

Short-term Bond System

**in accordance with the Principles for Financial Market
Infrastructures (FMI)
in accordance with Key Considerations (KC)**

Drafted by: Petr Kocfelda
Methodology and Development of Payment Systems Division
Cash and Payment Systems Department

28 December 2018

1. Introduction

1.1. General Framework

The Committee on Payment and Settlement Systems (CPSS) and the International Organization of Securities Commissions (IOSCO) developed and published in April 2012 the *CPSS-IOSCO Report on the Principles for Financial Market Infrastructures* (hereinafter the “PFMI”). The PFMI provided new international standards for financial market infrastructures (FMIs), including payment systems (PSs) that are systemically important, central securities depositories (CSDs), securities settlement systems (SSSs), central counterparties (CCPs) and trade repositories (TRs). The PFMI also set forth five responsibilities of central banks, market regulators and other relevant authorities for FMIs as they relate to the regulation, supervision and oversight of FMIs.

The PFMI contain the *Disclosure Framework for Financial Market Infrastructures* (hereinafter the “Disclosure Framework”) and the *Assessment Methodology for the Principles for FMIs and the Responsibilities of Authorities* (hereinafter the “Assessment Methodology”), which aim to promote the observance of the principles and responsibilities set forth in the PFMI.

The Disclosure Framework serves as a key input to the Assessment Methodology. The Assessment Methodology provides guidance to assessors for evaluating observance of the 24 principles and five responsibilities set forth in the PFMI. The Disclosure Framework and Assessment Methodology are designed to promote greater transparency, objectivity and comparability of assessments of observance of the PFMI.

1.2. Framework for Settlement Systems Operated by Central Banks

The PFMI contain 24 principles for financial market infrastructures (FMIs), which are payment systems (PSs) that are systemically important, central securities depositories (CSDs), securities settlement systems (SSSs), central counterparties (CCPs) and trade repositories (TRs). Not all principles are applicable to all FMI. Principles 1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 21, 22 and 23 are applicable to important securities settlement systems.

In addition to this, the BIS Committee on Payments and Market Infrastructures (CPMI) published in August 2015 a document entitled “Application of Principles for Financial Market Infrastructures to Central Bank FMIs”, which states that the principles are applicable both to private sector financial infrastructures and to central bank financial infrastructures. Nevertheless, there are exceptions where the principles are applied differently to central bank infrastructures or they are not applicable to them, as central banks deal with the issue comprehensively as a part of their specifically central-banking activities. Specifically this concerns principle 2 – Governance Arrangements, Key Considerations 3 and 4, principle 3 – Framework for the Comprehensive Management of Risks, Key Consideration 4, principle 4 – Credit Risk, principle 5 – Security – Collateral, principle 6 – Margin, principle 13 – Participant Default Rules and Procedures, principle 15 – General Business Risk and principle 16 – Custody and Investment Risks.

Principles 1, 2, 3, 4, 8, 9, 11, 12, 13, 17, 18, 19, 20, 21, 22 and 23 can therefore be applied to the short-term bond system, which is an important securities settlement system and part of the central bank. This fact is taken into account in the assessment.

2. Objective of the Assessment

The assessor of the Short-term Bond System is the Financial Regulation and International Cooperation Department, Payments Regulation and Financial Innovations Division, Payments Regulation and Oversight Office.

The main information sources for an assessment of the Short-term Bond System were the documents stated in the annex to this assessment and ongoing consultations with the relevant system administrator.

The aim of an assessment is to ascertain whether the settlement Short-term Bond System corresponds to the internationally recognised PFMI standards issued by the Bank for International Settlements (BIS), the Committee on Payment and Settlement Systems (CPSS) and the Technical Committee of the International Organization of Securities Commissions (IOSCO) in April 2012.

An assessment is governed and structured in accordance with the Disclosure Framework and the Assessment Methodology, the aim of which is to support compliance with the principles and responsibilities stipulated in the PFMI.

A summary assessment of observance of the principles, including recommendations, is contained in part 4 of this document, a detailed evaluation report is contained in part 5 of this document.

3. Basic Information about Short-term Bond System

This section describes the Short-term Bond System (hereinafter the “SKD”), which is a systemically important securities settlement system in the Czech Republic.

The SKD is a system that is central records (a register) of book entry securities in accordance with **Article 33(2) of Act No. 6/1993 Coll., on the Czech National Bank, as amended**, and **Article 92(3) of Act No. 256/2004 Coll., on capital market undertakings, as amended**. The SKD is a settlement system for transactions in book entry securities maintained in the records in accordance with **Article 33(4) of Act No. 6/1993 Coll., on the Czech National Bank, as amended**. The SKD is a settlement system with irrevocability of settlement orders in accordance with **Act No. 256/2004 Coll., on capital market undertakings, as amended**.

The SKD rules are determined by the Czech National Bank (hereinafter the “CNB”) in accordance with **Article 85 and Article 92(3) of the Capital Market Undertakings Act, as amended**, and in accordance with **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**, the CNB is the operator of the SKD (the “Operator”).

The SKD rules set out the method of maintaining records and settling transactions in book entry securities (hereinafter “securities”) representing a right to the payment of the outstanding amount (bonds) in the Czech currency

- issued by the Czech Republic and with maturities of up to one year,
- issued by the CNB,
- issued by other issuers and with maturities of up to one year.

3.1. Basic Principles of SKD

The SKD is based on the following principles:

- The SKD functions as a CSD for short-term bonds with maturities of up to one year
- Real-time gross settlement, RTGS
- electronic connections between agents and the SKD
- the delivery versus payment principle (DVP) model 1 based on an on-line connection with the CERTIS payment system operated by the CNB
- settlement in central bank money
- finality of settlement at the end of operating hours on the day of settlement
- the option of requesting an intraday credit secured by securities in the SKD through the SKD
- the option of automatic return of an intraday credit
- a change to an intraday credit into an overnight credit
- transaction and system security.

3.2. Participation in SKD

The SKD rules stipulate:

- A contract on participation in the SKD is concluded by the CNB only with an agent, i.e. a

legal entity stated in Article 84(1) of the Capital Market Undertakings Act.

- A custodian is a legal entity with which the CNB has concluded a contract on a client account in the SKD. A contract on a client account in the SKD is concluded by the CNB only with an entity stated in Article 92(2) of the Capital Market Undertakings Act.
- A client is a legal entity or natural person with which the CNB concludes a contract on securities owner account in the SKD.

An agent can be, based on a contract on participation in the SKD, entitled to arrange for other participants – i.e. custodians and clients - electronic access to its asset accounts in the SKD and to obtain information that concerns them from the SKD.

Only a custodian can have one or more client accounts in the SKD. A client account is opened based on a contract on client account in the SKD.

Only a client may have one or multiple owner accounts in the SKD. An owner account is opened on the basis of a contract on a securities owner account in the SKD.

3.3. Transaction Types

- purchase and sale of securities
- repo transactions
- sell and buy transactions
- intraday credit
- transfers of securities
- pledging of securities
- exchange of securities

3.4. Description of SKD's Activities

The SKD ensures, in particular, keeping of records of securities by issuer and by owner, as well as records of SKD participants, primary sale of government bonds, CNB bonds and other short-term bonds within the framework of the SKD, execution of participants' instructions for the registration of facts relating to the securities within the SKD, settlement of securities transactions within the SKD, redemption of bonds and the pay-out of yields on them. Within the framework of the SKD, an option to use various auction algorithms when covering investors' orders in an auction is offered. The SKD gives banks access to intraday credit, which the CNB extends through the CERTIS system.

3.5. Accounting Day

At 08:00 the staff run Opening of accounting day, if **Primary sale** is planned for this accounting day, it is possible to select a specific issue or all issues that have Primary sale on that accounting day; an issue for Primary sale is stated in the written materials handed over to SBO, so that an issue can be registered.

Continuous processing starts at 08:30, if an **Issue matures** on that day, it is necessary to select the relevant maturing issue and run it; subsequently print or send electronically to the relevant agent of the issuer all summaries concerning the matured issue.

Throughout an accounting day the staff monitors **Continuous processing** and the statuses of all settlements.

At 17:30 the staff ends **Continuous processing** and creates the necessary summaries concerning the accounting day. It runs **Close of day**.

3.6. Measures Concerning Control of Credit and Liquidity Risk

Within the SKD, securities transfers - be they for consideration or without consideration - are settled for the clients and custodians on the basis of the instructions given by their agents. The settlement of securities transfers for consideration is executed by the SKD for the clients and custodians in conjunction with the CERTIS system (the CNB's interbank payment system) on the delivery versus payment principle. This involves the transfer of securities from the asset account of the client who is the seller, or the asset account of the custodian in which the seller's security is recorded, to the asset account of the client who is the buyer, or the asset account of the custodian in which the buyer's security will be recorded, and the payment of the agreed-upon purchase price by the buyer to the seller.

The securities settlement process starts with the blocking of the securities in the asset account of the client or custodian. On the basis of this blocking, an order to the CERTIS system (a "third party order") is automatically, without undue delay, created for the transfer of the respective amount from the interbank payment account of the buyer's agent, or the bank of the buyer's agent, with a mention of the respective money account of the agent, to the money account of the seller. The connection between the SKD and the CERTIS system is fully automated and the order is usually executed in a couple of minutes. Once the financial transfer has been completed, the blocked securities are transferred from the asset account in which the securities of the seller have been recorded until that moment, to the asset account in which the securities of the buyer will be recorded.

Overdrawing a securities asset account and debit balances on a securities asset account are not permitted.

3.7. Intraday Credit for Banks

One of the important functions of the SKD is to enable banks that are SKD clients to obtain interest-free intraday credit, which the CNB extends to them for transactions in the CERTIS system. Depending on the bank's activities, its intraday credit can be increased or decreased arbitrarily at any time between the opening of the SKD accounting day (8.30 a.m.) and the closing of the CERTIS accounting day (4 p.m.). When the bank's intraday credit is increased or repaid, the securities remain in the client's asset account. The client obtains the credit at his own instigation by issuing an instruction to have the securities switched from "free status" to the status intended for the intraday

credit (“K status”). Immediately thereafter, his intraday credit in the CERTIS system is increased. By switching the securities from K status to free status the client issues an instruction for the repayment of the intraday credit.

If the client fails to repay the intraday credit on the basis of his own instruction, at the closing of the CERTIS accounting day the SKD automatically repays the credit to the debit of the bank’s money account in the CERTIS system. If the balance in this account is not sufficient to cover the repayment of the intraday credit, instructions for a Lombard repo as a result of non-repayment of intraday credit (the first part and the second part) are automatically created. The first part of the instruction is created automatically and the respective transaction is settled immediately after the closing of the CERTIS accounting day. Based on this, the securities in K status are transferred to the asset account of the CNB. The second part of the transaction, with the settlement date on the subsequent accounting day, is created only after the CNB has completed the Lombard rate in the respective instruction, which remains in unfinished status until this happens. The bank's instructions and transactions relating to the Lombard repo as a result of non-repayment of intraday credit are listed in its Survey of Instructions and its Survey of Settlements. It can display their details, but it does not enter these instructions in the system. The transactions are settled solely on the basis of automatically generated instructions, which are completed by the CNB, and the instructions are not matched with the counterparty. An intraday credit can be drawn also against a pledge of securities entered in the CSD.

3.8. Setting of Charges

The CNB sets charges in connection with the actual costs of SKD operations.

3.9. Selected statistical data for 2015 - 2017

Year	2015	2016	2017
Total number of transactions	7,897	9,873	18,918
Total value of transactions (CZK ‘000,000,000)	29,749	38,556	125,617
Total value of issued securities (CZK ‘000,000,000)	3,129	2,061	9,411
Average daily number of transactions	29	39	76
Average daily nominal value of transactions in CZK ‘000,000,000	124	161	533

4. Summary Assessment of Observance of the Principles

An evaluation of the SKD in accordance with the PFMI principles was performed in ongoing fashion during 2018. It can be stated that, with three exceptions, the SKD complies with all the principles that apply to systematically important payment systems. A certain shortcoming is the fact that the SKD does not use internationally accepted communication procedures and standards, see the description below.

Principles 1, 2, 3, 4, 8, 9, 11, 12, 17, 18, 19, 20 and 23 are complied with entirely, there are no comments or other recommendations regarding them.

Principle 13 is complied with to a large extent:
Testing and assessment of its procedures in case of participant default is not performed in the SKD.

Principle 21 is complied with to a large extent:
The SKD does not have mechanisms for the regular review of its efficiency and effectiveness.

Principle 22 is not complied with.

Ratings summary

Rating category	Principle
Observed	1, 2, 3, 4, 8, 9, 11, 12, 17, 18, 19, 20, 23
Broadly observed	13, 21
Partly observed	0
Not observed	22
Not applicable	2 (Key Consideration 3 and 4), 3 (Key Consideration 4), 5, 6, 7, 10, 14, 15, 16, 24

Principles 7, 14 and 24 do not apply to settlement systems.

Principles 2 (Key Considerations 3 and 4), 3 (Key Consideration 4), 5, 6, 10, 15 and 16 are not relevant for the SKD.

Recommendations for SKD

Based on principle 13, it is recommended that testing and assessment of procedures in case of participant default is performed.

Term: in the course of 2019

Based on principle 21, it is recommended that a mechanism be established for the Short-term Bond System

regular assessment of the efficiency and effectiveness of the SKD.

Term: in the course of 2019

Based on principle 22, it is recommended that internationally accepted communication procedures and standards be created and used in the SKD.

Date: IVQ.2019

5. Questions by Key Considerations for the Principles for FMIs

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 and relevant jurisdictions

The SKD is a system that is central records (a register) of book entry securities in accordance with **Article 33(2) of Act No. 6/1993 Coll., on the Czech National Bank, as amended**, and **Article 92(3) of Act No. 256/2004 Coll., on capital market undertakings, as amended**. The SKD is a settlement system for transactions in book entry securities maintained in the records in accordance with **Article 33(4) of Act No. 6/1993 Coll., on the Czech National Bank, as amended**. The SKD is a settlement system with irrevocability of settlement orders in accordance with **Act No. 256/2004 Coll., on capital market undertakings, as amended**.

The SKD rules are determined by the Czech National Bank (hereinafter the “CNB”) in accordance with **Article 85 and Article 92(3) of the Capital Market Undertakings Act, as amended**, and in accordance with **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**, the CNB is the operator of the SKD (hereinafter the “operator”).

The SKD rules and contracts on participation in the SKD are governed by Czech law and are operated only in the Czech Republic.

Important aspects of activities are the irrevocability of settlement; the dematerialisation of securities; the provisions for DvP; settlement in central bank money; financial security – collateral.

A high degree of legal certainty is provided by contracts with SKD participants.

The dematerialisation and transfer of securities is set out by the SKD Rules, the electronic SKD system does not enable any other method of records of securities.

An agent is obligated to have an “agent’s money account”, either its own payment system account in the CERTIS payment system operated by the CNB or to have an account with a bank that has a payment system account. This account is stated in the contract on participation in the SKD. Payments for custodians and clients of an agent are, as a part of settlement and other transactions handled by the SKD, paid for from an agent’s money account stated in the contract on participation in the SKD.

In the event that the asset account of the transferor does not contain sufficient securities by the end of the set period on the day of settlement, the SKD will defer the relevant instructions for registration of transfer to the following accounting day, but no later than the end of the set hours of the fourth subsequent accounting day or the end of the set period of the accounting day one

Short-term Bond System

accounting day before the date of maturity of the securities transferred, whichever accounting day is earlier (hereinafter the “Extended Period”); an instruction for registration of transfer is then automatically cancelled. The transferor and the transferee are informed of this fact by their agents. During the extended period the transferor and the transferee can individually cancel settlement.

The moment of acceptance of an order for settlement, in the case of transactions that are not settled on the delivery versus payment principle, is understood to be the moment at which securities on an asset account are blocked for the purposes of transfer. The moment of acceptance of an order for settlement, in the case of transactions that are not settled on the delivery versus payment principle, is understood to be the moment at which a payment order is created and sent to the CERTIS payment system.

A settlement order cannot be rescinded from the moment of acceptance of the order for settlement.

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

The SKD’s rules, including the annexes containing sample contracts are assessed and commented on by the relevant CNB units. All comments and any discrepancies are dealt with or corrected. External entities do not participate in comment proceedings.

Rules, procedures and sample contracts are, after the end of comment proceedings, approved by the director of the Cash and Payment Systems Department.

Since the end of 1995, when the SKD was brought into operation, there has not been any breach of rules, procedures and contracts.

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.

SKD participants must be informed of every change to the Rules or their annexes and a reasonable period must also be set by which such activities must be adapted to a change to the SKD, or they can express their non-consent to the change and file notice of termination of a contract on participation in the SKD or a contract on asset account in the SKD. Information about changes to the Rules, their annexes and their updated text is published at the CNB’s website.

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

The SKD provides services only in the Czech Republic and is governed by the legal order of the Czech Republic.

The contracting parties that sign the relevant contracts undertake to resolve any disputes resulting from such contracts preferentially by negotiations at the level of their representatives who are authorised to conclude such contracts. If they do not manage to resolve a dispute in this way, the contracting parties agree that the relevant courts of the Czech Republic have the jurisdiction to hear

and decide disputes resulting from such contracts.

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.

The SKD provides services only in the Czech Republic and is governed by the legal order of the Czech Republic. There is therefore no risk of a conflict between legal standards.

Assessment of Principle 1: Observed

Recommendations and comments: 0

Principle 2: Governance Arrangements

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

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

The CNB's aims are stipulated in the Act on the CNB, in accordance with Article 2 of the Act on the CNB; the CNB cares for financial stability and the safe functioning of the financial system in the Czech Republic. The Act also imposes on the CNB the duty of helping to ensure the security, reliability and effectiveness of payment and settlement systems and helping to develop them. The CNB assesses its results regularly in the CNB annual report.

The aim of the SKD as such is to ensure the error-free performance of all functions, i.e. records of securities by their issuer, records of securities on asset accounts, records of SKD participants (hereinafter "Participants"), primary sales of securities as a part of the SKD, the execution of Participants' instructions to register facts concerning securities in the SKD, the settlement of securities transactions in the SKD, ensuring the maturity of securities and the payment of revenues on them.

The aims are achieved as standard.

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.

The SKD is a settlement system with irrevocability of settlement that is part of the CNB. The system for management and administration of the SKD, including the Bank Board, is included in the hierarchical structure of the CNB, which is publicly available at www.cnb.cz. Members of the Bank Board and the governor are appointed by the President of the Czech Republic in accordance with Act No. 6/1993 Coll., on the CNB. The basic internal regulation that defines the organisational arrangement of the CNB determines and sets out the principles of the internal governance arrangements of the CNB, determines the levels of management and powers of CNB managerial employees, defines the powers of CNB organisational units, the principles of their co-operation and communication between them is the CNB Organisational Rules. The Organisational Rules and amendments thereto are approved by the Bank Board. The CNB Organisational Rules are the CNB's basic internal regulation that is a binding initial document for the preparation of related internal regulations and managerial acts of the CNB.

At the same time, the CNB is the institution that has oversight of the financial market in the Czech Republic.

The CNB is the owner of the SKD. The Cash and Payment Systems Department is the administrator and also operator of the system. Operations are ensured specifically by the Short-term Bond System

Methodology and Development of Payment Systems Division, Payments Operation and Development Office. The Cash and Payment Systems Department issues the SKD Rules, is responsible for the methodology for concluding contracts with SKD Participants, for the design and development of the SKD and, in connection with the Information Systems Department, for the conclusion of contracts with SKD Participants. The Information Systems Department is responsible for security and the technical administration of the system, drafts the procedures for SKD recovery.

In the Financial Regulation and International Cooperation Department, Payments Regulation and Financial Innovations Division, is the Payments Regulation and Oversight Office, which is responsible for oversight in the SKD. A control function is also performed by the Internal Audit Department.

The functions of operator and oversight are therefore separate based on separate powers of the operating units.

The responsibilities of the SKD – CNB to SKD Participants are dealt with by contracts with SKD Participants.

The CNB has placed at its website detailed information about the SKD and its operation, including the SKD Rules. SKD Participants and the public have access to this information.

The SKD, as a part of the CNB, is subjected to an annual external audit. Inside the CNB it is subjected to internal audits. The output from the audit reports is documented and serves as one of the sources for acceptance of other measures concerning the risk management system. The output from external audit reports is publicly accessible.

For the purpose of discussing the needs of users, a users' committee is established in the SKD. The mandate of the users' committee, the system for its management and organisational procedures are publicly available at the CNB website. The users' committee arranges regular meetings and submits reports to the SKD's management.

The CNB issues the SKD Rules, which state information about the governance arrangements. Participants must be informed of every change to the Rules or their annexes and a reasonable period must also be set by which such activities must be adapted to a change to the SKD, or they can express their non-consent to the change and file notice of termination of a contract on participation in the SKD or a contract on asset account in the SKD. Information about changes to the Rules, their annexes and their updated text is published at the CNB's 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 conflicts of interests of members of the board of directors. The board should review both its overall performance and the performance of its individual board members regularly.

Roles and responsibilities of the board of directors – in the CNB's case the Bank Board

The CNB Organisational Rules stipulate the levels of management at the CNB, which are:

- The Bank Board, which is the top managerial level and runs the CNB as a collective body;

- Directors of departments, directors of independent departments and branch directors, who are the middle level of management;
- Directors of divisions in departments and directors of divisions at branches, who are the middle level of management;
- Office managers, who are the bottom level of management.

The Organisational Rules also describe in detail the principles, forms and tools of management, including the internal CNB control system. The roles and duties of the Bank Board are clearly defined in the Organisational Rules. The CNB website also contains the management system and organisational structure of the CNB, which make it clear who is responsible for the SKD's operation.

The Organisational Rules and information at the CNB's website are updated during every change.

Review of Performance

Every year the CNB publishes its operations and the results achieved, including an assessment of the functioning of the SKD system, in the CNB annual report.

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

The appointment of the members of the Bank Board is set out by the Constitution and the Act on the CNB. The dismissal of the members of the Bank Board is set out by the Act on the CNB. The act also defines the requirements that are placed on the members of the Bank Board.

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

Roles and responsibilities of management

Management's roles and aims are contained in CNB forecasts, the duties are clearly set out in the CNB Organisational Rules.

Experience, skills and integrity

Directors of departments, directors of independent departments, deputy directors of departments, directors of divisions in a department and directors of branches are placed in managerial positions after the prior approval of a proposal from the Human Resources Department by the Bank Board. When selecting managers, the Human Resources Department ensures that managerial employees have a clean criminal record and have sufficient experience and the mix of abilities necessary for the operation and management of the of risks in the SKD. In addition to this, with regard to the fact that the SKD operator is the central bank, the requirement of a clean criminal record is placed on all CNB employees.

If it is necessary to dismiss the management, the Bank Board dismisses an employee from his Short-term Bond System

managerial position, if an agreement on the option of dismissal and resigning from position has been concluded with such employees.

Office managers are authorised to manage an office in a written decision of a director of a department, independent department or branch who, when making a selection, takes into account their experience and abilities. These directors decide on an amendment to the extent of the authorisation of an office manager or the cancellation of the authorisation of an office manager.

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.

Risk management framework

The organizational framework for the management of assets and the management of risks concerning IS/IT is documented in ***CNB Instructions No. 32/2007, stipulating the security policy for information technology of the CNB***, and in the related ***Methodology Sheet of the Information Systems Department No. 720/9/2015 Procedure for Asset Management and Risk Management in IS/IT at the Czech National Bank***. The methodology sheet describes how to perform identification and assessment of information assets in information systems and information technology, how to perform a risk analysis, propose measures to eliminate such risks and determine the remaining risks. The output is then a "Security Profile" in the form of an Excel table that contains the method of identification and assessment of assets, an estimate of risks and a plan for dealing with risks for every information system in the CNB, i.e. including the SKD. The security profile is approved by the director of the relevant administrative unit, director of the technical administrative unit and director of the Information Systems Department.

The security profile of the SKD is analysed, reviewed and updated every year. The security profile includes a list of all processes and activities of the SKD, a list of all elements in the information technology system, the identification, analysis and monitoring of risks arising, the possibility of the occurrence of inherent risks, their evaluation and the probability of their occurrence, an analysis of the impact of the risks and measures leading to reductions in risks.

If a CNB employee ascertains, when operating and using the SKD, an extraordinary situation concerning a material or technical defect that prevents the use of the SKD, he will promptly pass on information about the material defect by e-mail or telephone to the administrator. The administrator will decide on a substitute solution or arrange an alteration to the SKD by handing over a request to the technical administrator.

In the event an extraordinary situation caused by serious economic reasons that prevents a Participant from performing activities arises, caused, for example, by the introduction of a measure to deal with a crisis in accordance with a special legal regulation for a Participant, the director of the department of the administrator or an employee authorised thereby will decide on how to proceed, e.g. on the blocking of asset accounts, the blocking of securities on asset accounts, the blocking of an issue that a Participant made or the end of activities by a Participant. Decisions are recorded in written form. In the event of an extraordinary situation caused by the CNB receiving information about the insolvency of a Participant, this information will be accepted by the director of the department of the administrator or an employee authorised thereby, he will assess it, issue an instruction to block a Participant's asset accounts and refuse other instructions of the Participant or

decide on another procedure. Decisions are recorded in written form.

In the event of an extraordinary situation caused, in particular, by serious economic or technical reasons that endanger the essence of the records and the settlement of securities in the SKD, the director of the department of the administrator or an employee authorised thereby will decide on the suspension of the SKD's activities. Decisions are recorded in written form.

The administrator outlines the risk framework in co-operation with the technical administrator, or other competent units interested in the SKD's activities.

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

Identification and consideration of stakeholder interests

The CNB can ask the Users' Committee to provide its opinion on any activities or decisions concerning the SKD. The conclusions of an audit of the SKD are handed over to the Users' Committee, if the conclusions concern criteria for the acceptance of issuers or users into the SKD or if the conclusions concern any other aspect of the Users' Committee's mandate or if the conclusions could influence the level of services provided through the SKD, including ensuring continuity of operations.

The Users' Committee provides opinions on fundamental measures that have an impact on users. The Users' Committee can submit a non-binding opinion containing detailed reasoning concerning the SKD's price structure.

Disclosure

The CNB issues the SKD Rules, which state information about the governance arrangements. SKD Participants must be informed of each amendment to the Rules or their annexes.

Assessment of Principle 2: Observed

Recommendations and comments: 0

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.

Risks that arise in or are borne by the FMI

The SKD is exposed to system risk, operational risk, liquidity risk, credit risk, financial risk, human factor failure risk and systemic risk.

The measurement and assessment of risks related to the SKD is performed using the SKD's Security Profile (see Principle 2, KC 6), which must be updated once a year.

The operation of the system is continuously monitored by the operator and SKD Participants.

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.

All information about the SKD is stated in the SKD Rules and their annexes, which are published at the CNB website.

Limitations on risks are ensured by the statement of the Participants' rights and duties in the SKD Rules. Another limitation on risk is the use of the Real Time Gross Settlement Model and the DVP settlement principle, which ensures inseparable settlement of securities and the related financial transfer. The definition of the irrevocability of settlement and separate billing of cash and investment instruments of a Participant reduces the aforementioned risk.

The participation principle of the settlement system helps limit the risk. Suitable conditions are set for participation in the settlement system with the irrevocability of settlement based on the statutory determination of the possible Participants. Compliance with this principle and the requirements of the Rules, including the technical and information duties, limits the system risk.

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.

The SKD is not linked to any entities outside the CNB. As far as concerns other FMI, the SKD is linked only to the CERTIS payment system also operated by the CNB.

Risk management tools

The risk management tools are stated in the SKD Security Profile.

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 an FMI from providing critical operations and services

In the event an extraordinary situation caused by serious economic reasons that prevents a Participant from performing activities arises, caused, for example, by the introduction of a measure to deal with a crisis in accordance with a special legal regulation for a Participant, the director of the department of the administrator or an employee authorised thereby will decide on how to proceed, e.g. on the blocking of asset accounts, the blocking of securities on asset accounts, the blocking of an issue that a Participant made or the end of activities by a Participant. Decisions are recorded in written form. In the event of an extraordinary situation caused by the CNB receiving information about the insolvency of a Participant, this information will be accepted by the director of the department of the administrator or an employee authorised thereby, he will assess it, issue an instruction to block a Participant's asset accounts and refuse other instructions of the Participant or decide on another procedure. Decisions are recorded in written form.

In the event of an extraordinary situation caused, in particular, by serious economic or technical reasons that endanger the essence of the records and the settlement of securities in the SKD, the director of the department of the administrator or an employee authorised thereby will decide on the suspension of the SKD's activities. Decisions are recorded in written form.

Recovery or orderly wind-down plans

Crises and extraordinary situations are dealt with by Act No. 240/2000 Coll., on crisis management and on an amendment to some acts, as amended, which determined for the CNB in Article 13 its duties when preparing for crises, in particular the duty to process a crisis plan in the area of monetary policy and banking and to co-operate with ministries on the drafting of crisis plans.

Based on the aforementioned act, the CNB drafted a crisis plan whose aim is to prepare the CNB to deal with extraordinary events that could interfere with or damage the CNB's integrity and destabilise the performance of the CNB's decisive activities concerning the financial market in the Czech Republic. Implementing documentation for the crisis plan contains specific procedures for the resolution of individual extraordinary events. This documentation, inter alia, contains procedures for the recovery of information systems.

The SKD contains a strategy for ensuring the continuity of operations, the source document is the emergency plan that stipulates the procedure for recovering the SKD's operations in the event of an emergency, the continuity of the most important operations during catastrophic scenarios, including natural disasters, pandemics, physical attacks, undesirable interference from outside, terrorist attacks and cyber attacks. The procedure for recovering operations after an accident includes and stipulates the most appropriate strategy for recovery for the most important operations and the recovery of the most important operations. It ensures that backup systems commence processing without undue delay.

The procedure for recovery of operations defines a secondary processing point with sufficient resources, capacities, functions and staff that are suitable from the viewpoint of the SKD's operational needs and the risks that it faces, with the aim of ensuring the continuity of the most important operations in the event the main processing point is not in operation.

The emergency plan is regularly tested in accordance with the importance of the expected possible emergencies with the full participation of users. Records of testing are recorded and, based on them, measures for improvement are adopted to ensure the continuity of the SKD's operations.

Assessment of Principle 3: Observed

Recommendations and comments: 0

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.

With regard to the fact that the SKD does not provide credit to Participants, it is not exposed to credit risk.

Sufficient coverage can be obtained by SKD Participants – Banks:

- Through a payment from another bank;
- Through a loan on the money market;
- In the form of a fully-collateralised intraday credit from the CNB;
- In the form of a fully-collateralised overnight credit from the CNB.

For this reason the CNB does not have a framework for the management of credit exposures of the individual Participants.

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.

With regard to the above, the CNB does not measure or monitor the credit exposures of SKD Participants. SKD Participants (banks), however, are enabled, based on a separate contract, to draw an intraday credit secured by liquid securities. This reduces the source of credit risk of Participants.

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.

Coverage of exposures to each participant

The SKD is a system that is based on the RTGS Model.

For the purposes of smooth settlement of transactions in the CERTIS payment system the CNB can provide, through the SKD, an intraday credit to clients - banks in accordance with a Framework Agreement on Provision of Intraday Credit concluded.

An intraday credit can be provided at any time during the period from the opening of an accounting day in the SKD until the start of closing of the accounting day in the CERTIS payment system based on an order for the provision of an intraday credit that is input by the SKD client. The amount of the intraday credit can be up to the amount of the securities held on the client account.

KC 4, 5 and 6 do not apply to SSS systems.

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.

With regard to the fact that the SKD does not provide credit to Participants, it is not exposed to credit risk and it does not suffer credit losses.

Assessment of Principle 4: Observed

Recommendations and comments: 0

Principle 5: Security – 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.

Principle 5 does not apply to the SKD.

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.

Principle 6 does not apply to the SKD.

Principle 7: Liquidity risk

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

The SKD does not have liquid resources and this principle does not apply to it.

Principle 7 does not apply to SSS systems.

Principle 8: Settlement Finality

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

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

Point of settlement finality

The moment of acceptance of an order for settlement, in the case of transactions that are not settled on the delivery versus payment principle, is understood to be the moment at which securities on an asset account are blocked for the purposes of transfer.

The moment of acceptance of an order for settlement, in the case of transactions that are not settled on the delivery versus payment principle, is understood to be the moment at which a payment order is created and sent to the CERTIS system.

A settlement order cannot be rescinded from the moment of acceptance of the order for settlement.

SKD Participants are informed through their agents.

The SKD performs monetary settlement in the Czech currency in central bank money.

The CNB, i.e. the SKD and SKD Participants conclude contracts, contracts on participation in the SKD and contracts on asset accounts in the SKD that confirm these principles.

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

Final settlement on the value date

The SKD is designed for the settlement and crediting of securities on the same day, settlement is performed using the Real Time Gross Settlement Model and on the DVP model 1 settlement principle, which ensures the indivisible settlement of securities and the related financial transfer.

A deferral of unintended final settlement to the next day has not been recorded in the SKD.

Intraday or real-time final settlement

The SKD ensures final settlement in real time. SKD Participants are informed electronically through their agents.

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.

The moment of acceptance of an order for settlement, in the case of transactions that are not settled on the delivery versus payment principle, is understood to be the moment at which

securities on an asset account are blocked for the purposes of transfer.

The moment of acceptance of an order for settlement, in the case of transactions that are not settled on the delivery versus payment principle, is understood to be the moment at which a payment order is created and sent to the CERTIS system.

A settlement order cannot be rescinded from the moment of acceptance of the order for settlement.

Based on a new instruction from a Participant, the SKD cancels its previous instruction to transfer a security or other transaction in a security, unless the moment of acceptance of the order for settlement has occurred for the previous order.

Exceptions and extensions of the period are not permitted.

Information about this is stated in the SKD Rules.

Assessment of Principle 8: Observed

Recommendations and comments: 0

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 risk 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.

The SKD performs monetary settlement in central bank money and only in CZK.

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 risk or liquidity risk.

N/A

Key Consideration 3: If an FMI settles in commercial bank money, it should monitor, manage, and limit its credit risk 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.

N/A

Key Consideration 4: If an FMI conducts money settlements on its own books, it should minimise and strictly control its credit risk and liquidity risk.

The CNB is also an SKD Participant and uses its own money account for settlement.

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

The SKD does not use a settlement bank for settlement.

Assessment of Principle 9: Observed

Recommendations and comments: 0

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.

Principle 10 does not apply to the SKD.

Principle 11: Central Securities Depositories (CSD)

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.

Safeguarding the rights of securities issuers and holders

An issue is understood to mean securities issued by the same issuer, with the same nominal value, maturity and with the same ISIN or with an issue code allocated by the operator.

Every issue is linked by a simple asset account of the issuer and agent that has access to the asset account.

Securities issues are designated in the SKD using a code allocated by the SKD or an ISIN.

Every issue is issued only from one account of the owner - issuer.

It is possible to perform an increase or reduction in the volume of the current issue.

Securities in one issue are fungible and are not numbered.

A new issue must be recorded in the SKD before the day of issue.

The SKD's notification of the division of securities in a new issue among the first transferees must be performed through an auction point.

A record is maintained of all transactions and the participating parties have it available.

Only a client can issue securities in the SKD. A client that intends to issue securities must use the services of an agent that has access to its owner's account.

Records of issues contain basic information about individual issues, i.e. in particular:

- The name of the security;
- The date of issue;
- The security's maturity date;
- The security's nominal value;
- The volume of an issue in the nominal value;
- The value of the security upon maturity;
- Information about the blocking of the issue;
- Information about the account owner and the account type on which the security is recorded;
- Information about the issuer.

An extract from records contains information in accordance with the previous paragraph.

The SKD contains records only of bonds maturing within 1 year, inclusive, denominated in CZK.

It is only possible to record:

- Bonds without a coupon (discounted) whose issuer, on maturity, will pay out the nominal value of the bond (if appropriate, reduced by tax);

- Bonds with a coupon that is paid out (if appropriate, reduced by tax) on the issue's maturity together with the principal;

With regard to the interchangeability of the securities, it is not possible to ensure that they are distinguishable for any purposes (e.g. tax). An issuer must therefore act in such a manner that securities are interchangeable also from the tax viewpoint (e.g. in the event of withholding tax it is necessary to sell discounted securities for the same price).

One issue can be sold progressively in several tranches. Individual tranches of an issue are differentiated in the SKD records using the issue serial number, securities of individual tranches in one issue are, however, interchangeable.

Periodic reconciliation of securities issues

At the end of a set period of an accounting day a check is performed during which there is a comparison of the previous daily final balance of individual issues of securities with all settlements of individual issues processed during the relevant day and with the current daily final balance of individual issues of securities on securities accounts. Any non-compliance or discrepancies resulting from the reconciliation process are analysed and an attempt at resolving them is made before the start of settlement on the following accounting day. If this problem cannot be resolved by the end of the following business day, the operator will suspend settlement of an issue of securities, until the problem is corrected. If settlement is suspended, the operator will inform the Participants and all entities involved in the settlement process of this without undue delay. An operator informs the Participants after the problem is corrected.

In the SKD it is possible, at any time, to differentiate securities of one owner or custodian on asset accounts from the securities of another owner or custodian. A client account contains accounts that enable a custodian to hold securities that belong to various clients of the relevant custodian on one asset account ("Omnibus Client Segregation"). A custodian offers its customers a choice between Omnibus Client Segregation and segregation of individual clients; in the event of segregation of individual clients, the securities of individual clients are entered on individual asset accounts of clients.

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

In the SKD overdrawn securities asset accounts and debit balances on securities asset accounts are not permitted.

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.

Securities entered in the SKD do not physically exist and are represented only by an entry in the SKD database.

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

See reply to Key Consideration 1 - Periodic reconciliation of securities issues.

A custody of securities service is not performed in the SKD.

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 the SKD it is possible, at any time, to differentiate securities of one owner or custodian on asset accounts from the securities of another owner or custodian. A custodian offers its customers a choice between Omnibus Client Segregation and segregation of individual clients; in the event of segregation of individual clients, the securities of individual clients are entered on individual asset accounts of clients. Omnibus Client Segregation enables a custodian to hold securities that belong to various clients of the relevant custodian on a client account, on one asset account.

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.

The SKD does not provide services other than central safekeeping and administration of securities and settlement.

Assessment of Principle 11: Observed

Recommendations and comments: 0

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.

In an exchange mutually-conditional free transfers of securities in two different issues are performed between two asset accounts. The securities must be available on the accounts of both parties, then the securities are blocked on both accounts and there is also a transfer of securities.

Exchanges are settled transaction for transaction.

After the agreement of the conditions of an exchange, by a stipulated deadline both parties submit instructions for the transfer of the securities that are the subject of the exchange to the SKD, at the same time as transferors and transferees. Irrevocability occurs at the same time as the blocking of the securities on both accounts. The securities are then transferred.

Assessment of Principle 12: Observed

Recommendations and comments: 0

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.

Participant Default Rules and Procedures

The SKD operator will not execute the instruction of a party, if it is in conflict with the Rules or a valid contract. The operator will refuse to execute a party's instruction, if it finds that it is in conflict with legal regulations.

If, by the end of the accounting day in the CERTIS payment system on the day of settlement there are not sufficient funds on the money account of the transferee's agent, the transaction is not executed and the transfer of the securities is not registered by the SKD. The securities blocked for the purposes of transfer on the asset account of the transferor are unblocked by the SKD and it informs the transferor and the transferee of the non-executed transfer through their agent. This is performed automatically.

Use of Financial Resources

In the event of a lack of liquidity the CNB offers parties an interest-free intraday credit secured by liquid securities of the parties recorded in the SKD or in the Central Depository. The CNB does not use its own unsecured funds in these operations.

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.

In the event an extraordinary situation caused by serious economic reasons that prevents a Participant from performing activities arises, caused, for example, by the introduction of a measure to deal with a crisis in accordance with a special legal regulation for a Participant, the director of the department of the administrator or an employee authorised thereby will decide on how to proceed, e.g. on the blocking of asset accounts, the blocking of securities on asset accounts, the blocking of an issue that a Participant made or the end of activities by a Participant. Decisions are recorded in written form. In the event of an extraordinary situation caused by the CNB receiving information about the insolvency of a Participant, this information will be accepted by the director of the department of the administrator or an employee authorised thereby, he will assess it, issue an instruction to block a Participant's asset accounts and refuse other instructions of the Participant or decide on another procedure. Decisions are recorded in written form.

In the event of an extraordinary situation caused, in particular, by serious economic or technical reasons that endanger the essence of the records and the settlement of securities in the SKD, the director of the department of the administrator or an employee authorised thereby will decide on the suspension of the SKD's activities. Decisions are recorded in written form.

Telephone, e-mail and web applications are used for communication.

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

The information is published at the CNB's website in the SKD Rules. Other procedures are not published.

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.

The SKD does not perform testing and review of its procedures in case of Participant default. With regard to the fact that the RTGS model is used, the default of an SKD Participant has an impact only on its counterparties. Any consequences of a chain reaction cannot be monitored. Default occurs in quite exceptional cases.

Assessment of Principle 13: Broadly observed

Recommendations and comments: The SKD does not perform testing and review of its procedures in case of Participant default.

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.

Principle 14 does not apply to SSS systems.

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.

The SKD is not a trading system, the SKD is part of the CNB.

The principle does not apply to central banks.

Principle 15: not relevant for central banks

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.

The principle is not relevant for central banks.

Assessment of principle 16: not relevant for central banks

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

Security measures to reduce operational risk that are realised and documented as a part of CNB security are also applied to the SKD. This primarily concerns ensuring building security, the separation of the location of the main and backup information systems, the links between them due to the updating of systems and data in real time, operations on reliable technologies, duplicate data storage on disk media, the availability of replacement power sources, the drafting and testing of a continuity of activities plan, testing of sufficient capacity for processing all settlements, the replaceability of key workers and, last but not least, mechanisms aimed at uncovering cyber attacks and at preventing them. Other specific securities measures include, for example, the limited group of workers and their access to the rooms for the main and backup workplace, regular data archiving, repeated audits of the system, checks on access rights to the system, direct checks on data from the system by system Participants, electronic checks on input data, audit trails for data, system checksums. The tools for limiting risks also include, for example, the four-eyes method if there is a change to data in operations concerning money accounts, the sending of e-mails about a change made, logging of the process of transaction processing and logging of users' activities, monitoring of activities.

No failure points were identified.

Policies, processes and controls

The CNB's basic internal regulation (Statutes) is the Organisational Rules, which are a binding initial document for the preparation of related internal regulations and managerial acts of the CNB.

The Organisational Rules

- Define the organisational structure of the CNB;
- Determine and set out the principles of the CNB's internal governance arrangements;
- Define the levels of management and powers of CNB managerial employees;
- Define the powers of CNB organisational units and the principles of their co-operation and communication between them.

The Organisational Rules and amendments thereto are approved by the Bank Board.

The CNB issued Instructions 40/2002 for personnel work at the Czech National Bank. These instructions set out, in connection with the CNB Work Rules, the performance of activities by the CNB concerning labour law relations, remuneration of employees and performance of HR work at the CNB. They define the rules and procedures applied during searches, selection and hiring of new employees for employment relationships, when remunerating employees, when determining the working hours of specific groups of employees, when maintaining records of working hours, when amending and terminating employment relations and when assessing the level of work results achieved and employees' abilities.

Developments in new information systems and applications or alterations to current information systems and applications are discussed and approved by the Commission for Information Technology, the members of which are the directors of all CNB departments, which ensures information is shared across the CNB. In addition to this, the Information Systems Department is responsible, inter alia, for basic coordination, integration and the methodology of managing all projects concerning IS/IT at the CNB.

All risks are handled in the SKD Security Profile.

The SKD is subjected to an external audit every year and to an internal audit repeatedly. Based on the output from the assessment of risks and from the audits, any measures to reduce risks to which the CERTIS system is exposed, including operational risks, are taken.

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 guidelines, procedures and controls should be reviewed, audited, and tested periodically and after significant changes.

The issue of operational risks is dealt with in the CNB by Instructions of the Czech National Bank 80 for managing operational risks at the Czech National Bank, which are effective from 1 January 2018.

The management of operational risks function at the CNB is handled in decentralised fashion. The Bank Board is responsible for the setting of the management of operational risks function. The directors of CNB organisational units are responsible for executing the operational risk management function. The director of the General Secretariat is responsible for the methodological management and coordination of the operational risk management function and, inter alia, determines the employees in the General Secretariat that handle such activities.

Directors of CNB organisational units, inter alia, determine the contact persons for management of operational risks for the units they manage.

In the Cash and Payment Systems Department, Decision of the Director of the Cash and Payment Systems Department 1/2018, stipulating the procedures for management of operational risks in the Cash and Payment Systems Department, has been issued. The decision sets out the duties of employees of the Cash and Payment Systems Department, in particular reporting of operational risk events.

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.

Act No. 240/2000 Coll., on crisis management and on an amendment to some acts, as amended, determines for the CNB in Article 13 its duties when preparing for crises, in particular the duty to process a crisis plan in the area of monetary policy and banking and to co-operate with ministries on the drafting of crisis plans.

Based on the aforementioned act, the CNB drafted a crisis plan whose aim is to prepare the CNB to deal with extraordinary events that could interfere with or damage the CNB's integrity and destabilise the performance of the CNB's decisive activities concerning the financial market in the Czech Republic. Implementing documentation for the crisis plan contains specific procedures for the resolution of individual extraordinary events. This documentation, inter alia, contains procedures for the recovery of information systems.

The SKD contains a strategy for ensuring the continuity of operations, the source document is the emergency plan that stipulates the procedure for recovering the SKD's operations in the event of an emergency, the continuity of the most important operations during catastrophic scenarios, including natural disasters, pandemics, physical attacks, undesirable interference from outside, terrorist attacks and cyber attacks. The procedure for recovering operations after an accident includes and stipulates the most appropriate strategy for recovery for the most important operations and the recovery of the most important operations. It ensures that backup systems commence processing without undue delay. The emergency plan is published on the CNB intranet.

The procedures for SKD recovery stipulate the procedures when dealing with individual emergency situations in the SKD information system. Key emphasis is then placed on the option of recovering the system in the location of the backup side, which is located a sufficient distance away and is not subject to the same threats as the primary side. Thanks to the technical solution and real-time availability of the backup side, it provides the same performance, capacity and functionality as the primary side.

Testing of infrastructure based on the SKD Recovery Procedure is performed periodically in a testing environment. Based on the experience obtained during testing, the SKD Recovery Procedure is altered.

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.

Although the trend in the number of operations in the SKD is rising, with regard to the relatively low number of operations in absolute values the SKD's capacity is sufficient.

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

Physical security

For this purpose the CNB has issued Instructions 53 dated 19 May 2010 to ensure security for buildings and defined space of the Czech National Bank, the transport of money and other valuables and for the use of weapons and ammunition held by the Czech National Bank on a firearms licence.

The task of building security is to prevent and limit loss to life and the health of persons in buildings and losses to the CNB's assets, the protection of the CNB's interests in buildings and documentation about extraordinary events, offences and criminal activities for the needs of the police.

The instructions are based, for example, on Act No. 412/2005 Coll., on the protection of secret information and on security capacity, Act No. 239/2000 Coll., on the integrated emergency system and on an amendment to some acts, Act No. 40/2009 Coll., the Criminal Code, Act No. 141/1961 Coll., on criminal court proceedings (the Criminal Code), following on from Instructions of the CNB 31/2011, on the regime for entry by persons and vehicles to buildings and defined space of the Czech National Bank and on the regime for their movement and, last but not least, the CNB Crisis Plan.

Information security

Act 181/2014 Coll., on cyber security and on an amendment to related acts (the Act on Cyber Security), imposes duties concerning cyber security, inter alia, on the controller of an information system for critical information infrastructure and on the administrator of an important information system, which the SKD undoubtedly is. The CNB established a Commission for Cyber Security (hereinafter the “Commission”), the chairman of which is the director of the Information Systems Department. The Commission discusses trends in the CNB’s security policy concerning IT, assesses and recommends for approval fundamental internal regulations concerning IT, e.g. training on IT security (extent, frequency) and user requirements. The Commission is regularly informed by the Information Systems Department of:

Category III security incidents (very serious cyber security incidents during which the security of services or assets provided is directly and seriously compromised);

The status/updating of security profiles of individual systems;

Compliance with the plan for IT security training;

The results of audits and remedies accepted concerning IT security, where the implementer of the recommendations is the Information Systems Department.

Once a year the Commission discusses, assesses and recommends for approval the Security Information Systems and Technology (IS/IT) chapter from the document Report on Security Status in the Czech National Bank.

The requirements under the Act on Cyber Security are handled in Methodology Sheet of the Information Systems Department 720/9/2015, stipulating the procedure for asset management and risk management concerning IS/IT at the Czech National Bank. The methodology sheet describes how to perform identification and assessment of information assets in information systems and information technology, how to perform a risk analysis, propose measures to eliminate such risks and determine the remaining risks. The output is then a “Security Profile” in the form of an Excel table. All risks of the CERTIS system are then handled in the CERTIS Security Profile.

The aforementioned methodology sheet follows on from Instructions of the CNB 32/2007, stipulating the CNB’s security policy for information technology (hereinafter the “Instructions”). The IT security policy sets out the security aims and defines the basic principles of IT security and the resulting duties of users, material and technical administrators and information systems of the CNB, managerial employees and organisational units of the CNB.

The Instructions clearly define the responsibility of individual units in the CNB for the management and organisation of IT security. These units are primarily the Information Systems Department, which also works with the other interested units – the Administration Department, the Human Resources Department and also the Cash and Payment Systems Department.

The Information Systems Department is responsible for the updating of the IT security policy based on regular assessments of the achieved state of information technology security, an assessment of security risks and developments in information technology in accordance with the relevant standards and regulations. An assessment is performed by the Information Systems Department in co-operation with the Internal Audit Department or an external auditor.

The Instructions contain penalty provisions whose task is to ensure compliance with the principles contained in the various areas of the security policy.

The Information Systems Department has also drafted a number of other methodological sheets that deal with, for example, procedures for creation, recovery and the method of handling passwords and accounts in information systems and the system environment of the CNB, procedures related to the collection, assessment and storage of security logs, procedures for managing

vulnerabilities in the IS/IT in the system environment of the Czech National Bank and others.

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.

Objectives of business continuity plan

The CNB drafts a crisis plan whose aim is to prepare the CNB to deal with extraordinary events that could disrupt or damage the CNB's integrity and destabilise the performance of decisive activities. Implementing documentation for the crisis plan contains specific procedures for the resolution of individual extraordinary events. This documentation, inter alia, contains procedures for the recovery of information systems.

The procedure for recovering operations after an accident includes and stipulates the most appropriate strategy for recovery for the most important operations and the recovery of the most important operations. It ensures that backup systems commence processing without undue delay.

Design of business continuity plan

According to the operational plan of the Information Systems Department, the plan for the recovery period for the purposes of dealing with extraordinary events in accordance with the crisis plan should cover 8 hours.

For the purposes of solutions to ordinary defects in connection with "best effort" practice the recovery time is set:

SKD	2 hours between 07:00-17:30
-----	-----------------------------

CNB network	25 hours contractual fix time for the correction of a defect. These 25 hours, however, will not have as a consequence a 25-hour outage of the application, as in the event of an outage to the part of the network where the primary servers are connected processing is moved to the backup side. A 25-hour outage can therefore occur, but only under the condition that there is a complete outage of the network in both computer centres.
-------------	--

Secondary site

The SKD recovery procedure is based on the fact that all the decisive components of the system base and applications are backed up and dealt with automatically or through a manual transfer to a backup component. Backup components – the backup side – are located at a sufficiently and also reasonably remote location (Zličín - 20 km), which is connected by optical cables and its physical and technological security is of at least the same standard as the security for the primary side.

In the event an SKD Participant is not able to hand over and accept data through the SKD, it is possible to hand data over/accept them in a replacement manner, by fax, e-mail or in person at the CNB.

The procedure for recovery of operations defines a secondary processing point with sufficient resources, capacities, functions and staff that are suitable from the viewpoint of the SKD's operational needs and the risks that it faces, with the aim of ensuring the continuity of the most important operations in the event the main processing point is not in operation.

Review and testing

Testing of the recovery procedure, i.e. individual procedures realising the transfer and return of processing between the services on the primary and backup sides, is performed at least once a year. On at least one accounting day in a year the management of the SKD is realised by operational personnel on the backup side in Zličín.

The emergency plan is regularly tested in accordance with the importance of the expected possible emergencies with the full participation of users. Records of testing are recorded and, based on them, measures for improvement are adopted to ensure the continuity of the SKD's operations.

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.

The identification, monitoring and management of all risks is dealt with in the CERTIS Security Profile, see above.

Assessment of Principle 17: Observed

Recommendations and comments: 0

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

The SKD rules stipulate:

- An **agent**, i.e. a legal entity stated in Article 84(1) of the Capital Market Undertakings Act, with which the CNB concludes a contract on participation in SKD. An agent can be, based on a contract on participation in the SKD, entitled to arrange for other participants – i.e. custodians and clients - electronic access to their asset accounts in the SKD and to obtain information that concerns them from the SKD.
- A **custodian**, i.e. a legal entity stated in Article 92(2) of the Capital Market Undertakings Act, with which the CNB concludes a contract on client account in the SKD. A client account is opened based on a contract on client account in the SKD. Only a custodian can have one or more client accounts in the SKD.
- A **client** is a legal entity or natural person with which the CNB concludes a contract on securities owner account in the SKD. An owner account is opened on the basis of a contract on a securities owner account in the SKD. Only a client may have one or multiple owner accounts in the SKD.

The CNB is also an agent and client. As an agent it works, in particular, for the Ministry of Finance of the Czech Republic and also for some central banks.

Access to trade repositories

The SKD is not a trading system.

N/A

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 endeavor to set requirements that have the least-restrictive impact on access that circumstances permit.

Justification and rationale of participation criteria

The criteria for participation are set out by the law and the Rules, so they are public.

Act No. 256/2004 Coll., on capital market undertakings, determines the criteria for participation in the SKD, see KC 1.

In an annex to an application for participation in the SKD a domestic legal entity states in the case of an agent its declaration or that of the agent's bank that it agrees that its cash account can be debited with a payment by a third party based on an SKD instruction. The agent will also state the its tax identification number;

In an annex to an application for participation in the SKD a foreign legal entity states:

- an official document confirming the existence of the legal entity, date of establishment and its registered office. The accuracy of documents shall be confirmed by an impression of the Apostille stamp or a stamp of the embassy or legation of the Czech Republic in the country in which the legal entity has its registered office. Unless any other procedure for

verifying public instruments is stipulated in an international treaty, a verified translation into Czech shall be attached to these documents; i.e. if a foreign legal entity has its registered office in a country which has signed the European Convention on the Abolition of Legalisation of Documents executed by Diplomatic Agents or Consular Officers, or a bilateral agreement, it shall be proceeded in line with these documents;

- in case of a client/custodian, an official document of its tax domicile. This document must be updated on a regular basis, namely at least once a year;
- a list of members of the statutory body or a power of attorney verified by a notary giving the entrusted parties the authority to sign on behalf of the relevant company with a verified translation into Czech;
- in case of a client/custodian - a foreign legal entity having its registered office or place of business outside the states of the European Union or the European Economic Area submits a legal opinion elaborated by a renowned lawyer's office (engaged in international law or the law of the given state) with a licence to perform its activity in a state of the European Union or in the European Economic Area and with the respective insurance of this activity, in which it will be certified that the legal order, by which bankruptcy proceedings with respect to the foreign legal entity's assets or any other possible measures of a public authority directed against the foreign legal entity's assets are governed, does not impede the irrevocability of the orders for settlement stipulated by Czech law. This certificate, submitted together with a verified translation into Czech, must be updated on a regular basis, at least once a year. Further to an agreement with the CNB, it is not necessary to submit the certificate (if the CNB has already received such a certificate no older than one year about the legal order of the given state);

For the purposes of the SKD the identity of a domestic natural person shall be verified by an official document (ID card, passport, driving licence, gun licence, birth certificate).

In an annex to an application for participation in the SKD a foreign natural person states:

- an official document of his tax domicile; this document must be updated on a regular basis, at least once a year;
- in case of a foreign person having his place of business outside the states of the European Union or the European Economic Area he shall submit a legal opinion elaborated by a renowned lawyer's office (engaged in international law or the law of the given state) with a licence to perform its activity in a state of the European Union or in the European Economic Area and with the respective insurance of this activity, in which it will be certified that the legal order, by which bankruptcy proceedings with respect to the foreign person's assets or any other possible measures of a public authority directed against the foreign person's assets are governed, does not impede the irrevocability of the orders for settlement stipulated by Czech law. This certificate, submitted together with a verified translation into Czech, must be updated on a regular basis, at least once a year. Further to an agreement with the CNB, it is not necessary to submit the certificate (if the CNB has already received such a certificate no older than one year about the legal order of the given state);
- For the purposes of the SKD, identity shall be verified by an official document (ID card, passport, driving licence, gun licence, birth certificate).

The application shall bear the date and signature of the statutory body of the legal entity or individual (natural person) who makes the application.

Least restrictive access

If there is a change to the SKD Rules, the requirements regarding access are assessed.

Disclosure of criteria

The criteria are stated at the CNB's website in the SKD Rules.

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

The CNB monitors its participants' compliance with the access criteria daily. The SKD administrator monitors the behaviour of SKD participants through the SKD application, which enables, for example, the displaying of the current position of a Participant, the displaying of a daily statement, a list of instructions input, the state of performance of settlement, drawing of intraday credits, etc. The valid SKD Rules are always followed.

Suspension and orderly exit

The CNB is entitled to terminate a contract in writing, if an SKD Participant breaches it.

The CNB is entitled to withdraw from a contract with immediate effect, if an SKD Participant breaches its duties in a significant manner resulting from such contract or the Rules.

The CNB is also entitled to withdraw from a contract if it ascertains binding facts that could, in a material manner, endanger the ability of an SKD Participant to meet its obligations under the contract or the Rules (e.g. the implementation of a decision against an agent or a risk of bankruptcy).

The procedures are stated in the SKD Rules and in their annexes, which are publicly accessible.

Assessment of Principle 18: Observed

Recommendations and comments: 0

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

The tiered participation arrangements are described in Principle 18.

The data about SKD Participants are recorded electronically in the SKD database and also in SKD Participant documentation.

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

Payments for custodians and clients of an agent are, as a part of settlement and other transactions handled by the SKD, paid for from an agent's money account stated in the contract on participation in the SKD. Credit items are paid directly into the money accounts stated in the contract on asset account of securities owner (client) or in a contract on asset account of client (custodian).

An agent, who is an obligated person as per the provisions of the act on some measures against the money laundering, shall be responsible for the proper identification of custodians and clients to whom he is authorized to ensure electronic access to their asset accounts as well as for the compliance with other obligations stipulated by this act, especially the meeting of the obligation to maintain identification data of custodians and clients whose provision, including the provision of copies of appropriate documents, may be required by the operator.

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.

The volumes of transactions of individual SKD Participants are not statistically assessed. The transaction volumes of the SKD Participants do not have an influence on the size of the risk.

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

If there is an amendment to the SKD Rules, the risks regarding the tiered participation arrangements are assessed.

Assessment of Principle 19: Observed

Recommendations and comments: 0

Principle 20: FMI Links

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

The SKD does not have any link with other FMI entities, with the exception of the CERTIS payment system, with which it communicates directly as a part of the CNB’s electronic structure.

Assessment of Principle 20: Observed

Recommendations and comments: 0

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.

SKD Participants have the option of expressing their requirements regarding the aforementioned parameters, in particular through the Users' Committee.

SKD Participants can communicate their needs also to workers with the SKD administrator and operator. The needs are subsequently analysed and dealt with.

No larger complaints have appeared, in addition to the ordinary minor operating problems.

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.

The main aim of the system's owner and operator is to operate the system safely, reliably and effectively. The aims are met if the SKD Participants are to perform all their settlements in the shortest time possible.

The Users' Committee provides opinions on fundamental measures that have an impact on users. The Users' Committee can submit a non-binding opinion containing detailed reasoning concerning the SKD's price structure.

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

With regard to the low number of operations, the system is sufficiently robust and effective. In the case of DVP transactions that are demanding in time terms and if the acquiring and transferring parties have sufficient funds, the time for settlement is just a few minutes (1-3).

The number of outages in the SKD is up to five a year.

Assessment of Principle 21: Broadly observed

Recommendations and comments: The STBS should have established mechanisms for the regular review of its efficiency and effectiveness.

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.

Communication procedures

The SKD has its own communication procedures and standards. Users have their own interactive access to the SKD and communicate through a user interface.

Communication standards

The SKD does not use internationally accepted communication standards.

An expansion of the application interface based on ISO 15022 through the SWIFT network is being prepared for the SKD.

Assessment of Principle 22: Not observed

Principle 23: Disclosure of Rules, Key Procedures, and Market Data

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

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

Rules and procedures

The fundamental documents are the SKD Rules, including annexes, which contain specimen contracts.

SKD Participants must be informed of every change to the Rules, their annexes or the Participation Manual and a reasonable time must also be set by which such activities must be adapted to a change to the SKD, or they can express their non-consent to the change and file notice of termination of a contract on participation in the SKD or a contract on asset account in the SKD.

The CNB learns whether the documents are clear and comprehensive from the reactions of SKD Participants, with which it is in everyday contact. If a procedure or process is not quite clear, based on the comments the CNB will specify it.

Disclosure

If a CNB employee ascertains, when operating and using the SKD, an extraordinary situation concerning a material defect that prevents the use of the SKD, he will promptly pass on information about the material defect by e-mail or telephone to the administrator. The administrator will decide on a substitute solution, or arrange the alterations to the SKD through the handover of a request to the technical administrator by opening an incident in the ServiceDesk system (hereinafter "SD"), by sending an e-mail or telephoning the helpdesk. A record of requests for alteration is maintained in the SKD List of Changes.

In the event an extraordinary situation caused by serious economic reasons that prevents a Participant from performing activities arises, caused, for example, by the introduction of a measure to deal with a crisis in accordance with a special legal regulation for a Participant, the director of the department of the administrator or an employee authorised thereby will decide on how to proceed, e.g. on the blocking of asset accounts, the blocking of securities on asset accounts, the blocking of an issue that a Participant made or the end of activities by a Participant. Decisions are recorded in written form. In the event of an extraordinary situation caused by the CNB receiving information about the insolvency of a Participant, this information will be accepted by the director of the department of the administrator or an employee authorised thereby, he will assess it, issue an instruction to block a Participant's asset accounts and refuse other instructions of the Participant or decide on another procedure. Decisions are recorded in written form.

In the event of an extraordinary situation caused, in particular, by serious economic or technical reasons that endanger the essence of the records and the settlement of securities in the SKD, the director of the department of the administrator or an employee authorised thereby will

decide on the suspension of the SKD's activities. Decisions are recorded in written form.

The SKD informs SKD Participants about amendments to the rules by e-mail.

The SKD discloses the relevant rules and key procedures to the public at the CNB's website.

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.

All information is stated in the SKD Rules, see above.

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 operator is in everyday contact with system Participants. In the event of a lack of clarity, employees answer questions from SKD Participants.

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.

The CNB notifies of its charges in part VI of the Pricelist for money and trading services of the CNB - Short-term Bond System, the Pricelist is published at the CNB website.

The CNB informs participants of changes to charges two months in advance. The description of prices is brief and accurate and enables comparisons with other FMI.

The CNB does not disclose its technologies and communications procedures.

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.

The CPSS-IOSCO *Disclosure framework for financial market infrastructures* was completed in 2007.

Updating is performed after important changes.

As far as concerns the statement of basic information to the public, the SKD publishes at its website Average Prices/Values of Short-term Bonds for each Trading Day, the current and historical Summary of Bonds Entered in the SKD, Monthly Statistics on Securities Issued, the Volume of Transactions and the total number of transactions, including graphics.

All the aforementioned information, including the SKD Rules, are in Czech and English.

Assessment of Principle 23: Observed

Recommendations and comments: 0

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.

Principle 24 does not apply to SSS systems.

Annex

The documents are used as a source of information about the SKD.

- Short-term Bond System Rules
- Short-term Bond System Participations Manual
- Short-term Bond System Operating Regulations
- SKD Emergency Plan
- Act No. 6/1993 Coll., on the Czech National Bank, as amended
- Act No 256/2004 Coll., the Capital Market Undertakings Act, as amended.
- 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.