the most realistic way, without causing unacceptable business impact, to ensure their effectiveness and viability and in order to provide assurance that a real incident could be successfully managed. All relevant staff are trained to be competent in the execution of incident and crisis management plans and business recovery procedures. To ensure that CEU is able to respond to an incident in a rapid, controlled and effective manner, an incident and crisis management process is in place for the timely detection, escalation and assessment of incidents and the prompt activation of the BCM plans.

Additionally, CEU implemented a default management process in order to weather the default of a major CEU participant in an orderly manner, even under stressed market conditions. For further details, please refer to [Principle 13](#).

The systems architecture is designed to satisfy high availability requirements. The systems infrastructure is duplicated between two distant data centers. Components such as network communications, servers and storage are running in parallel in the two centers. Core systems are clustered and load-balanced between the centers to allow quick take-over in case of failure. All data is synchronously mirrored in real-time between the two centers. For systems hosted in the Cloud, CEU deploys complete redundancy installations among three availability zones (AZs). This is complemented by the high availability of OpenShift container orchestration cluster technology¹² and database running in cluster constellations.

The design described above in combination with the RTO of two hours facilitates the completion of settlement by the end of the day also in extreme circumstances such as the full loss of one data center. The last system unavailability test, based on the scenario of the full loss of one data center or of the primary AZ, was conducted in October and November 2025, respectively. The availability of CEU's business critical applications was validated within the RTO period and the infrastructure's security was maintained at all times. Tests, outcomes and implemented solutions demonstrated the effectiveness of CEU's contingency measures and that activities can be successfully maintained. No material issues were identified during the test and identified improvements have been successfully addressed and resolved.

¹² OpenShift container orchestration cluster technology: an enterprise-grade Kubernetes platform by Red Hat. It automates the deployment, scaling, management and self-healing of containerized applications across a cluster, ensuring seamlessly high availability and load balancing.

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.

CEU fully endorses standardisation and has been leading in standards implementations. All connectivity channels are fully ISO 15022 (and ISO 20022 for investment funds) compliant, IP based, and in line with European Post Trade Forum (EPTF) Barrier 2 (former Giovannini barrier 1) on communication protocols as stipulated in the "Giovannini File Transfer Rulebook" of 2007.

In particular, instructions, be it for securities or cash, can be processed via CEU's suite of connectivity products as described below. All of these settlement services are fully STP compliant:

- **CASCADE:** CASCADE is a mainframe user-to-application (U2A) connectivity channel based on proven, up-to-date technology. The harmonised security and user management streamlines participants' access to a range of services. CASCADE is based on ISO 15022 and ISO 20022 message terminology.
- **CASCADE via Swift:** CASCADE is available via Swift. This solution is used by participants that have large transaction volumes and automated interfaces between their in-house back-office systems and CEU. In the vast majority of cases, for correctly formatted instructions, no manual intervention is required.
- **CASCADE via LIMA/File Transfer:** This service offers bi-directional high-volume data transfer, both ISO 15022 and 20022 messages as well as human readable messages. It can be seamlessly integrated with a participant's in-house systems and is fully automated, making it an ideal component in an STP environment using VPN with standard messaging technology. This solution is used by participants that have large transaction volumes and automated interfaces between their in-house back-office systems and CEU for their messages.
- **Xact Web Portal:** The Xact Web Portal is a screen based, user-to-application (U2A) connectivity channel based on proven, up-to-date portal technology. The harmonised security and user management streamlines participants' access to a range of services. Xact Web Portal is based on ISO 15022 and ISO 20022 message structure and terminology.
- **Xact File Transfer:** This solution offers bi-directional high-volume data transfer, both ISO 15022 and 20022 messages as well as human readable messages. It can be seamlessly integrated with a participant's in-house systems and is fully automated, making it an ideal component in an STP environment. Xact File Transfer can also be used via internet, virtual private networks (VPNs) or SwiftNet.
- **Xact via Swift:** ClearstreamXact is also available via Swift. This solution is preferred by participants that have large transaction volumes and automated interfaces between their in-house back-office systems and CEU. As CEU's processing is fully STP, in the vast majority of cases, for correctly formatted instructions, no manual intervention is required.

CEU's settlement services are fully STP compliant.

From a global ISO perspective, CEU is a liaison institution to the Securities Evaluation Group and the Registration Management Group.

When considering messaging standards, CEU has helped develop and has implemented ISO 15022 since its inception. CEU participates in the Maintenance Working Group. This body decides on the yearly evolution of the standard. The other main messaging norm for CEU's industry is ISO 20022. In this area, CEU is already supporting ISO 20022 formats for SRD II Shareholder Identification Requests and will continue to expand its ISO 20022 offering according to the market standards and timelines for adoption of the new format. CEU also contributes to the yearly maintenance of this standard.

In terms of reference data standards, CEU has adopted all the main applicable ISO standards. Cross-border operation is at the heart of CEU's activity. The only way to make processes and systems work efficiently in such an environment is to use ISO standards and to mandate its providers to only use such standards. CEU applies the same communication standards for cross-border operations as for all other operational activities.

For CEU participants acting in ICP (Indirect Connected Participant) mode or DCP (Direct Connected Participant) mode, the following connectivity standards are implemented:

- CASCADE-Host and CASCADE-PC/HOB RD VPN (CASCADE Online)
- Xact File Transfer for the transmission of ISO 15022 and ISO 20022 messages to CEU
- Swift ISO 15022 messages to CEU via the Swift network
- ISO 15022 messages to CEU via MQ; Xact Web Portal (based on ISO 20022 standards and terminology)
- Xact via SwiftNet FINplus (also supports Shareholders Identification Disclosure Requests seev.045 and seev.046 in ISO 20022 format)

CEU participants acting in DCP mode can also communicate their instructions online via the web-based T2S GUI via Swift or the SIA-Colt network. In addition, they can send ISO 20022 messages to T2S via Swift or SIA-Colt.

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.

CEU's rules and procedures are set out in a series of documents as defined in [Principle 1](#) that enable participants to clearly identify and fully understand the risks and responsibilities of a participant in CEU's system. These documents are written in a comprehensive and clear manner to help participants understand the following:

- Fees applied to the services (the fees are published in the Fee Schedule)
- System design and operations (set out in the Client Handbook, the Market Link Guides and Connectivity Manuals)
- Participants' rights and obligations (stipulated in the GTCs and Special Conditions)
- Risks of participating in the system (described in the Client Handbook and complemented by the Market Link Guides, which provide market-specific legal, operational and custody information)

The documents are updated regularly and made available publicly to all current and prospective participants on the company's website www.clearstream.com.

The main indicators used by CEU to determine whether its rules and procedures are clear and comprehensive are the following:

- Participants' feedback: This is collected by relationship managers and the Client Services team. Based on the continuous flow of questions received from the participants, Clearstream assesses whether the current documentation provided to participants is sufficiently clear.
- Training offers: For new products or major changes to the system, relationship managers organise detailed information sessions to participants, via presentations and – if needed – also in meetings including respective product owners. During these sessions and/or via Client Services, CEU collects the comments and takes the necessary steps to rectify any perceived lack of understanding by the participants. Especially for connectivity products, CEU offers its participants dedicated training sessions, to which they can subscribe.¹³

¹³ In addition, material changes affecting market access arrangements are communicated to participants through announcements and reflected in the relevant Market Link Guides and operational documentation.

- GTCs: Section 307 (1) of the Bürgerliches Gesetzbuch (German Civil Code) requires GTCs to be clear and comprehensible. CEU's GTCs are the legal basis of the contractual relationship between CEU and its participants. The process for changing the company's GTCs is described in number II paragraphs 5 and 6 of the GTCs.
- Operational information review: Operational information is reviewed at least twice per year, whenever there is a major IT release bringing new and enhanced product and service functionalities. In addition, updates are implemented on an ad hoc basis, when participants (via Client Services) or internal control bodies request clarification. The same applies to Market Link Guides as well as Market Taxation Guides. These guides are additionally reviewed whenever material changes occur to market access arrangements, depositories, custodians, asset servicing providers, legal opinions or local market requirements.
- Webinars and tutorial videos: CEU publishes webinars and videos on its website in order to provide punctual and specific information on its products and services, as well as events organised by CEU.

Furthermore, an overview of CEU's default rules and related procedures, that is the company's [default management](#) process, is available online.

CEU also publishes general information on its business continuity framework in [Principle 17](#) and the [Association of Global Custodians \(AGC\) questionnaire](#).

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.

CEU's as well as the participants' contractual rights and obligations are clearly described in CEU's [General Terms and Conditions](#) (GTCs). These rules are publicly available on the company's website and can be downloaded in German (legally binding version) or English (convenience translation). The GTCs comprehensively consider CEU's role as the German central securities depository (CSD) in accordance with the Depotgesetz (German Securities Deposit Act) and CSDR, as a credit institution according to the provisions of the Kreditwesengesetz (German Banking Act) and as a recognised SSS. The main legal provisions relevant for the establishment and the operation of CEU are described under [Principle 1](#).

The descriptions and information provided in CEU's [Client Handbook](#) are technical rules according to number I of the company's GTCs. Such information can be consulted in conjunction with other CEU publications: [CASCADE Online Handbook](#) (CASCADE-Host interface) and [Connectivity Manuals](#). Moreover, CEU's announcements and other user manuals on connectivity, which contain further details concerning the use of CEU's services, are available on the company's website www.clearstream.com.

The connectivity manuals mentioned above provide details of the communication processes and messages supported by CEU, including the messages that participants may use for sending and processing instructions and the messages that CEU uses for reporting to participants (for details on these communication standards, see [Principle 22](#)).

Announcements give details, in English and, for the majority, in German, of changes in custody, clearing and settlement, changes in taxation, changes to fees and charges, and other information about changes in the markets, as well as CEU's products and services. The information given to participants in announcements is integrated, where applicable, into the Client Handbook, the Market Link Guides, the Market Taxation Guides and other reference documents as appropriate.

The Market Link Guides, presented in the [Market Coverage](#) section on the Clearstream website, give details of the links that have been established between CEU and domestic markets for which CEU offers settlement and custody services. Details include, among others, types of securities traded, types of link, depositories and agents, settlement rules and times, custody services and foreign exchange. In addition to information on operational arrangements, these Guides provide, in accordance with CSDR, information on the legal terms and conditions of the link arrangements including key elements of the local legislation such as recognition of nominee concept, nature of rights on the securities and impact of insolvency laws. The information is based on legal opinions issued by external law firms appointed by CEU. In this context, the company also provides information on the rules governing the finality of transfers of securities and cash (settlement finality).

Finally, CEU discloses information on its [governance](#) (composition of the management bodies, articles of association and [shareholding structure](#)), the [regulatory status](#), its [annual accounts](#), the [annual reports](#) of the ultimate holding company as well as its [ratings](#). This information helps participants to evaluate the risks regarding CEU's services, but also on the company's legal, regulatory, corporate, commercial and operational environment.

On a non-binding basis, CEU also provides [information related to tax regime](#) in connection with the services provided in relation to each market, highlighting that participants shall make their own tax assessment with respect to any aspects of the activities performed with CEU.

Additional information and documentation supporting participants in their risk assessment include:

- [Pillar III disclosure report](#)
- [Default management process](#)
- Business continuity management
- [CSDR Article 38 disclosure document](#)
- [AFME questionnaire](#)
- [AGC questionnaire](#)

Key consideration 3

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

The documentation made available through the website provides information related to, without limitation:

- Full range of activities and operations performed in CEU's environment
- Accounts (opening and closing of accounts), segregation of assets
- Type of assets, their eligibility and any circumstances that could affect their fungibility
- Execution of the instructions and communication means, including the key times and dates
- Liability regime (including the degree of discretion under which CEU exercises its rights, the exclusion of liability and the mitigating measures)
- Securities interest that CEU may have over the assets held in custody, such as the rights of pledge, retention and set off

- Record keeping and data protection regimes
- Settlement services, including finality and cancellation
- Cash financing services
- New issues and custody business services, including timelines, procedures and dates
- Fees applicable to the services
- Markets covered and the specificities of each market, including the local settlement rules and times
- Impact on participants' assets
- Conditions leading to a suspension or a termination of the services by CEU
- Termination of the services by the participant
- Disclosure requirements applicable in each market

Within its worldwide Client Services structure, CEU maintains a proactive relationship model. Participants are constantly informed about any changes and enhancements to CEU's systems via announcements on the company's website. Participants can also subscribe to receive email alerts of the publication of such announcements. The Client Services team is the general point of contact for daily operational queries. The Client Services Officers – available on a 24-hour basis through Clearstream's global office presence – provide a single point of entry for queries and issues. Participants are also given the possibility to perform a due diligence visit on CEU, which would allow them to increase their understanding of CEU's rules and procedures. CEU's relationship managers meet with participants in person or virtually on at least an annual basis. This provides an opportunity for participants to raise potential issues and feedback in general.

Participants are offered training on an ad hoc basis on subjects of their choice. Specific training is offered by the Client Connectivity team to help participants understand the technical setup in place and to ensure that they are fully aware of the functionalities available and their limitations, contributing to establishing risk awareness on CEU's products.

Relationship managers produce call reports of their interactions with participants. These reports form documentary evidence of the judgment of relationship managers, and, where relevant, will include elements demonstrating whether participants have a clear understanding of CEU's rules and procedures, as well as an appropriate understanding of risk. The reports would lead to further interaction on the part of the relationship manager or escalation within CEU where any of these elements were felt to be insufficient.

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.

Fees are published – in accordance with Article 34 (1) and (2) of CSDR – at the level of individual services in the [Fee Schedule](#) and are intended to help participants in understanding the fees applied to the services. The Fee Schedule also contains a statement on CEU's pricing policy and available 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.

CEU publishes its [self-assessment against the CPMI-IOSCO disclosure framework](#) on its website every two years. The company also publishes its monthly figures; please refer to the most recent publication in the Headlines section of the [Newsroom](#).

Principle 24: Disclosure of market data by trade repositories

A TR should provide timely and accurate data to relevant authorities and the public in line with their respective needs.

Not applicable to CEU.

Published by

Clearstream Europe AG
www.clearstream.com

Registered address

Clearstream Europe AG
Mergenthalerallee 61
65760 Eschborn
Germany

Document number: 7512