



# Corporate Governance & Business Ethics

Version 2.2 / Public / September 2022

# Contents

<b>1. About the Company</b>	<b>5</b>
1.1 General Information	5
1.2 Owner, Share Capital	5
1.3 Business Area	5
1.4 Corporate Strategy	6
1.4.1 The functional model of OeKB CSD	6
1.4.2 Transparent, standardised services	6
1.5 Organisational Structure	7
1.5.1 Organisation Chart	7
1.5.2 Employee involvement in the organisational structure	8
1.6 Supervisory Authorities	8
<b>2. Bodies of the Company</b>	<b>9</b>
2.1 Management Board	10
2.1.1 Management Board's Reports to the General Meeting	10
2.1.2 Management Board's Reports to the Supervisory Board	10
2.2 General Meeting	11
2.3 Supervisory Board	11
2.3.1 Risk Committee	12
2.3.2 Audit Committee	13
2.3.3 Remuneration Committee	14
<b>3. Key Personnel</b>	<b>15</b>
3.1 Key Personnel/CSDR	15
3.1.1 Chief Risk Officer (CRO)	15
3.1.2 Chief Compliance Officer (CCO)	16
3.1.3 Chief Technology Officer (CTO)	17
3.1.4 Head of Internal Audit	18
3.2 Key Personnel	19
<b>4. User Committee</b>	<b>20</b>
4.1 Responsibilities	20
4.2 Composition/Nomination of Members	20
4.3 Functioning	20

4.4	Rules of Procedure.....	20
<b>5.</b>	<b>Internal Audit.....</b>	<b>21</b>
<b>6.</b>	<b>Internal Control Mechanisms .....</b>	<b>23</b>
<b>7.</b>	<b>Risk Management .....</b>	<b>24</b>
<b>8.</b>	<b>Compliance Management System.....</b>	<b>26</b>
8.1	Complaint Mechanism.....	27
8.2	Conflicts of Interest and Corruption Prevention .....	27
8.3	Whistleblowing System.....	28
8.4	Prevention of Money Laundering and Terrorist Financing .....	29
8.5	Securities Compliance.....	29
8.6	Data Protection .....	29
8.7	Retention of Records.....	30
8.8	Outsourcing and Procurement of Services .....	30
<b>9.</b>	<b>Information Security Management System.....</b>	<b>32</b>
<b>10.</b>	<b>Process Management.....</b>	<b>33</b>
<b>11.</b>	<b>External Audit.....</b>	<b>35</b>
<b>12.</b>	<b>Publications.....</b>	<b>36</b>
<b>13.</b>	<b>Business Ethics .....</b>	<b>37</b>
13.1	Code of Conduct.....	37
13.2	Diversity, Communication Policy.....	37
13.3	Corporate Social Responsibility (CSR) Management .....	38

With its Corporate Governance and Business Ethics document, OeKB CSD GmbH (hereinafter referred to as OeKB CSD) ensures compliance with the organisational requirements pursuant to Chapter II Section 1 and the conduct of business rules pursuant to Chapter II Section 2 as laid down in Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 (hereinafter referred to as CSDR).

---

# 1. About the Company

---

## 1.1 General Information

OeKB CSD is a limited liability company established in the municipality of Vienna, with its registered address at Strauchgasse 1-3, 1010 Vienna (Austria). It is registered in the companies register of the Vienna Commercial Court with the number FN 428085 m.

OeKB CSD is a central securities depository (CSD) according to the EU Regulation (EU) No 909/2014.

OeKB CSD was granted the licence as a CSD according to Article 17 of Regulation (EU) No 909/2014 and received the permission to provide banking-type ancillary services according to Article 54 of Regulation (EU) No 909/2014 as well as a licence for “providing cash accounts to and accepting deposits from, participants in a securities settlement system and holders of securities accounts, within the meaning of point 1 of Annex I to Directive 2013/36/EU” according to Section C lit. a) of the Annex to Regulation (EU) No 909/2014 (CSDR) in conjunction with Article 1 para. 1 of the Austrian Banking Act (Bankwesengesetz, BWG, Federal Law Gazette No. 532/1993) by the Austrian Financial Market Authority (FMA) in the third quarter of 2018.

## 1.2 Owner, Share Capital

OeKB CSD is a 100% subsidiary of Oesterreichische Kontrollbank Aktiengesellschaft (hereinafter referred to as OeKB), registered in the companies register of the Vienna Commercial Court with the number FN 85749 b in the municipality of Vienna and the registered address at Am Hof 4, 1010 Vienna. OeKB made an initial capital contribution in the amount of EUR 20,000,000 (in words: twenty million euros), which represents the full share capital as well as 100% of OeKB CSD's shares.

## 1.3 Business Area

As central securities depository (CSD), OeKB CSD plays an important and central role in Austria's capital market. It is in charge of holding securities deposited with OeKB CSD in a central depository (collective clearing custody), which can be disposed of by way of instruction. It functions as a services hub for participants in the Austrian capital market:

- It accepts securities from capital-raising issuers for safekeeping and administration on the investors' behalf.
- It processes investors' instructions for the settlement of securities transactions they placed on the stock exchange and over the counter.

- It coordinates the issuers' payments to the investors to settle the investors' claims to the issuers as evidenced by the securities.

## **1.4 Corporate Strategy**

The corporate strategy defines

- The role and the mandate;
- The functional model of OeKB CSD;
- The objectives;
- The business model as well as
- Current measures taken to achieve the objectives.

### **1.4.1 The functional model of OeKB CSD**

A functional model serves as the foundation for the organisational structure as well as for the procedural structure, for corporate documentation, and for the legal relationships with customers (General Terms and Conditions, GTC) to comply with the framework set forth in Regulation (EU) No 909/2014 (CSDR), on the one hand, and to ensure the best possible organisation to fulfil the role and the mandate, on the other hand. In accordance with this model, OeKB CSD provides the following five functions as the minimum service level in the meaning of Article 32 para. 1 of the CSDR:

- Notary Service & Safekeeping;
- Securities Account Administration;
- Cash Account Administration;
- Settlement; and
- Asset Servicing.

In accordance with the objective defined in the corporate strategy of using at least 60% of human resources exclusively for operational services, the organisational structure focuses on the three groups of Notary Service & Safekeeping, Accounts & Settlement and Asset Servicing. These three groups render all operational services to be provided within the scope of OeKB CSD's five functions.

The operational tasks are assigned to these three groups in such a way that the services to be provided by each group are almost equal to the tasks of one or several functions in accordance with the functional model of OeKB CSD. This facilitates a clear delimitation of the areas of responsibility and is in line with the GTC structure and the customers' needs.

### **1.4.2 Transparent, standardised services**

In accordance with its corporate strategy, OeKB CSD does not offer any services that are to be agreed individually to market participants, but solely standardised/automated services based on internationally customary standardised business processes and interfaces.

Therefore, all legal relationships between OeKB CSD and its customers can be agreed in the form of the General Terms and Conditions of OeKB CSD (GTC) and its Annexes. The GTC are structured according to OeKB CSD's five functions and ensure separate access to the specific services rendered. The GTC are available on OeKB CSD's website [www.oekb-csd.at](http://www.oekb-csd.at).

The GTC and their annexes document

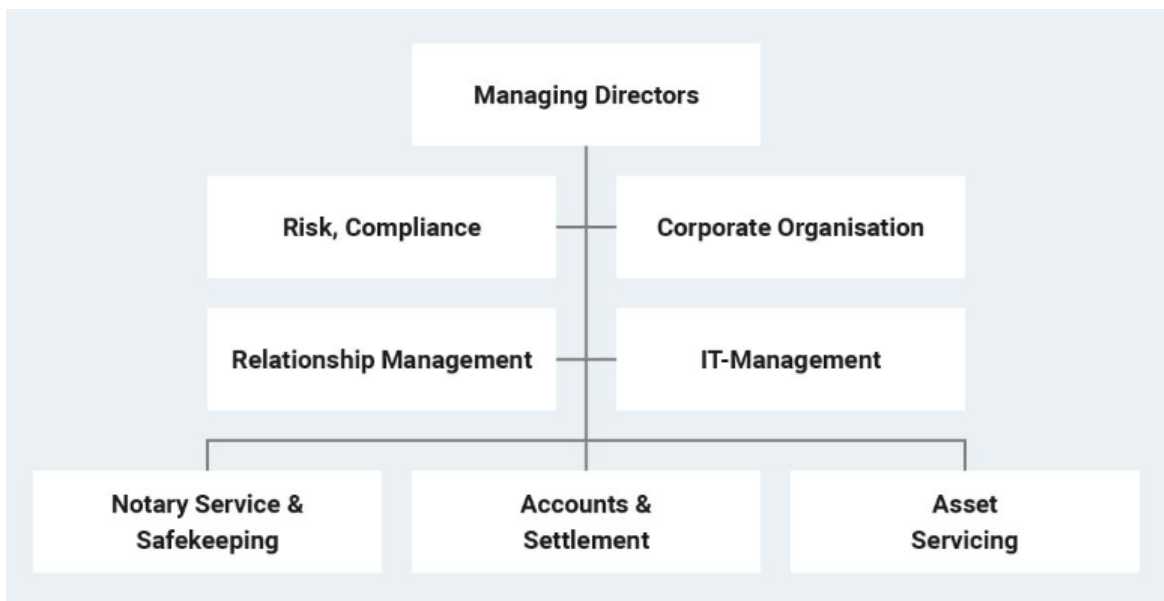
- The criteria for participating in the securities settlement system;
- The current list of participants in the securities settlement system (list of participants of SSS/securities account holders);
- The procedure regarding a suspension and the orderly exit of a participant from the securities settlement system who has violated or no longer meets the participation requirements;
- The key aspects of the procedure in the event of default of one of the participants in the securities settlement system including the circumstances under which measures may be taken, and including information as to who may take such measures and the scope of the potential measures to be taken, also with regard to own positions, resources and assets and those of the customers;
- All organisational and technical processes and interfaces between OeKB CSD and its customers; as well as;
- All fees and charges for each service and task rendered separately, including the discounts and rebates as well as the conditions for granting corresponding reductions (fees);

thus stipulating these transparently and exhaustively. Hence, there are no relevant agreements between OeKB CSD and its customers with regard to the services rendered by OeKB CSD apart from the GTC and their Annexes.

## 1.5 Organisational Structure

### 1.5.1 Organisation Chart

OeKB CSD has established an organisational structure and a continuously applied decision-making processes which ensure the documentation of reporting requirements and assigned functions and tasks (organisation charts, job descriptions, responsibilities, reporting lines).



### 1.5.2 Employee involvement in the organisational structure

The role of each OeKB CSD employee is defined by the function group to which they are assigned. The description of the function groups contains the job title, the objectives, the tasks, the specification of services, the job profile, and the salary range. OeKB CSD employees comply with the procedures as required to properly fulfil their tasks and are familiar with the corresponding written documents and process instructions. Training on the relevant statutory provisions takes place on a regular basis. Employees need to confirm that they acknowledge the provisions.

## 1.6 Supervisory Authorities

### Competent authorities

Pursuant to Article 11 CSDR, the Austrian Financial Market Authority (FMA) is the competent authority for OeKB CSD as central securities depository in the meaning of the CSDR and as a credit institution under the Austrian Banking Act.

For OeKB CSD as a system in the meaning of the Settlement Finality Act (Finalitätsgesetz, FinalitätsG, Austrian Federal Law Gazette I No. 123/1999), the Payment System Supervisory Authority located at the Oesterreichische Nationalbank (OeNB) is the competent authority.

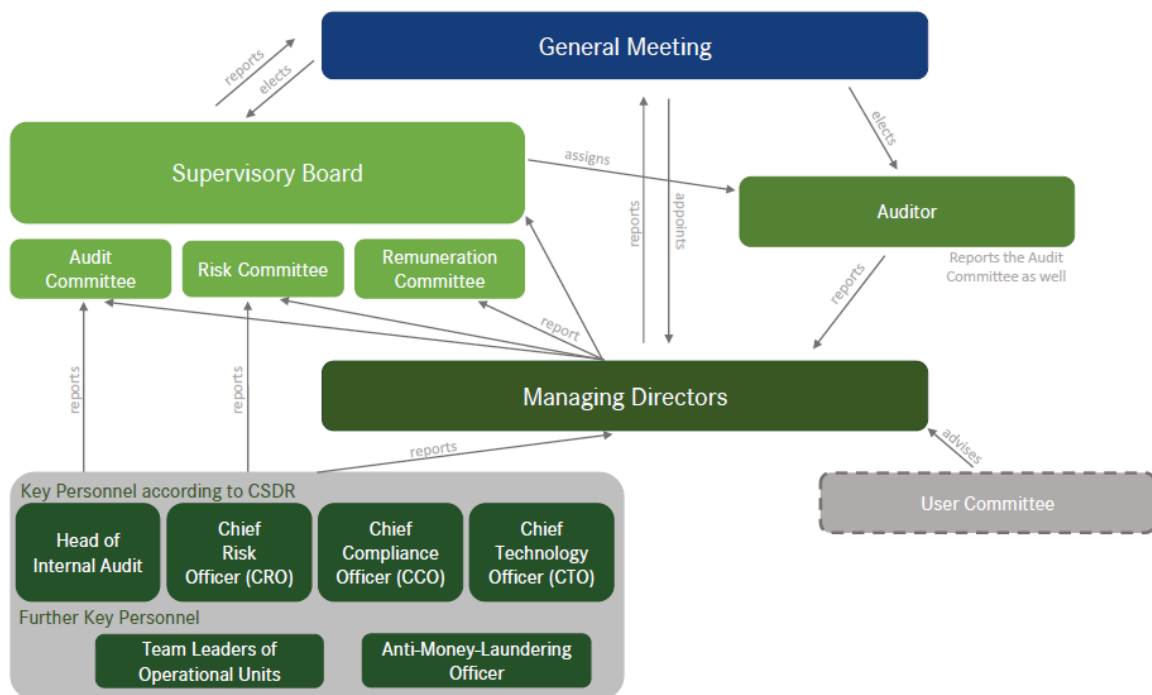
### Relevant authority

Pursuant to Article 12 CSDR, the OeNB is the relevant authority for OeKB CSD as central securities depository in the meaning of the CSDR.



## 2. Bodies of the Company

OeKB CSD's bodies are the Management Board of the Managing Directors, the General Meeting and the Supervisory Board.



The fit & proper policy lays down the selection strategy, the criteria for evaluating the appropriateness, the required documents and the procedure for ensuring the appropriateness as well as the re-evaluation, if necessary, of the Supervisory Board members and the Managing Directors.

As they are in charge of managing and monitoring the institution, specific requirements apply to the Managing Directors and the Supervisory Board members with respect to their technical and personal skills as well as their personal reliability. The required expertise, skills, and experience of every single person with regard to the collective requirements to the bodies' composition ensure that informed and substantiated decisions are made for the management of OeKB CSD based on a sound understanding of OeKB CSD's business, its risks and governance structure as well as on familiarity with the regulatory framework.

In combination with the corporate strategy, the risk policy & risk strategy as well as the rules of procedure of the Management Board and the Supervisory Board and other mechanisms and procedures, the fit & proper

policy is designed to ensure the prudent management of OeKB CSD and to increase risk management effectiveness.

## **2.1 Management Board**

OeKB CSD is managed by at least two, but no more than five managing directors (Job Profile MD, Fit & Proper Self Assessment). The company is represented jointly by two managing directors, or by one managing director and an authorised signatory holding joint power of attorney, or - consistent with statutory restrictions - by two authorised signatories holding joint power of attorney. Appointing authorised signatories holding individual power of attorney and conferring power of attorney to single individuals for the entire business operations is not permitted.

In its activities, the Management Board is bound by the resolutions of the General Meeting and obligated when exercising its powers to adhere to any and all restrictions laid down by law, the company's Articles of Association, the resolutions adopted by the General Meeting and the Supervisory Board as well as the rules of procedure for managing directors.

The Management Board is jointly responsible for managing OeKB CSD's business and shall consensually exercise all Management Board tasks. The Management Board shall meet or have conference calls whenever necessary, but usually once a week.

### **2.1.1 Management Board's Reports to the General Meeting**

Pursuant to Article 11 para. 1 of the Articles of Association, the Management Board shall, in the first five months of every financial year, prepare the financial statements and the management report for the preceding financial year and, after the auditor's audit, present them to the Supervisory Board and to the shareholders together with a proposal for the appropriation of profits.

In addition, at the OeKB CSD's sole shareholder's request, the managing directors shall promptly report to it about the company's affairs and, within the scope of its report to the General Meeting, inform it of any and all incidents and occurrences that could be of particular importance to the company.

### **2.1.2 Management Board's Reports to the Supervisory Board**

The Management Board shall report to the Supervisory Board on fundamental aspects regarding the future OeKB CSD business policy at least once a year and present a forecast of the anticipated development of net assets, financial position and profit or loss (annual report).

In addition, the managing directors shall, on a quarterly basis, report to the Supervisory Board on the course of business and the performance of the company as compared with the forecast and taking into consideration the future development (quarterly report).

The managing directors are obliged to promptly report to the Supervisory Board on material events, in particular if the company might be seriously harmed or if circumstances exist which may be significant to the company's profitability and liquidity (special report). If necessary, the General Meeting shall be convened.

## 2.2 General Meeting

The General Meeting is the highest-ranking body of OeKB CSD. OeKB is the sole shareholder of OeKB CSD. The document "Eigentümerstruktur der OeKB CSD" provides an overview of OeKB CSD's ownership structure. Resolutions which are reserved for the shareholders, as specified by law and the Articles of Association, shall be passed by the General Meeting.

Pursuant to the Articles of Association, the ordinary General Meeting shall take place annually within the first eight months of the financial year. Within these eight months, the shareholders shall make decisions with respect to the audit and approval of the financial statements, the use of the net profit or loss for the year, the formal approval of the activities of the managing directors and the Supervisory Board in the preceding financial year, and the appointment of the auditor.

Apart from the cases stipulated by law, an extraordinary General Meeting shall be convened whenever the interests of the company require such a meeting or when shareholders whose original contributions amount to at least one tenth of the share capital request the convening of such a meeting in writing, stating the purpose.

In addition to the matters reserved by law, the General Meeting is responsible in particular for

- Resolutions on the appropriation of profit or loss (net profit or loss for the year);
- The appointment of the auditor;
- The appointment and removal of the managing directors and the conclusion and termination of the managing directors' employment contracts;
- The formal approval of the managing directors' activities;
- Resolutions on the dissolution of the company and the appointment and removal of liquidators and their representation rights; and
- Resolutions on any amendments to the Articles of Association.

## 2.3 Supervisory Board

OeKB CSD's Supervisory Board consists of a minimum of three and a maximum of twelve adequate members, two of which shall be independent and able to guarantee that they exercise their functions on the Supervisory Board free from shareholders' interests and in the interest of the participants in OeKB CSD's securities settlement system. They shall not have any legal relationship with the company, the shareholders, or third parties that would hinder them from exercising their supervisory board activities independently.

The Supervisory Board shall monitor OeKB CSD's Management Board with respect to its legality, expediency, and efficiency. To this end, the managing directors shall submit annual, quarterly, and special reports to the Supervisory Board and are asked to report to the Supervisory Board of their own accord whenever necessary.

The Supervisory Board as a body can request a report on the company's affairs from the managing directors at any time.

The Supervisory Board shall be convened whenever this is necessary to perform its duties, but at least one meeting per quarter shall take place.

The principles, the framework, and the duties of the Supervisory Board are laid down in the Rules of Procedure for the Supervisory Board.

Pursuant to Article 8 para. 2 of the Articles of Association, the Management Board needs the Supervisory Board's consent for the following transactions and matters:

- The acquisition and sale of investments (Article 189a no. 2 of the Austrian Uniform Commercial Code (Unternehmensgesetzbuch, UGB) as well as the acquisition, sale, and closure of companies and plants;
- The acquisition, sale, and mortgaging of properties;
- The establishment and closure of branches or branch offices;
- Determining the annual budget (consisting of investment and finance plans, projections for the balance sheet and the income statement);
- Investments that, individually or in total within a financial year, exceed the amount of EUR 50,000;
- Issuing bonds, taking out loans and credit lines that, individually or in total within a financial year, exceed the amount of EUR 100,000;
- Adding as well as discontinuing lines of business;
- Defining general principles of business policy;
- Entering into work contracts and service contracts with third parties (outsourcing) that, individually or in total within a financial year, exceed the amount of EUR 50,000.

Article 48 of the Commission Delegated Regulation (EU) 2017/392 sets forth that OeKB CSD's Supervisory Board shall establish the following committees from amongst its members, whose responsibilities and powers are defined by the Supervisory Board as part of the regulatory requirements:

- A Risk Committee;
- An Audit Committee and
- A Remuneration Committee.

Each committee consists of the Chairperson of the Supervisory Board or his or her deputy and one further member to be appointed from among the members of the Supervisory Board. Definitions and responsibilities of the committees are laid down in the Rules of Procedure for the Supervisory Board.

### **2.3.1 Risk Committee**

The Risk Committee was established pursuant to Article 48 of the Commission Delegated Regulation (EU) No 2017/392 in accordance with the provisions laid down in Article 39d BWG.

The Risk Committee advises OeKB CSD's Supervisory Board and Management Board on the current and future risk appetite and oversees the implementation of the risk strategy.

The Risk Committee shall hold at least one meeting per financial year. The Chief Risk Officer (CRO) shall attend the meetings and report on the types of risk and the company's risk situation.

Consistent with the statutory provisions, the responsibilities of the Risk Committee include:

- Advising the Management Board on the company's current and future risk appetite and its risk strategy;
- Monitoring the implementation of the risk strategy in the context of controlling, monitoring, and limiting the risks affecting the company, the capital adequacy, and the liquidity;
- Verifying whether the company's pricing adequately takes the risk strategy into account and, if this is not the case, ordering the Management Board to prepare a plan with remedial measures, and approving it;
- Verifying whether the incentives offered by the remuneration scheme take into account the company's risk, capital, and liquidity structures as well as the probability and due date of revenues (the responsibilities of the Remuneration Committee notwithstanding).

### **2.3.2 Audit Committee**

The Audit Committee was established pursuant to Article 48 of the Commission Delegated Regulation (EU) No 2017/392 in accordance with the provisions laid down in Article 30g of the Austrian Limited Liability Company Act (Gesetz über Gesellschaften mit beschränkter Haftung, GmbHG) and Article 63a BWG.

The Audit Committee advises the Supervisory Board and the Management Board on checking and overseeing internal audit activities and on monitoring the effectiveness of the internal control system, the internal audit system and the risk management system.

The Audit Committee shall meet at least twice in a financial year.

Consistent with the statutory provisions, the responsibilities of the Audit Committee include:

- Checking and overseeing internal audit activities, monitoring the effectiveness of the company's internal control system, the internal audit system, and the risk management system as well as advising the Management Board in this context and reporting to it and to the Supervisory Board;
- Monitoring the company's financial reporting process and issuing recommendations or suggestions on ensuring its integrity;
- Monitoring the external audit;
- Verifying and monitoring the external/statutory auditor's independence, especially with regard to the additional services provided to the company;
- Auditing the financial statements and preparing their approval, auditing the suggested distribution of profits and the management report as well as reporting the audit results to the Supervisory Board;

- Delivering the report on the findings of the external audit to the Supervisory Board and a statement on how the external audit contributed to the reliability of financial reporting as well as on the Audit Committee's role in this regard;
- Conducting the procedure for selecting the external auditor, taking into account the adequacy of the fee as well as making a recommendation for the auditor's appointment to the Supervisory Board.

### **2.3.3 Remuneration Committee**

The Remuneration Committee was established pursuant to Article 48 of the Commission Delegated Regulation (EU) No 2017/392 in accordance with the provisions laid down in Articles 39b and 39c BWG.

The Remuneration Committee advises the Supervisory Board on the remuneration policy and the remuneration practices it oversees and advises the Management Board on remuneration matters.

The Remuneration Committee shall hold at least one meeting per financial year.

Consistent with the statutory provisions, the responsibilities of the Remuneration Committee include:

- Advising the Management Board on remuneration matters and on adopting resolutions on the subject of remuneration;
- Approving the general principles of the company's remuneration policy and remuneration practices;
- Overseeing and regularly monitoring the remuneration policy, the remuneration practices, and the incentive structures relevant to remuneration for the company's employees, in each case in the context of controlling, monitoring, and limiting the company's risks, capital adequacy, and liquidity, taking into account the long-term interests of the company's sole shareholder, investors, and employees as well as the economic interest in a functioning capital market and in a stable financial market;
- Responsibility for implementing the company's remuneration policy and remuneration practices it has approved;
- Reviewing the remuneration of the managing directors and of senior executives in the fields of risk management and compliance.

---

## 3. Key Personnel

---

### 3.1 Key Personnel/CSDR

Pursuant to the Commission Delegated Regulation (EU) No 2017/392, OeKB CSD shall have a Chief Risk Officer (CRO), a Chief Technology Officer (CTO), a Chief Compliance Officer (CCO), and an internal audit function. The key personnel shall be staffed with qualified persons. They are responsible for implementing at OeKB CSD the principles and procedures that were defined by the Management Board and the Supervisory Board.

The Management Board is in charge of staffing the key personnel. Each person nominated for such a position has to pass a corresponding fit & proper assessment. The Supervisory Board shall be notified of any appointment among key personnel.

OeKB CSD's key personnel are entitled at their own discretion to report to the Supervisory Board and its committees as well as to the Management Board on individual matters relating to their function at any time.

#### 3.1.1 Chief Risk Officer (CRO)

The responsibilities of the CRO are defined in the risk policy and risk strategy. Accordingly, the CRO is responsible for putting a risk management system (RMS) in place which meets the regulatory requirements and is suited to identify, measure, control, and manage all risks relevant to OeKB CSD.

He supports the Management Board in determining the risk policy and risk strategy, prepares the quarterly risk reports and participates in the meetings of the Risk Committee of the Supervisory Board in order to report to it pursuant to Article 39d para. 3 BWG.

OeKB CSD's Risk Management Committee (RMC) reports to the CRO and – based on the risk reports and the risk policy and risk strategy – prepares appropriate measures and procedures in cooperation with the CRO to achieve the risk management objectives. Such measures include establishing organisational framework conditions as well as designing the reporting process and developing business processes. The RMC meets on a quarterly basis or, if required, ad hoc in extraordinary meetings.

Together with OeKB CSD's Management Board, the CRO is responsible for overseeing the implementation of the guidelines and measures suggested by the RMC and adopted by the Management Board.

The tasks and the organisation of the RMC are specified in the Articles of Association for OeKB CSD's Risk Management Committee.

A detailed task description is provided in the job profile for the CRO.

## **Reports of the Chief Risk Officer (CRO)**

Apart from continuous communication between the Management Board and the CRO about the current risk situation, the CRO prepares the quarterly risk report of OeKB CSD based on the reports on the current risk situation and the events or near-events of default or loss that have occurred as documented by the group leaders (who also perform operational risk management). This risk report shall be integrated in OeKB CSD's quarterly report to the Supervisory Board.

Furthermore, the CRO reports directly to the Risk Committee of the Supervisory Board of OeKB CSD on any and all risk issues at least once a year.

### **3.1.2 Chief Compliance Officer (CCO)**

The tasks of the CCO are defined in the Compliance Management System (CMS). Accordingly, OeKB CSD has established a permanent and effective compliance function which operates independently from other functions of OeKB CSD. It is guaranteed that the compliance function has the necessary authority, resources, and expertise and has access to all relevant data and information. The competences granted to the compliance function of OeKB CSD and the requirements it has to meet take into account the nature, scope, and complexity of its operations as well as the nature and the range of the services and activities rendered in the course of these operations.

The CCO monitors, administers, and regularly assesses the adequacy and effectiveness of the provisions introduced as well as the measures taken by OeKB CSD to prevent and remedy any compliance deficiencies, and advises the Management Board with regard to the principles, strategies, and procedures it needs to define in cooperation with the Supervisory Board to ensure compliance with all statutory requirements relating to OeKB CSD, including the regulatory requirements for central securities depositories as stipulated by the CSDR and its implementing regulations.

Furthermore, the CCO advises and supports the persons responsible for OeKB CSD services and activities to comply with the legal provisions relevant to OeKB CSD, in particular with regard to the requirements of the CSDR and its implementing regulations.

The CCO regularly prepares reports on the compliance with the statutory requirements by OeKB CSD and its employees and defines an effective procedure for a course of action in case of compliance deficiencies. The CCO provides not only information and training but is also the point of contact for all operational departments of OeKB CSD to clarify legal questions.

In coordination with the Management Board the CCO is responsible for developing the methodology of the compliance management system, with the main task being to ensure adequate information within the entire company. All employees have a confidential information channel to the CCO. Monitoring compliance with the statutory requirements and corporate guidelines is not the CCO's task alone, but is incumbent upon all personnel bearing responsibility in the company. The CCO is in charge of improving the effectiveness of monitoring and the reliability of compliance with the requirements by implementing targeted measures.

A detailed task description is provided in the job profile for the CCO.



### **Reports of the Chief Compliance Officer (CCO)**

The CCO shall regularly report to the Management Board on compliance activities within the company and on compliance-relevant issues from the business environment. The CCO is the main advisor to the Management Board in all matters concerning compliance.

The CCO reports to the Management Board on compliance-relevant issues within OeKB CSD on a regular basis. A written compliance report shall be prepared and presented to the Supervisory Board at least once a year. This report shall include in particular information on compliance of OeKB CSD and its employees with the CSDR and the related Commission Delegated Regulations. Beyond that, the CCO may or shall report directly to the Supervisory Board of his own accord or at the Supervisory Board's request.

### **3.1.3 Chief Technology Officer (CTO)**

In accordance with Article 49 of the Commission Delegated Regulation (EU) No 2017/392, OeKB CSD has a Chief Technology Officer (CTO). This officer is responsible for the technical supervision and monitoring of the IT systems' operation as described in further detail below.

The CTO is responsible for controlling all IT tasks of OeKB CSD as well as for ensuring that the services are rendered by IT providers to OeKB CSD.

On top of that, the CTO of OeKB CSD is responsible for specifying the requirements for and monitoring the IT systems' operation by IT providers with the proviso that the operation of the IT systems

- Is designed to meet the operational requirements of OeKB CSD and to manage the risks that OeKB CSD is or may be exposed to; and
- Conforms with the requirements stipulated by the CSDR and its implementing regulations and that they are reliable and scalable to process additional information as required, even under tense market conditions.

In order to perform his duties, the CTO has all the necessary powers and resources and has access to all information relevant to his duties. When performing his core tasks, the CTO is independent from other functions of OeKB CSD.

A detailed task description is provided in the job profile for the CTO.

### **Reports of the Chief Technology Officer (CTO)**

The CTO shall have the IT systems checked at least once a year and shall perform a corresponding assessment. In this process, particular emphasis shall be put on information security, and the measures, principles, and procedures taken in this context shall be scrutinised and assessed. The CTO shall submit the results of this check and assessment to OeKB CSD's Management Board in a written, sufficiently detailed report.

Upon the Supervisory Board's request, the CTO shall report to the Supervisory Board on the observations made within the scope of technical supervision and monitoring of the IT systems' operation, if necessary, he shall make recommendations regarding procedures, provisions, and measures to be taken.

Furthermore, the CTO is entitled to report at his own discretion to the Supervisory Board or the Management Board on individual matters relating to the operation of the IT systems at any time.

#### **3.1.4 Head of Internal Audit**

The Head of the Internal Audit department is responsible for

- Planning audits;
- The performance and quality assurance of audits;
- Arranging special audits;
- Reporting to the Management Board, Supervisory Board, and Audit Committee; and
- The coordination with the external auditor.

The key personnel position of Head of Internal Audit is filled by an OeKB employee. This employee performs his tasks on the basis of an agreement between OeKB CSD and OeKB on the provision of resources for the performance of internal audit activities. Within OeKB, a separate organisational unit is in charge of the tasks of internal auditing pursuant to Article 42 BWG. Based on the agreement concluded with OeKB, OeKB CSD uses the option pursuant to Article 42 para. 6 BWG to utilise against payment the necessary human and material resources of the group's own organisational unit at OeKB for the performance of the activities of an internal audit. The agreement ensures that the ultimate responsibility, control, and oversight regarding matters of internal auditing of OeKB CSD remain with OeKB CSD, to the extent required by the CSDR. OeKB provides qualified staff who – when performing their activities for OeKB CSD – report solely to OeKB CSD's Management Board and do not take any instructions from OeKB with respect to internal auditing.

The Head of Internal Audit has direct and unrestricted access to the Chairperson of the Supervisory Board and the Audit Committee and communicates directly, i.e. he has the opportunity to hold confidential discussions without the presence of the Managing Directors.

The Internal Audit department exercises its tasks in an independent, unbiased, and impartial manner within the scope of the legal requirements and in doing so is guided by professional standards.

A detailed task description is provided in the job profile for the Head of Internal Audit.

#### **Reports of the Head of Internal Audit**

The Head of Internal Audit reports to the Management Board, usually in written form. In general, the written report consists of a cover sheet, a summary, and a detailed report.

Audit findings, especially those of a critical nature, must always be discussed with the responsible employee in order to give him or her the opportunity to comment. Such comments shall be included and highlighted in the audit report.

Based on the detailed report, the main audit areas and findings are discussed with the Management Board. In this final meeting, those audit findings are identified, which are to be reported by OeKB CSD to the User Committee. Members of the User Committee shall not be provided with any information that may give them a competitive advantage.

The Internal Audit department shall also report to the Chairperson of the Supervisory Board and the Audit Committee on a quarterly basis on the audit areas and significant findings based on the audits performed. The obligation to report ad hoc to the Management Board or the Chairperson of the Supervisory Board in case of extraordinary events remains unaffected. The Audit Committee shall be informed annually about the effectiveness of the company's internal control system, the internal audit system, and the risk management system.

Internal Audit shall report on the audit plan to the competent authority at least once a year.

### **3.2 Key Personnel**

According to the fit & proper policy of the OeKB Bank Group, the following functions are also defined as key personnel at OeKB CSD in terms of the fit & proper requirements:

- Team leaders of the operational units ("Board-1")
- Anti-Money-Laundering Officer (AML) according to Article 23 para. 3 of the Financial Market Money Laundering Act (Finanzmarkt-Geldwäschegesetz, FM-GwG, Federal Law Gazette I No. 118/2016)

---

## 4. User Committee

---

As required by the CSDR, OeKB CSD has established a User Committee representing the interests of securities account holders and issuers. In accordance with its rules of procedure, the User Committee shall advise the OeKB CSD Management Board in matters that are substantive for issuers and securities account holders. It consists of seven members, four of which are nominated by the securities account holders and three by the issuers of securities held in the accounts of OeKB CSD according to procedures specified in the General Terms and Conditions. More details on the rules governing the User Committee are provided in the General Terms and Conditions of OeKB CSD.

### 4.1 Responsibilities

The User Committee has the following responsibilities:

- advising OeKB CSD's Management Board in accordance with the User Committee's Rules of Procedure (Annex 31 of the General Terms and Conditions);
- e.g.: fundamental operational matters of the SSS (Securities Settlement System), criteria for the acceptance of securities, requirements for securities account holders, scope of services.

OeKB CSD's Management Board must inform the supervisory authority if it decides not to follow a recommendation made by the User Committee.

### 4.2 Composition/Nomination of Members

The four securities account holders and the three issuers with the largest transaction volume at OeKB CSD have the right to nominate members.

Nominated persons shall be personally reliable and shall have sufficient experience on the Austrian capital market as well as the required knowledge of the activities of central securities depositories. The term of the mandate is two years.

### 4.3 Functioning

The User Committee exercises its work independently and without any direct influence by the CSD Management Board. Its members shall participate in the meetings personally. The activities shall be exercised in the interest of the participants in the SSS, free of own interests. The members are required to disclose any conflicts of interest.

### 4.4 Rules of Procedure

The User Committee's Rules of Procedure shall be decided by OeKB CSDs Management Board and published as an annex to the General Terms and Conditions of OeKB CSD.

---

## 5. Internal Audit

---

The Internal Audit department is an independent control body established by law that reports directly to OeKB CSD's Management Board in organisational and disciplinary matters. Internal Audit performs continuous and comprehensive reviews of the legality, propriety, and expediency of business and operations throughout OeKB CSD.

The Organisational Guidelines for OeKB CSD's Internal Audit department are issued by OeKB CSD's Management Board and apply to Internal Audit within the scope of its activities.

The audit activity of the Internal Audit department shall be based on the statutory provisions and the relevant annual audit plans which need to be approved by the Supervisory Board or the Audit Committee. The areas required by law shall be audited at any rate. The audit plan has to be written once a year and shall be brought to the attention of the Management Board, of which confirmation is to be obtained, and approved and adopted by the Supervisory Board or the Audit Committee.

Within the scope of its activities, the Internal Audit department examines in particular:

- All legally prescribed audit areas;
- All operating and business activities of OeKB CSD;
- Bank-internal regulations (organisational guidelines, authority orders, and work instructions).

The audit plan by the Internal Audit department is risk-oriented using a standardised method and systematic analysis of the risk potential of all audit areas. The scope of the audit is determined on the basis of the risks and weaknesses that are already known or presumed. The frequency of audits depends mainly on the statutory requirements. Audit areas which are not covered by statutory requirements are audited at appropriate intervals depending on their risk level.

Irrespective of the audit plan, special audits may be carried out at any time. Adequate resources for special audits are set aside in the audit plan.

Internal Audit updates the audit map annually, where all audit areas and audit intervals are recorded. The audit plan is then based on this audit map.

In the audit report, Internal Audit distinguishes between "findings", accompanied by necessary "measures", and "recommendations". Findings are assigned to one of four risk classes according to the hazards and risks associated with the deficiency:

RK1 = low risk finding

RK2 = medium risk finding

RK3 = high risk finding

RK4 = significant finding according to BWG

The findings and measures presented by Internal Audit are identified separately in the report and recorded on the intranet. For each measure, a responsible person and an implementation date are agreed with the Management Board. The person responsible for the matter shall inform the Internal Audit department as soon as the decided measures have been completed.

Internal Audit will review the implementation of the adopted measures with regard to the implementation date and record it in a quarterly follow-up report.

Internal Audit also reports directly to the Chairperson of the Supervisory Board and the Audit Committee on a quarterly basis on the audit areas and findings resulting from audits carried out in risk classes 3 and 4.

---

## 6. Internal Control Mechanisms

---

The Internal Control System encompasses the principles, procedures and measures (rules) implemented at OeKB CSD, which are aimed at the organisational implementation of the decisions of the Management Board

- For ensuring the effectiveness and efficiency of the business activities (this also comprises the protection of assets, including the prevention and detection of misappropriation of assets);
- Regarding the propriety and reliability of internal and external accounting; as well as
- On compliance with the statutory provisions relevant for the company.

The guideline for the Internal Control System (ICS) defines all essential rules and measures for the ICS of OeKB CSD with the objective to establish the procedures for the

- Identification of ICS-relevant processes in accordance with the defined scoping criteria;
- Recording and evaluation of associated risks;
- Definition and documentation of appropriate controls for these risks;

and to determine any further activities/procedures required for this purpose. This ensures that the ICS is

- Complete;
- Logical and understandable;
- Set up efficiently;
- Actually followed in practice; and
- Integrated in existing risk management systems.

The ICS officer is responsible for the uniform documentation of the ICS, the regular scoping and updating of the documentation as well as the correct presentation of the ICS in the risk report. The Guideline for the Internal Control System (ICS) specifies the roles and responsibilities within the ICS (incl. those of the ICS officer).

---

## 7. Risk Management

---

Based on the business of OeKB CSD, the corporate strategy, and the regulatory framework, the Management Board of OeKB CSD, in coordination with the CRO of OeKB CSD, formulates the risk policy and risk strategy for OeKB CSD. The risk policy and risk strategy shall be reviewed annually and presented to the OeKB CSD Supervisory Board in the first quarter of each calendar year after discussion in the Risk Committee.

In this policy, the management of OeKB CSD sets out the

- Risk policy principles;
- Principles of risk assumption, measurement, and management (incl. risk appetite and risk acceptance level);
- Current risk-strategy orientation;
- Risk management governance framework (incl. risk management process and reporting); and
- Risk management organisation.

The following 4 maxims are defined in the risk policy and risk strategy:

- OeKB CSD avoids products/services that could jeopardise the business model, is in constant contact with the relevant stakeholders, and monitors the market environment as well as regulatory developments that may jeopardise the business model. Maxime: "We do the right thing".
- Processes and systems, including business continuity management, are set up and designed to avoid (reputational) damage that could jeopardise the business model. Maxime: "We are reliable".
- OeKB CSD attaches great importance to motivated, reliable, and well-trained employees who meet the high ethical standards of conduct (Code of Conduct). Maxime: "We are competent and act fairly".
- OeKB CSD acts exclusively within the framework of legal regulations and is compliant with the legal and regulatory requirements to which it is subject. Maxime: "We know, appreciate, and act within the existing legal framework".

The risk management principles defined in the risk policy and risk strategy serve as a guideline for the CRO and the Risk Management Committee (RMC) to formulate the Risk Management System (RMS), which comprises all guidelines, manuals, and documents relevant for the risk management of OeKB CSD and the standards and methods defined therein. The RMS fulfils the objective of identifying, measuring, managing, and controlling all risks relevant to OeKB CSD.

OeKB CSD defines risk acceptance levels for the individual risks documented in the risk map, taking into account the company's objectives, risk-bearing capacity and risk appetite. These risk acceptance levels are specified and controlled by Key Risk Indicators (KRI), which are defined in the risk map for each risk type. Responsibility for compliance with each KRI is assigned to the OeKB CSD functionaries responsible for the respective risks, which are documented in the risk map.

The risk management organisation of OeKB CSD meets the requirements of the Three Lines Model:



- The first line is the operational management. In addition to the Management Board, these are primarily the group leaders of the operations teams as well as the CTO. They identify, analyse, and evaluate risks and eliminate or reduce unacceptable risks through targeted measures.
- The second line defines the framework conditions for risk management in consultation with the Management Board, reviews the risks for their viability for OeKB CSD, and ensures the effectiveness of risk management by, for example, drawing up guidelines and procedural models or by monitoring and supporting the first line. This is also where the company-wide summary reporting of OeKB CSD's risks takes place. The members of the 2nd line are first of all the CRO, then the CCO, who is responsible for compliance with applicable legal requirements within the company, and the CISO.
- The third line is the Internal Audit as an independent body, which looks at OeKB CSD's risk management from an independent perspective and reviews and evaluates the effectiveness, internal control mechanisms as well as the work of the first two lines.

All documents relating to risk management can be accessed electronically by all OeKB CSD employees.

---

## 8. Compliance Management System

---

Compliance means adhering to laws, regulations, guidelines, and voluntary codes within the company. The Compliance Management System (CMS) serves to achieve and continuously ensure compliance with these binding rules. Thus, the CMS is understood to include all principles as well as organisational and operational measures aimed at ensuring that an organisation and its employees act in accordance with the rules.

The starting point of the CMS are the company's business activities and the regulatory framework derived from them. They define the minimum scope of the CMS.

The compliance culture significantly determines how compliance is perceived, accepted, and implemented in a company. Based on the regulatory framework and the compliance culture, compliance goals are set, for the pursuit of which it is necessary to establish a compliance organisation and set up a compliance management programme.

In order to achieve the practical implementation of the principles and measures taken within the framework of the CMS, these must be communicated to the employees accordingly and their application must be explained in training courses.

The regulatory framework and the company's business activities cannot be defined once and for all, but are subject to an evolutionary process. Continuous monitoring of regulatory developments and regular evaluation and adjustment of the principles and measures defined within the framework of the CMS ensure that the CMS remains effective and efficient as an instrument for ensuring compliance.

In the event that the occurrence of a compliance case is suspected, the CCO will evaluate whether the suspicion may turn out to be substantiated. Sanctions are in place and will be applied in the event of deliberate and culpable violations of laws, internal guidelines, or process instructions. The type of sanction, such as an admonition, caution, transfer, or (immediate) termination, depends on the severity of the rule violation. In any event (except in the case of termination or immediate termination), the employee concerned must undergo intensified personal training.

The scope of compliance at OeKB CSD can be defined as follows:

- **Business-specific compliance:** the business-specific regulatory framework of OeKB CSD results from its business activity as a central securities depository that provides banking-like ancillary services.
- **Topic-specific compliance:** in addition to the business-specific compliance and at a more detailed level, topics have developed that are a subset of the regulatory framework and thus of business-specific compliance. Due to their significance, their depth of detail, or the scope of the associated requirements, however, these topics are considered so essential that they are treated as separate compliance topics in common compliance practice.

Some areas of topic-specific compliance are described in more detail below:

## 8.1 Complaint Mechanism

Feedback on services and service quality is important to OeKB CSD in order to continue working successfully. Pursuant to Article 32 CSDR and Article 39e BWG, OeKB CSD has established a transparent and adequate procedure for processing complaints received from customers and business partners.

The complaint mechanism aims to identify, analyse, and remedy any recurring or potential legal or operational risks and to maintain customer satisfaction in spite of the occurrence of a negative episode. In this context, OeKB CSD follows the guidelines of the Joint Committee on Complaint Handling for Securities Trading (ESMA) and Banking (EBA).

In most cases it is possible to resolve any issues in direct consultation with the responsible customer relationship manager. Therefore, in the event of a complaint, the customer is encouraged to first contact the responsible account manager (specialist departments, Relationship Management). In principle, however, every complainant is free to contact the Complaints Office set up specifically for this purpose, even for the initial contact.

The Complaints Office serves as an ombudsman's office. It was established with the aim to give customers the opportunity to address their concerns to a "neutral" body, i.e. one that is not directly involved in day-to-day operations.

Generally, complaints can be made by telephone, email, or post. In addition, complaints to the Complaints Office can also be submitted via the feedback form on the website of OeKB CSD ([Link](#)).

Alternatively, customers of OeKB CSD can address their complaints to the Joint Conciliation Board of the Austrian Banking Industry (Gemeinsame Schlichtungsstelle der Österreichischen Kreditwirtschaft).

## 8.2 Conflicts of Interest and Corruption Prevention

### Conflicts of Interest

Conflicts of interest are situations in which the interests of employees may run contrary to OeKB CSD's interests and those of its customers or business partners. Conflicts of interest may stem from operational, organisational, or ethical circumstances or be due to close personal relationships between employees and business partners or their representatives, or between employees.

Accordingly, employees holding responsible positions, for instance, who are engaged in business matters involving customers and business partners of OeKB CSD (e.g. senior executives, holders of power of attorney, representatives, account managers) are allowed to have private orders exercised by customers and business partners they serve, only if it is not to their personal advantage. The respective employees of OeKB CSD are permitted to have such business relations only at arm's length conditions.

Any existing and potential conflicts of interest, particularly due to personal relationships, must – in the employee's own interest – be reported to the CCO and the Management Board. As far as allowed by law, they will make the necessary arrangements in the individual case to ensure that the conflicts of interest reported have no adverse effects on the employee and on the business activities of OeKB CSD.

As regards personal relationships at the workplace, employees must not be in a supervising, subordinate, or monitoring position vis-à-vis the person they are closely associated with.

The principles for dealing with conflicts of interest are described in a separate guideline (Conflicts of Interest Guideline). This guideline contains behavioural instructions on how to avoid and deal with conflicts of interest. The aim of this guideline is also to ensure that OeKB CSD's services are always provided in the best interest of its customers.

### Corruption Prevention

Even though the employees of OeKB CSD are not officeholders within the meaning of Article 74 of the Austrian Penal Code (Strafgesetzbuch; StGB), it seems appropriate, based on its central position in the Austrian capital market, that its employees comply with the more stringent provisions of the criminal law on corruption, which is applicable to officeholders.

In its Anti-Corruption Guideline, OeKB CSD has described how to deal with offering, granting, or promising advantages. As a general rule, benefits which - regardless of their value - may influence the decision(s) of the recipient are inadmissible and may not be granted, offered, or promised.

## 8.3 Whistleblowing System

Employees reporting any indications of misconduct represent an effective means of identifying and preventing it in the future. Pursuant to Article 65 para. 3 CSDR, Article 7 para. 1 of the CSD Enforcement Act (Zentralverwahrervollzugsgesetz, ZvVG, Federal Law Gazette I No. 69/2015), Article 99g para. 1 of the BWG and Article 159 para. 1 of the Stock Exchange Act (Börsegesetz 2018, BörseG, Federal Law Gazette No. 555/1989), OeKB CSD has therefore implemented a whistleblowing system, allowing each employee to report any breach or suspected breach of legal regulations as well as of internal guidelines.

If possible under the circumstances, whistleblowers are encouraged to report potential cases of misconduct to their immediate superiors or to topic managers as a first step. Reports can also be addressed to the CCO.

If this approach is not an option, employees can contact a dedicated law firm available for such reports. If an employee contacts the law firm with a report of potential violations, the role of the law firm is limited to that of a communication interface in which the law firm forwards the reported issue confidentially and in anonymised form to the Management Board of OeKB CSD.

If one of the Managing Directors of OeKB CSD is incriminated in the report, the law firm shall forward the reported issue to the other Managing Director of OeKB CSD not affected. If both Managing Directors of OeKB CSD are affected by the report, the law firm shall forward the report to the Chairperson of the Supervisory Board of OeKB CSD.

Whistleblowers shall not suffer any disadvantages, provided that the information they reported was given to the best of their knowledge and belief.

In addition to the whistleblowing system there are other authorities to which reports can be filed, such as the Financial Market Authority or the public prosecutor's office.

## 8.4 Prevention of Money Laundering and Terrorist Financing

OeKB CSD fulfils all requirements of the Austrian Financial Market Money Laundering Act (FM-GwG).

An Anti-Money Laundering Officer has been established and an Anti-Money Laundering Contact Person has been nominated, who is in charge of the AML agendas on site, coordinates matters with the AML Officer, and brings questions from the daily business to his attention. It is the AML Officer's task to write a process instruction and a guideline addressing the employees at OeKB CSD that contain precise rules of conduct and measures to be observed by the employees. These documents are updated annually or as needed.

A KYC process has been established. All customers of OeKB CSD are vetted when the business relationship is established and at regular intervals thereafter.

## 8.5 Securities Compliance

OeKB CSD's employees may have access to inside information within the scope of banking operations (Market Abuse Regulation Article 7 [MAR]). Any inside information received must not be used to gain a financial benefit for oneself or a third party, be it by acquisition or disposal, or recommendation of securities, or by passing on information to third parties (MAR, Article 8).

The employees of OeKB CSD have to disclose their securities transactions.

Insider information and compliance-relevant information must be reported to the Securities Compliance Officer.

Any abuse in this respect will have consequences under criminal law and civil service law.

All employees must – in addition to the statutory provisions – also adhere to the OeKB CSD compliance rules as defined in the Guideline on Securities Compliance of Employee's Securities Transactions.

## 8.6 Data Protection

OeKB CSD has a Data Privacy Guideline in place and supplementary instructions which govern the implementation of data privacy requirements.

The employees of OeKB CSD receive regular training on the requirements of data protection.

Compliance with the relevant laws and case law, the appropriateness of internal guidelines and instructions on data protection as well as the effectiveness of the organisational and operational structure are regularly reviewed and adjusted if necessary.

Based on the understanding of Art. 37 of the General Data Protection Regulation (GDPR), OeKB CSD has to appoint a Data Protection Officer (DPO). Considering it useful to take benefit from the expertise already available in data protection matters within the OeKB Bank Group, it was decided that OeKB AG would provide the DPO acting for OeKB CSD.

The responsibilities of the DPO of OeKB CSD are laid down by law in the GDPR and are further substantiated and supplemented in the Privacy Policy of the OeKB Bank Group and the Guideline of OeKB CSD on the Application of the Privacy Policy of the OeKB Bank Group, both as amended. He ascertains that the organisational and operational data protection structure of OeKB CSD is in accordance with the statutory provisions regarding data privacy applicable in Austria (Austrian Data Protection Act, Datenschutzgesetz, DSG and the GDPR, as amended) and the current case law in this regard. He is supported in his responsibilities by the Data Protection Coordinator at OeKB.

## **8.7 Retention of Records**

Records and data are stored (archived) in accordance with the Record Keeping Guideline. Thus, OeKB CSD ensures the long-term and timely storage of data and data carriers as well as their availability until expiry of a predefined retention period while maintaining their confidentiality and integrity pursuant to Article 29 CSDR.

## **8.8 Outsourcing and Procurement of Services**

In line with the corporate strategy, the comprehensive and targeted outsourcing of services, in spite of the considerable regulatory requirements laid down by the CSDR and the BWG, provides for comparatively low overheads of slightly more than 40% of human resources for positions in senior management, staff units, IT and administration departments within the company. Approximately 70% of the administrative effort account for the outsourcing of services, leaving only about 30% for personnel costs.

Services are purchased in a targeted manner and tasks are outsourced. In this context, OeKB CSD ensures the following:

- It retains the expertise and resources necessary for evaluating the quality of the outsourced services and the reliability of the service providers for supervising the service providers effectively, and for managing the risks associated with the outsourcing of services on an ongoing basis.
- OeKB CSD's responsibility is not delegated to the respective service provider by such agreements; rather, the legal relations of OeKB CSD with the participants in its Securities Settlement System (SSS) and the issuers remain unaltered, and OeKB CSD remains responsible to them for rendering its services.
- The agreements with the service providers ensure that OeKB CSD always has those means of monitoring and control at its disposal that are required for prudent and reliable risk and quality assurance management.
- OeKB CSD's rights and obligations are laid down in writing in the agreements with the service providers. They ensure that the outsourced services are permanently and consistently available to OeKB CSD to the respective extent required and that OeKB CSD can terminate these agreements without exception.

- Outsourcing of services does not prevent the exercise of supervisory and oversight functions, as on-site access of supervisory authorities is granted specifically in all the agreements to the largest possible extent.

For the outsourcing and procurement of IT services, the rules in the IT Outsourcing Guideline of OeKB CSD apply in addition.

---

## 9. Information Security Management System

---

The Information Security Framework defines strategies and rules to control, maintain, and continuously improve information security (availability, confidentiality, and integrity of information).

It describes the organisation, roles, responsibilities, competences, and associated processes and activities with regard to information security. It also defines the performance requirements regarding information security for 3rd party providers. The employees receive an awareness training on information security and current threats at least once per year.

The tasks of information security risk management are the identification, assessment, and treatment of risks to information security. This risk management process is defined in the risk policy and risk strategy. The results of this risk management process are recorded in the risk map and details are elaborated in the document "ICT Risks".

Measures taken by OeKB CSD to ensure ICT resilience and cyber security also form part of the information security management system. Also, an assessment of cyber security risks is carried out within the framework of IT and information security risk management.

The Information Security Quarterly Report is presented in the RMC and discussed with the Management Board to identify and mandate necessary actions.



---

## 10. Process Management

---

OeKB CSD is integrated into the overarching process management framework of the OeKB Bank Group. The framework aims at enabling all employees of the OeKB Bank Group to have a common understanding of process management, a structured, group-wide approach and a coordinated understanding of their roles. Process management at the OeKB Bank Group is therefore not to be seen merely as the documentation of information, but also calls on every employee to actively help shape his or her working environment. The process management framework includes in particular:

- The development and ongoing revision of processes;
- The modelling of processes; and
- The improvement and optimisation of processes.

To ensure end-to-end process responsibility and transparency, the responsibilities and roles of all parties involved are defined and standardised specifications are provided for process development and implementation in the OeKB Bank Group:

- The **Process Owner** is responsible for the goal-oriented, strategic control of the main process at process map level (main process level). The focus of his activities is both the target alignment of his own process with other processes and the selection of sustainable key figures for measuring the success of the process performance. He centrally coordinates all resources required for process control and execution. The role of Process Owner at OeKB CSD is performed by the Managing Directors.
- The **Process Manager** supports the Process Owner at process or sub-process level in the implementation of the process objectives and the operational execution of the process. In day-to-day business, he is often responsible for the operational management of the process. A Process Manager must be assigned to each process.
- The **Process Management Coordinator**, as a central role in OeKB CSD, supports and provides guidance to all other roles in process management. The responsibilities of the Process Management Coordinator include advising those responsible for process management on the fulfilment and implementation of their role tasks (especially process documentation), checking compliance with the group-wide process management methodology, and coordinating process interfaces.

The processes are divided into management processes, core processes, and support processes:

- **Management processes** include processes that support the strategic orientation. They form the framework for long-term corporate planning and control and have a significant influence on the core processes.

- **Core processes** affect the direct value creation based on the business model. They are processes that start with the customer's requirements and end with the fulfilment of the customer's requirements (end-to-end view). The core processes of OeKB CSD are based on its functional model.
- **Support processes** are needed to be able to deliver the value creation. The support processes ensure the smooth execution of the core processes based on the business model. They also generate customer benefits and contribute indirectly to value creation.

In the event of extensions or significant changes in the functional model (i.e. significant changes in the core processes), a structured impact assessment of the effects is required, based on the OeKB Bank Group's product introduction process (PEF). OeKB CSD defines its organisation-specific requirements for the product introduction process in its own checklist and appoints a PEF coordinator to ensure that the related analyses and tasks are carried out.

---

## 11. External Audit

---

As OeKB CSD is a medium-sized corporation within the meaning of Article 221 of the Austrian Commercial Code (UGB), it is subject to the obligation to have its financial statements audited in accordance with Article 268 UGB.

Based on the proposal of the established Audit Committee, the Supervisory Board submits a proposal to the General Meeting for the election of the auditor. Immediately after the General Meeting has elected the auditor, the remuneration of the auditor and any other significant parameters of his being commissioned to perform the audit are determined by the Supervisory Board by resolution, and based thereon the auditor will be commissioned by the Supervisory Board to carry out the audit. The chairperson of the Supervisory Board or, in his absence, his deputy, shall be responsible for this procedure.

---

## 12. Publications

---

OeKB CSD provides the following publicly available free information on its website at [www.oekb-csd.at](http://www.oekb-csd.at):

1. Information on its ownership structure, on its rules on corporate governance, also pertaining to its organisational structure and the core objectives and strategies, the key elements of the remuneration policy as well as fundamental financial information, including the most recent audited financial statements;
2. The rules of corporate governance and control, including the regulations applicable to OeKB CSD in its area of business;
3. Information on significant modifications to its rules on corporate governance, its objectives, strategies, key principles, and amendments to its applicable rules and procedures;
4. Customer information on securities account segregation;
5. Information on insolvency procedures of OeKB CSD;
6. Information on risks associated with the services provided by OeKB CSD.

---

## 13. Business Ethics

---

### 13.1 Code of Conduct

The Code of Conduct of the OeKB Bank Group describes our core values and standards for ethical business comportment. We expect all our employees to know and comply with them. Although the institutions of the OeKB bank group are not listed companies, they voluntarily orientate themselves along the standards of good and responsible corporate management according to the Austrian Corporate Governance Code.

The Code of Conduct is intended to serve as a guideline for us in our day-to-day business and in our dealings with internal and external stakeholders, supporting independent action and promoting an open, respectful, and responsible working atmosphere. The rules of conduct as described in the Code of Conduct provide an overview of these standards, on which we operate in different markets in various countries and regions and under changing conditions.

Any further details that may be required are set out in separate documents and are maintained by those responsible for the respective topics or by other competent personnel.

The Code of Conduct not only formulates our expectations towards ourselves, but also what we expect of others. We therefore refrain from doing business that violates the Code of Conduct and appreciate our stakeholders' acting according to comparable rules.

Every individual is responsible for compliance with the Code of Conduct in the context of business activities. In the event that a matter becomes known that violates our Code or poses a risk to the OeKB Bank Group, this shall be reported in accordance with our whistleblower system.

### 13.2 Diversity, Communication Policy

In terms of remuneration policy, great emphasis is put on gender equality. A person's gender has no influence on the individual career moves. Equal pay for equal work is a matter of course. The assessment of employees is based solely on professional and personal skills.

On the Supervisory Board, the Management Board and in the key positions, both men and women shall be represented with at least 40% each in total (cumulatively).

The communication policy is aimed at building and reinforcing trust between OeKB CSD and the stakeholders and at contributing to an understanding of OeKB CSD's tasks and positions.

### **13.3 Corporate Social Responsibility (CSR) Management**

CSR management goes far beyond compliance with mandatory statutory requirements, provisions and laws. The key principle is moral and social responsibility, which the respective organisation assumes on its own initiative. Essential characteristics are the continuous further development of the underlying principles, the documentation of measures and plans as well as the voluntary compliance with the defined principles.

OeKB CSD, as a 100% subsidiary of OeKB, is integrated in the CSR management of OeKB and has documented its measures in the corresponding report of the OeKB group.



