

# **National Settlement Depository**

## **Report on the description, design and efficiency of controls**

Prepared in accordance with International Standard on Assurance Engagements No. 3402 Type 2 (ISAE 3402), issued by the International Auditing and Assurance Standards Board

# Contents

**Section I: Independent Service Auditor's Assurance Report ----- 1**

**Section II: Assertion by Management----- 4**

**Section III: National Settlement Depository Company Profile Provided by Management 7**

**Section IV: Description of Control Procedures prepared by Management. Testing of design and operating effectiveness of Control Procedures performed by the independent auditor ----- 19**

# Section I: Independent Service Auditor's Assurance Report

## Section I: Independent Service Auditor's Assurance Report

To: National Settlement Depository (hereinafter, "NSD" or the "Company")

### Scope

We have been engaged to report on (i) the validity of the description of the controls (hereinafter, the "Control Procedures") presented on pages 7-35 (hereinafter, the "Description"), as related to NSD's settlement depository, clearing and repository services for the period from 1 January to 30 June 2017, and (ii) on the design and operating effectiveness of the Control Procedures related to the control objectives stated in the Description (hereinafter, the "Control Objectives").

The Description indicates that customers should be responsible for availability of certain control procedures at their end, which are essential for ensuring efficient, correct and controllable interaction with the Company. We have not evaluated the suitability of the design or operating effectiveness of such complementary customers' control procedures.

### Management's Responsibilities

NSD's management is responsible for (i) preparing the Description and the accompanying Assertion by Management at page 4, including the completeness, accuracy and presentation of the Description and the Assertion by Management; (ii) providing the services covered by the Description; (iii) stating the Control Objectives; and (iv) designing the Control Procedures, as well as implementing and ensuring their operating effectiveness so as to achieve the stated Control Objectives.

### Our Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

ZAO Deloitte & Touche CIS applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

### Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the design and operation of Control Procedures related to the Control Objectives, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization," issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the design and operating effectiveness of the Control Procedures comply with the Control Objectives.

The assurance engagement involved performing procedures to obtain evidence about the Control Procedures presented in the Description, as well as evidence that the design and operating effectiveness of the Control Procedures are in compliance with the Control Objectives. The procedures selected depended on the auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that the

design and operating effectiveness of the Control Procedures are not in compliance with the Control Objectives. Our procedures included testing the operating effectiveness of those Control Procedures that we consider necessary to provide reasonable assurance that the design and operating effectiveness of the Control Procedures are in compliance with the Control Objectives. We have also assessed the overall presentation of the Description, the appropriateness of the Control Objectives, and the suitability of the criteria as regards the compliance of the design and operating effectiveness of the Control Procedures with the Control Objectives. We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

#### Limitations

The Description is prepared to meet the common information needs of a broad range of NSD's customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their limitations, Control Procedures may not prevent or detect all errors or omissions in providing services or preparing reports. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that Control Procedures may become inadequate or fail.

#### Opinion

In our opinion, in all material respects:

- the Description fairly presents the processes of depository, settlement, clearing and repository services provided over the period of 1 January to 30 June 2017;
- the Control Procedures related to the Control Objectives stated are suitably designed to provide reasonable assurance that the Control Objectives can be achieved;
- the Control Procedures tested to provide reasonable assurance that the Control Objectives can be achieved, operated effectively during the period of 1 January to 30 June 2017.

#### Intended Users and Purpose

We have been engaged by NSD to prepare this report. Therefore, this report is only intended for the use of NSD. We permit NSD to provide this report in full to (i) customers who use depository, settlement, clearing and repository services, (ii) their auditors who have a sufficient understanding to consider this report, along with other information (including information about Control Procedures operated by customers themselves) when assessing the risks of material misstatements of customers' financial statements, and (iii) other stakeholders, in accordance with the Russian laws and Agreement No. № Aud/2017/46050 of 19 June 2017 between the Company and ZAO Deloitte & Touche CIS. In doing so, we do not assume any liability towards customers and their auditors.

ZAO "Deloitte & Touche CIS"

3 October 2017

# Section II.

## Assertion by Management



**NATIONAL  
SETTLEMENT  
DEPOSITORY**  
MOSCOW EXCHANGE GROUP

National Settlement Depository  
NSD

Postal address: 12 Spartakovskaya St., Moscow 105066, Russia  
Tel.: +7 495 234-48-27, fax: +7 495 956-09-38  
E-mail: info@nsd.ru, www.nsd.ru

## Section II: Assertion by Management

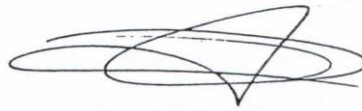
3 October 2017

The accompanying Description has been prepared for customers and their auditors, who have a sufficient understanding to consider the Description, along with other information, including information about control procedures by customers themselves, when assessing the risks of material misstatements of customers' financial statements. We confirm that:

- (a) The accompanying Description on pages 7-35 fairly presents the system for processing customers' transactions throughout the period from 1 January to 30 June 2017. The criteria used in making this assertion were that the accompanying Description:
  - (i) Presents how the system was designed and implemented, including:
    - The types of services provided, including, as appropriate, classes of transactions processed;
    - The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.
    - The related accounting records, supporting information, and specific accounts that were used to initiate, record, process and report transactions, including corrections of inaccurate information and transfers to the reports prepared for customers;
    - How the system deals with significant events and conditions, other than transactions;
    - The process used to prepare reports for customers;
    - Relevant Control Objectives and Control Procedures designed to achieve those objectives;
    - Control Procedures that we assumed, would be implemented by customers, and which, if necessary to achieve the Control Objectives stated in the accompanying Description, are identified in the Description along with the specific Control Objectives that cannot be achieved by ourselves alone;
    - Other aspects of our control environment, including risk assessment process, information systems (including the related business processes) and communication, control activities and monitoring Control Procedures that were relevant to processing and reporting customers' transactions;
  - (ii) Includes relevant details of changes to the service organization's system during the period from 1 January to 30 June 2017;
  - (iii) Does not omit or distort information relevant to the scope of the internal control system being described, while acknowledging that the Description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment.

- (b) The Control Procedures related to the Control Objectives stated in the accompanying Description were suitably designed and operated effectively throughout the period from 1 January to 30 June 2017. The criteria used in making this assertion were that:
- (i) The risks that threatened achievement of the Control Objectives stated in the Description were identified;
  - (ii) The identified Control Procedures would, if operated as described, provide reasonable assurance that those risks did not prevent the stated Control Objectives from being achieved;
  - (iii) The Control Procedures were consistently applied as designed, including that manual Control Procedures were applied by individuals who have the appropriate competence and authority, throughout the period from 1 January to 30 June 2017.

Chairman of the Executive Board



E.V. Astanin

National Settlement Depository

3 October 2017



Section III.

National Settlement Depository:  
Company Profile Provided  
by Management

# Section III:

## National Settlement Depository

### Company Profile Provided by Management

National Settlement Depository serves as Russia's central securities depository and is a member of the Moscow Exchange Group. The Central Bank of Russia has recognized NSD as a systemically important settlement depository, systemically important trade repository. In addition, the Payment System of NSD is recognized as systemically and nationally significant by the Central Bank of Russian Federation.

The Company provides services for on-exchange and over-the-counter (hereinafter, "OTC") transactions with all types of Russian securities and transactions with unit investment funds and securities of foreign issuers and provides bank account (settlement) services, including cash settlements for financial market participants.

#### Key areas of business

##### **Managing customer accounts**

1. Opening/closing accounts/securities accounts.

##### **Managing customer instructions**

1. Deposits/withdrawals of securities using the CSD's nominee holder account;
2. Interacting with trade and clearing accounts when settling trades in securities;
3. Acceptance of securities issues (additional issues)/issue-grade securities for servicing/ removal from servicing;
4. Transfers between securities accounts, control over cash settlements;
5. Transactions with securities on 'delivery versus payment' (hereinafter, "DVP") basis through international clearing and settlement centres and foreign depositories;
6. Liaising with the registrar when a depositor discontinues its nominal holder functions.

##### **Corporate actions (hereinafter, "CA") - Russian securities (mandatory and voluntary actions, including meetings)**

1. Exchanging CA information with registrars;
2. Recording corporate actions in the Company's systems, informing depositors about the upcoming CAs;
3. Helping security holders to exercise their rights in the event of voluntary CAs (processing depositors' instructions);
4. Allocating and transferring CA outcomes (both for mandatory and voluntary CAs);
5. Communicating the CA outcomes to the market.

##### **Corporate actions - foreign securities**

1. Accepting and processing incoming messages from higher-rank depositories/their agents;
2. Recording CAs in the Company's systems;
3. Informing depositors about the upcoming CAs (both mandatory and voluntary) in relation to foreign securities in the Company's accounts with higher-rank depositories;
4. Helping security holders to exercise their rights in the event of voluntary CAs (processing depositors' instructions);
5. Allocating and transferring CA outcomes (both for mandatory and voluntary CAs);
6. Communicating the CA outcomes to the market.

##### **Information management**

1. Recording/ amending questionnaires;
2. Recording/ amending bank details.

##### **Depository services**

1. Opening/closing active safekeeping accounts;
2. Transfers of securities;
3. Shifting of securities;
4. Opening/closing securities sub-accounts;

5. Performing routine business transactions (Operations Department): business day close and preparation of daily accounting records;
6. Performing transactions in the event of share buyback at the request of the shareholder (depositor of the Company);
7. Purchasing/selling shares from/to the Company on own behalf and at own account when performing treasury transactions;
8. Seizure/ removal of seizure on securities;
9. Cancelling non-executed customer orders;
10. Making rectifying entries to correct mistakes made when recording or executing customer orders;
11. Administrative blocking/unblocking of depository transactions;
12. Information-related transactions;
13. Depository services for initial public offering (IPO) shares of Russian issuers;
14. Safekeeping and/ or record-keeping of securities;
15. Withdrawals of securities from record-keeping/safekeeping;
16. Conversion/expedited conversion of depository receipts.

#### **Payment system / cash settlements**

1. Transactions in the Company's payment system;
2. Settlements in exchange markets;
3. Settlements in OTC markets;
4. Settlements on NSD's business transactions;
5. Opening/closing bank accounts;
6. Cash adequacy control;
7. Settlements on transactions of the Central Bank of Russian Federation;
8. Communications with clearing organizations, the Central Bank of Russian Federation and government authorities with respect to execution of agreements entered into and compliance with statutory regulations when opening/closing accounts;
9. Acting as a foreign exchange control agent. Preparing and filing foreign exchange control reports;
10. Settlements with correspondent banks and depository and clearing organizations;
11. Performing transactions in connection with the central depository functions;
12. Performing transactions in Russian rubles and foreign currencies on customer bank accounts;
13. Performing routine business transactions: business day close and preparation of daily accounting records;
14. Providing information on banking transactions, including processing of customer requests and preparing information for government authorities.

#### **Clearing and third-party services**

1. Settlements on DVP transactions;
2. Settlements on repurchase agreements;
3. Servicing of liabilities registered in the collateral management system.

#### **Repository services**

1. Registration of repository participants;
2. Performing repository transactions;
3. Routine closing of repository business day;
4. Preparing and filing repository reports;
5. Rendering services to customers.

#### **Information services**

##### **Corporate Information Centre**

1. Supporting core infrastructure information services for depositors;
2. Development of commercial corporate information products;
3. Development of a fair valuation centre for financial instruments;
4. Creating analytical products for users of financial information;
5. Interacting with domestic and global information vendors;
6. Supporting information provision to customers.

NSD customers are licensed participants of the securities market (1,500+ major banks, investment companies, brokerage houses, etc.).

**Documents and licenses**

NSD operates in accordance with its Articles of Association and is registered with the Unified State Register of Legal Entities. The Company holds a credit institution certificate from the Central Bank of Russian Federation (hereinafter, "Bank of Russia"); a banking license; a depository services license; a clearing services license; and a cryptographic services license.

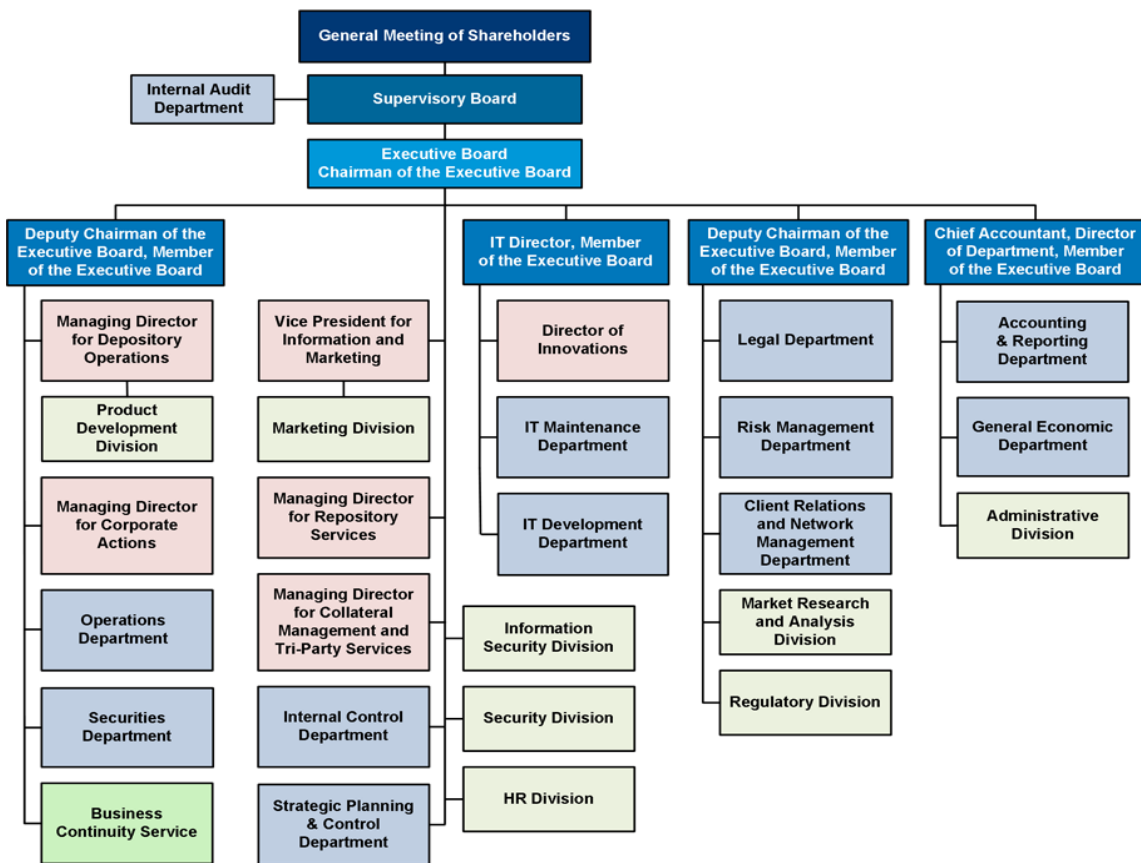
The Central Securities Depository status was assigned by Russia's Federal Financial Markets Service in its Order No. 12-2761/PZ-I of 6 November 2012. Professional Securities Market Participant License No. 045-12042-000100 of 19 February 2009 to conduct depository activities was issued by the Central Bank of the Russian Federation. License No. 3294 of 4 August 2016 to conduct banking transactions was issued by the Central Bank of the Russian Federation. License No. 045-00004-000010 of 20 December 2012 to conduct clearing activities was issued by the Central Bank of the Russian Federation. License No. 045-01 of 28 December 2016 to conduct repository activities was issued by the Central Bank of the Russian Federation.

**Organizational Structure**

In accordance with its Articles of Association, NSD's management bodies comprise:

- General Meeting of Shareholders – a supreme management body convened at least once a year;
- Supervisory Board - a supreme management body acting during the periods between General Meetings of Shareholders. The Supervisory Board members are elected by the General Meeting of Shareholders for the period of one year;
- Chairman of the Executive Board, a sole executive body appointed by the General Meeting of Shareholders; and
- Executive Board, a collegial executive body. Executive Board members are appointed by the Supervisory Board.

The Company's current organizational structure as of the date of this report is presented below.



Picture 1. NSD’s organizational structure

The Deputy Chairman of the Executive Board is responsible for day-to-day operations of the Company’s key business units. NSD’s s key business units comprise:

Client Relations and Network Management Department (CRNMD).

CRNMD is responsible for concluding contracts with customers; accepting instructions from customers; providing customers with reports on transactions made, securities account and bank account statements; and advising customers.

Operations Department is responsible for:

- Providing depositors and internal business units with corporate information regarding issuers, registrars, securities, and corporate actions of issuers;
- Executing corporate actions of issuers;
- Processing and executing customer orders to deposit and withdraw securities, as well as and to process and perform international trades;
- Processing and executing clearing trades;
- Settling trades on exchange and OTC markets in Russian rubles and foreign currencies;
- Settling Delivery Versus Payment customer trades in Russian Federation rubles and foreign currencies using international settlement and clearing organizations such as Euroclear and Clearstream;
- Accepting and executing settlement documents in rubles and foreign currencies;
- Controlling cash movements on Company's NOSTRO accounts in rubles and foreign currencies; and
- Acting as a foreign exchange control agent with respect to customers' transactions.

General Economic Department (hereinafter, "GED") is responsible for invoicing customers and monitoring payments of the invoices issued.

IT Development Department. The department's key functions include:

- Drafting and seeking approvals of terms of reference;
- Arranging and performing software upgrades, testing, implementation and support;
- Analysing and locating incidents arising in the course of software operation;
- Planning development of hardware and software systems at NSD, budget planning and procurement of equipment and software; and
- Communicating with the Moscow Exchange Group on matters related to joint development of software.

IT Maintenance Department is responsible for supporting the Company's use of information technologies and systems. Because the Company's activities, including many of its embedded business process Control Procedures, are heavily dependent on information systems, IT Maintenance Department, along with operational business units, should be considered as a key business unit supporting the Company's work streams.

The duties and powers of employees performing significant tasks are segregated throughout the Company. This principle is documented in the Company's internal regulations, including employees' job descriptions, and implemented as part of the procedures followed and employees' rights of access to information systems. The powers to perform the most significant tasks are delegated to the heads of respective business units. Compliance with the segregation of duties (hereinafter "SOD") principle and the legislative and regulatory compliance is monitored by the Internal Audit Department that is independent of the Executive Board. Certain transactions also require an approval from the Legal Department, Internal Control Department, Risk Management Department.

#### Foreign nominee accounts

After the corresponding part of the Federal Law "On the Central Securities Depository" came into force and the Company was assigned the status of the Central Depository, it became possible for foreign central securities depositories and international settlement and clearing centres to open foreign nominee accounts with the Company. At the same time, foreign securities depositories were allowed to open foreign nominee accounts with Russian depositories. The introduction of foreign nominee accounts can significantly reduce risks that foreign investors are exposed to on the Russian market and can ensure equal rights to local and foreign investors. Given that foreign central securities depositories and international settlement and clearing centres are allowed to open foreign nominee accounts, the Company will be able to continue the process of its integration into the global settlement system by improving bilateral relations with the central securities depositories of Commonwealth of Independent States (hereinafter "CIS") countries, Euroclear, and Clearstream and by opening securities accounts for new settlement institutions that had been unable to have a direct access to the Russian market until the Central Securities Depository was established. The Company acts as the National Numbering Agency in Russia and as the Substitute Numbering Agency for the CIS

countries. In these roles, it assigns ISIN, CFI and pre-LEI/LEI codes to securities. The Company is a direct member of the Banking Electronic Speed Payment System of the Bank of Russia (BESP).

### Corporate governance

In accordance with modern approaches to the corporate governance organization based on the best practice and the requirements of the RF legislation, the corporate governance at NSD covers the overall management of the Company's activities by NSD's General Meeting of Shareholders and Supervisory Board, as well as relations with NSD's executive bodies and other stakeholders (i.e., employees, customers, partners, counterparties, banking regulatory and supervisory authorities, and other government authorities and agencies) related to:

- Setting strategic objectives for NSD and implementing an effective governance system;
- Providing proper incentives for the Company's management and employees to pursue the Company's strategic objectives;
- Balancing shareholders' interests and interests of the Supervisory Board members, executive bodies' members, and other stakeholders; and
- Ensuring compliance with the Russian laws and regulations, the Company's Articles of Association and internal regulations.

The Company adheres to the key of Organization for Economic Cooperation and Development principles of corporate governance reflected in the Shareholders Agreement with respect to NSD, under which the corporate governance system should ensure:

- Equal treatment for all shareholders. All shareholders are entitled to effective protection in case of violation of their rights;
- Observance of the rights of stakeholders established by law;
- Timely and accurate disclosure of information on all material matters related to the Company including the financial position, performance, ownership, and the Company's governance;
- Strategic guidance and efficient monitoring of management by the General Meeting of Shareholders and Supervisory Board.

The Company's corporate governance structure is presented on Fig. 2. The activity and the composition of the units included into the corporate governance structure are governed by the corresponding Regulations.

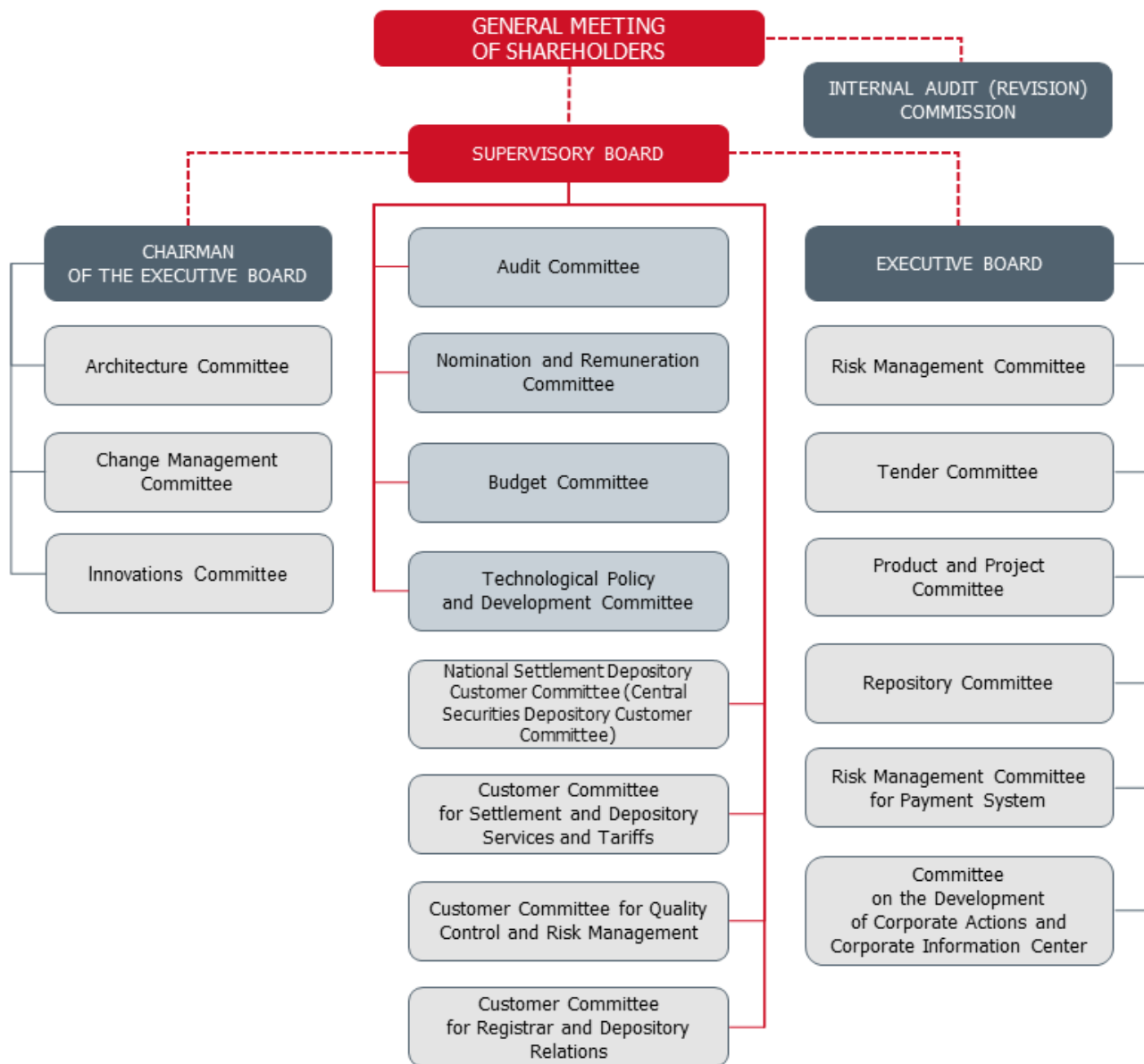


Figure 2. The Company's corporate governance structure

### Risk Management

The Company's senior management, corporate governance bodies and stakeholders are all involved in the risk management process, which is proved by corresponding protocols. Specifically, the risk management process involves the Company's Supervisory Board, the Supervisory Board's Audit Committee, the Customer Committee for Quality Control and Risk Management, the Risk Management Committee for Payment System, the Executive Board, and the Risk Committee. The management's functions and the corporate governance bodies' competencies in relation to risk and control issues are defined in the Company's corresponding internal documents – its Charter, Regulations for commissions and committees, Regulations for specific business units, job descriptions, etc. To ensure sustainability and efficiency of its operations, the Company consistently takes efforts to put in place and ensure the smooth operation of the risk management system, which is adequately aligned with the nature and the scale of the Company's business, the profile of risks it takes, and meets the needs of its further development. The risk management system is designed to ensure identification, assessment and mitigation of risks taken by the Company, as well as to control the related risk exposure and profile.

In its risk management efforts, NSD relies on international risk management practices, and requirements and recommendations of regulators. In particular, NSD has implemented the Three Lines of Defence Model, which addresses the following:

- The first line of defence (heads and employees of NSD's business units other than the Risk Management Department and the Internal Audit Department) is involved in risk identification, information collection, and assessment. They are also part of risk mitigation activities as regards executing business processes within their competencies in accordance with NSD's internal regulations.
- The second line of defence (Risk Management Department) is responsible for developing, implementing and improving the risk management procedures, tools and methodology; managing the risk identification and data collection at NSD; assessing risk levels, performing reviews and offering recommendations for risk mitigation techniques and controls structure. They exert control over implementation of their recommendations; ensure staff awareness about the risk management system in place at NSD; and prepare reports on issues related to risk management.
- The third line of defence (Internal Audit Department) provides assurance and independent analysis of the complete coverage and effectiveness of the risk assessment methodology and risk management procedures at NSD.

The Risk Management Department operates along three lines: financial risks, non-financial risks, and information risks. Financial risk management includes the liquidity risk, the market risk, and the credit risk management. Non-financial risk management involves the operating, strategic, legal, regulatory and reputational risk management. Information risk management is about management of risks associated with the ownership, development, operation and application of information technologies as part of the Company's activities.

#### Business continuity management

The continuity of the company's business processes is one of the most important tasks of NSD's management. In accordance with NSD's mission and operational model, the business continuity management system (BCMS) covers all of NSD's key business areas:

- Central Securities Depository;
- Payment and Settlement System;
- Repository;
- Tri-party Services;
- Information Centre;
- Technological services.

To meet the business continuity objectives, NSD applies the most recent methodologies developed by internationally recognized organizations and best practices, both foreign and domestic. The principal standard the Company seeks to follow in developing the BCMS is ISO 22301:2012 (Societal security — Business continuity management systems — Requirements).

The work aimed at ensuring the reliability of critical processes is done in a systematic and consistent manner. Business continuity management is supported by NSD's senior executives (with the Chairman of the Executive Board being in charge), and necessary resources are being allocated to ensure the proper security of business processes. The Company has a designated business unit responsible for ensuring business continuity — the Business Continuity Service (BCS). The BCS personnel has regular trainings offered by various specialist training organizations.

The Business Continuity Policy is a high-level document that describes the key approaches to the BCMS. This document is updated at least annually to reflect significant changes in the Company's organizational and staff structure or business processes.

The key business continuity objectives include:

- Ensuring the Company's ability to meet its obligations to customers and partners, and preventing disruption of the Company's day-to-day operations;
- Ensuring that all business continuity methods meet the applicable requirements of Russian Federation state authorities, laws and regulations, and the Company's policies, procedures, and plans;
- Mitigating consequences resulting from disruption of the Company's day-to-day operations (including financial losses, loss of data, and loss of reputation);
- Restoring the Company's business processes within the prescribed time limits, in the event of an emergency;
- Determining a list of the Company's critical processes;



- Maintaining the level of management at the Company, which allows for making reasonable and optimal management decisions and their timely and full implementation;
- Ensuring favourable work and safety conditions for the Company's employees, and safe environment for the Company's visitors.

NSD has in place an adequate backup infrastructure (the backup site and backup data centre) that meets all of the requirements applicable to such facilities.

The backup site operates as a "hot site". It is designed to accommodate the Company's mission-critical staff and provides capacities for running the key business processes. The backup site is located five kilometres from the main site. Redundant technical infrastructure, and power suppliers and telecommunications service providers different from those providing services to the main site, mitigate technology-related risks faced by the main site.

The backup data centre is located 16 kilometres from the main site. Both the main and backup data centres are subject to more stringent requirements that are based on the recommendations of the Uptime Institute (USA) laid down in the document "Data Centre Site Infrastructure Tier Standard: Topology".

The main and backup sites are supplied with power independently from each other. Their power supply systems use uninterruptible power sources and diesel generators programmed for automatic operation with the possibility of being manually operated, which are designed to provide emergency power to the Company. The available amount of fuel allows for the operation of diesel generators for eight hours, and thanks to an agreement with a supplier for prompt fuel deliveries self-contained power generation at the Company is ensured for an indefinite period of time. The availability and reliability of the Company's uninterrupted power supply system is ensured through monthly maintenance of uninterruptible power sources and diesel generators, as well as test runs of diesel generators in automatic and manual modes.

NSD has in place Business Continuity and Disaster Recovery Plans that are tested, reviewed, and updated on a continuous basis. The Company also implements various processes aimed at mitigating "non-standard" threats (e.g., the Epidemiological Risk Response Plan).

In addition, the Company runs tests of all elements of the BCMS on an annual basis, in particular:

- Testing of IT systems and technical infrastructure of the backup site (backup site availability testing);
- Testing of diesel generators' automatic operation and testing of the automatic transfer switch designed to switch to accumulators;
- Testing of the restoration of IT systems from backup server rooms/data centres;
- Testing of the interaction between the Moscow Exchange Group companies in case of emergencies.

Test results demonstrate NSD's high reliability as a settlement depository.

To ensure failure-free operation of the Company's IT systems, prevent loss of data, and secure high availability in the event of hardware or software failure, or in the event of emergencies, the Company's IT systems are geographically redundant and interconnected with the use of dedicated communication lines. The Company pays special attention to communication procedures to be used in the event of emergencies, which are tested on a regular basis. In the course of trainings arranged on non-business days, we test processes of cascade telephone alerting of the Company's employees.

As part of the measures aimed at improving the BCMS, we assess the business continuity procedures in order to determine their suitability, adequacy, and effectiveness. Such assessment is made on the basis of the measures taken and test and training results. External auditors are engaged by NSD to assess whether the BCMS meets the best practices in the area of business continuity.

### Risk insurance

On 25 January 2016, NSD and Ingosstrakh signed an agreement for package insurance of the professional securities market participant (Policy 433-151151/16). The insurance period is from 31 January 2016 through to 30 January 2017.

On 20 January 2017, NSD and Ingosstrakh signed an agreement for package insurance of the professional securities market participant (Policy 433-003101/17) for a new period. The insurance period is from 31 January 2017 through to 30 January 2018.

The policy liability limit was fixed at USD 65 million for any and all claims.

The insurance policy covers all property interests of the Company (policy holder) related to any damage inflicted upon them as a result of financial frauds and cyber-crimes (wilful misconduct of the policy holder's

employees and third parties), as well as losses arising from a failure by the policy holder to perform their professional duties to third parties.

The insurance policy covers the types of the Company's activity that are carried out in accordance with its valid licenses, incorporation documents, and contracts, as well as:

- Central Securities Depository services;
- Clearing services;
- Repository services;
- Services associated with safekeeping of securities not related to the depository services; and
- Depository related services.

#### Information security

The information security (IS) framework at NSD complies with the Russian laws, and a set of documents on the standardisation issued by the Bank of Russia (Maintenance of Information Security of the Russian Banking System Organisations - hereinafter, the Bank of Russia Recommendations on Standardisation, or RS BR IBBS), the NSD's Information Security Policy, as well as a number of best practices and international standards. This framework is designed to safeguard assets of customers serviced at NSD, as well as banking, settlement, and information automated solutions in place at NSD. The responsibility for effective management of the information security risk at NSD is vested in the Information Security Department that works to counter potential threats and exposures. In accordance with the RS BR IBBS requirements, the Department actively participates in the development of specifications, implementation of software and hardware solutions, performs vendor due diligence, regulates user access and separation of duties process, sets up and provides technical support for the information protection means, assigns access rights, and maintains key information. To maintain and enhance the achieved IS level, NSD develops information protection solutions designed for automated systems. In the reporting year, the Company launched and successfully completed the project aimed at implementing a vulnerability testing system, made improvements to the automated system of IS related events monitoring, implemented an automated system for recording user authorities and rights, and started the test operation of the centralised access control system on the IDM platform. Also, a confidential information leakage protection solution was deployed. The above-mentioned improvements made it possible to raise the level of security of the NSD's IT environment on the whole, and their critical information systems in particular, mitigate substantially regulatory and operating risks arising as a result of the use of digital solutions. The Company carries out internal activities on a consistent basis to prevent unauthorised access to sensitive information. The span of the IS system has been expanded, with more rigorous controls over the actions of users of information resources put in place, resulting in better efficiency and accelerated response to detected deficiencies. The results of Control Procedures are reported to stakeholders. These reports are used to update the protection processes for confidential information. The Information Security Department works continuously to improve their guidelines and regulations: they perform an ongoing monitoring of legal and regulatory changes and make relevant and timely amendments to existing versions of internal documents.

#### HR policy

As part of its human resources policy, the Company carries out the following main functional activities:

- Designing organisational and staff structures, and making staff list;
- Managing the career development and reward system;
- Managing the financial and non-financial motivation system;
- Performance management;
- Building and developing a corporate training system;
- Staff recruitment;
- Implementing projects on corporate culture development; and
- Human resources administration.

The Human Resources Division's activities are defined and regulated as related to HR administration, staff recruitment, performance management, motivation and social policy, and functional and position hierarchy. The Company has the Code of Professional Ethics approved by NSD Supervisory Board's decision of 16 October 2012.

New joiners sign their Job Descriptions and familiarize themselves with the Internal Work Order Regulations, the Regulations on-the-job safety activities, the Regulations on bonuses, the Regulations on the Corporate Social Policy, the List of Confidential Information, the Instruction on Compliance with the Information Security Procedures, the Memorandum on Information Security Incident Response, the Regulations on Anti-Corruption and Anti-Bribery Activities, and other internal documents, and sign Non-Disclosure Obligation, take induction training on risk management, business continuity, anti-money laundering and terrorism financing, and other compliance procedures.

The Company encourages training and staff development initiatives. Company employees actively participate in international and Russian forums and conferences; attend workshops and training sessions on professional activity-related topics; take secondments and undergo relevant professional certification. Performance appraisal is conducted against both corporate and personal goals. Goals setting and performance appraisal are done on an annual basis. Performance appraisal includes a review of whether an employee has accomplished the set goals and meets the requirements of the corporate competencies and values framework. Candidates for vacant positions are selected in accordance with the established job requirements as confirmed by corresponding line managers, and also in accordance with the requirements of the Bank of Russia.

### Internal control system

The NSD's internal control framework is a combination of internal control bodies and functional areas designed to ensure compliance with the procedures aimed at achievement of objectives set by the laws of the Russian Federation, regulations of the Central Bank of Russia, NSD's incorporation and internal documents. The Company's internal control system appropriately matches the nature and the scope of NSD's business in their capacity as a non-banking lending institution, central depository, professional participant of the securities market, and a clearing house.

The internal control is realised to ensure:

- Efficiency and effectiveness of NSD's financial and operating performance when handling banking and other transactions, and efficiency of assets and liabilities management (including safeguarding of assets), as well as banking risk management;
- Reliability, completeness, objectivity, and timeliness of preparation and submission of financial, accounting, statistical and other reports for both external and internal users; and information security (protection of NSD's interests (objectives) in the information space, defined as a combination of information, information infrastructure, entities engaged in collection, creation, dissemination and use of information, and a system of regulation of relationships arising in this regard);
- Compliance with regulatory and legal acts, standards of self-regulating organisations, NSD's incorporation and other internal documents; and
- Prevention of NSD's involvement and its employees' participation in any unlawful activities, including money laundering and terrorism financing, as well as timely submission of relevant information to government authorities and the Bank of Russia in accordance with the Russian laws. To ensure compliance with Regulation of the Bank of Russia of 16 December 2003 N 242-P "On Internal Control in Credit Institutions and Banking Groups", NSD has established the Internal Control Department and Internal Audit Department, which operate on a permanent basis.

### Information systems

The Company uses several information systems for the purpose of conducting its depository, clearing, and settlement business. Since the Company predominantly operates with uncertificated securities, the role of information systems for the Company's business is seen as significantly increasing. The Company's key information systems (its depository and settlement systems) are located in the Data Processing Centre of Moscow Exchange. Data mirroring in the Moscow Exchange Standby Data Processing Centre has been organised for the Company's information systems. The Company and Moscow Exchange have signed an agreement for rendering services, which provides for Moscow Exchange responsibility and liability in relation to the level of services for the provision of server capacities.

The server room located at the Company's premises accommodates office systems, as well as systems performing auxiliary functions for the Company's core systems. The Company has developed a set of business continuity documents. A business continuity plan is tested on a regular basis, with on-site visits to the backup office.

The Company uses the following information systems (hereinafter referred to as "IS"):

- Alameda - the Company's depository and clearing accounting system;
- ASER - the Company's core hardware/software suite operating online to enable an automated payment process;
- CFT - information system for accounting, balance sheet, preparation of regulatory and internal reporting;
- KBD - corporate database;
- DPO - Alameda add-on, including depository, clearing and repository functionality;
- REPO-X - main system of the Company's repository;
- LUCH (EDM) - software suite that is part of the local workstation of the Company's electronic document management system, enabling information interaction between the participants and the Company through the Company's electronic document management system with the use of e-mail and/or WEB-services;
- Delo - electronic document management system;

- SWIFT – worldwide interbank financial telecommunication and payment system;
- IAS ROP - the Company's business process monitoring system;
- RedMine - system for registering and managing IS changes based on requests, including incidents and errors;
- Omnitracker - processing of phone calls and e-mails in the Help Desk mode for the Company employees.

#### Complementary controls of NSD customers

Various aspects of the internal control environment such as control regulations and Control Procedures presented in this report, cover the specific area of the overall structure of the internal control environment of each of the Company's customers, which pertains to the services provided by the Company. One should also take into consideration the existence of internal control elements with specific Company customers in the combination with the Company's general control framework, as well as the discussed Control Procedures in place at the Company.

In addition, the Company believes that its customers should be responsible for availability of certain control procedures at their end, which are essential for ensuring efficient, correct and controllable interaction with the Company. The Company believes that such control procedures should be in place at their customers, and therefore, many of the Company's internal procedures have been developed based on the assumption that the customer also control procedures its interaction with the Company. Each of the Company's customers should independently assess its own structure of the internal control environment in order to determine the existence of the recommended Control Procedures. The presented list of control procedures reflects only those measures that are related predominantly to information exchange between the customer's staff and the Company. Therefore, the list suggested below should not be considered as an exhaustive list of all potential control procedures. The list of control procedures on the part of the Company's customers, which should be taken into consideration by the customers' independent auditors when they conduct an overview of the general internal control framework on the part of the customers, includes, without limitation, the following control procedures:

- The customers comply with and control compliance with the Company's terms and conditions of depository activities. Information provided by the Company's customers is in compliance with the contracts for rendering depository and clearing services, as well as with other contractual obligations between the Company and the customer. The customers inform the Company in a timely manner about any changes in their banking details, addresses, and telephone numbers.
- The customers are expected to implement appropriate Control Procedures in order to make sure that the Company receives in a timely manner corresponding notifications about deposits of securities to the Company's account.
- The Company is advised in a timely manner by its customers of any changes pertaining to their professional license, any changes in the list of authorised representatives entrusted by the customer to pass and to receive instructions from the Company.
- The customers are expected to properly Control Procedures the process of sending and receiving of messages by electronic communication channels, ensuring appropriate protection of the information and the systems from any unauthorised access or intervention.
- Reports on securities movements and balances, reports on the status of instructions, notifications on transfers of yields on securities, as well as payment statements on writing off funds in payment for cash settlement services rendered by the Company, are reviewed by the customers in a timely manner. Upon detection of any discrepancies, the customers are expected to duly inform the Company to this effect in written form.
- The Company receives on a timely basis instructions pertaining to the issuers' corporate actions.
- In accordance with their contractual obligations, the customers control procedures on a daily basis the content of the Company's website for any requests from the issuers and registrars for the provision of any information, and furnish the required information upon such requests in a timely manner.

The scope of service auditor's engagement does not cover NSD's control procedures applied to monitor the performance of its subcontractor's control procedures which could include the analysis of the assurance report on control procedures at a contractor, as the Company does not engage any subcontractors as part of the services included in the Description.

Section IV:  
Description of Control  
Procedures prepared by  
Management. Testing of  
design and operating  
effectiveness of Control  
Procedures performed by the  
independent auditor

# Section IV: Description of Control Procedures prepared by Management. Testing of design and operating effectiveness of Control Procedures performed by the independent auditor

## Introductory paragraph

This report is intended for customers who have used NSD's services and their auditors, and includes the description of the Company's internal control system and the results of the Control Procedures' testing for operating effectiveness throughout the period from 1 January to 30 June 2017.

This section covers the following information provided by the Company:

- Control Objectives set by the Company's management,
- Control Procedures specified by the Company to achieve the Control Objectives.

Moreover, the following information provided by ZAO Deloitte & Touche CIS is also included in this section:

- Description of Control Procedures' testing performed by ZAO Deloitte & Touche CIS to determine whether the Company's Control Procedures were operating effectively to achieve the Control Objectives. ZAO Deloitte & Touche CIS determined the nature, timing and extent of testing performed;
- the results of Control Procedures' testing performed by ZAO Deloitte & Touche CIS.

Our testing was performed in accordance with International Auditing and Assurance Standards Board International Standard on Assurance Engagements No. 3402 Type 2. Our testing of the Company's Control Procedures was limited to the Control Objectives and related Control Procedures specified in Section IV of this document, and was not extended to controls described in Section III but not included in Section IV, or to the control procedures that may be in effect at the customers.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities to obtain an understanding and to assess control risk at the user entities. Control procedures at user entities and the Company's management components should be considered in conjunction. If there are no effective control procedures implemented at user entities, the Company's management components may fail to make up such deficiencies.

### Description of testing performed

ZAO Deloitte & Touche CIS performed testing of Control Procedures specified in this section for the period from 1 January to 30 June 2017. Such tests covered the Control Procedures that were in place during the period from 1 January to 30 June 2017. Besides, the Control Procedures were tested based on the Control Objectives set by NSD with respect to such Control Procedures.

In addition to the tests below, we have also obtained reasonable assurance, by means of inquiry of key management personnel and Control Procedures' owners, that each of the Control Procedures listed below operated as described throughout the period from 1 January to 30 June 2017. The description of the tests is presented below.

Testing procedure	Description
<b>Corroborative inquiry</b>	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
<b>Observation</b>	Observed the performance of the control multiple times throughout the report period to evidence application of the specific control activity.
<b>Review of documentation/monitoring</b>	We performed the review of the reports and related documents demonstrating the performance of certain Control Procedure.
<b>Reperformance of Control Procedures</b>	We entered the test data, performed the recalculation and compared the expected and final results.

### Report on testing results

The concept of materiality is not applied when reporting the results of tests of Control Procedures for which deviations have been identified because we do not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, we report all deviations.

**Objective 1. Control procedures provide reasonable assurance that accounts are set up and administered in accordance with complete and authorised customer agreements and applicable regulations.**

Nº	Control procedure	Testing performed	Test results
1.1	The CRNMD Director approves an order to open a depo account, and contract with the customer is signed by both parties following the review of the customer's documents by authorised employees of the Legal, Security, Client Relations and Internal Control departments. If no exceptions are identified, the approval sheet is signed by the authorised employees of the above department. If exceptions are identified then the documents are returned to the customer and the contract is not signed.	For a sample of open depo accounts we examined the checklists and ensured that the customers' documents were reviewed by the responsible departments prior to signing the contract and opening the depo account.	No exceptions noted
1.2	Unique account numbers are automatically generated by Alameda (for depo accounts) based on the master-data entered by a CRNMD employee.	Based on the observation of the process for opening depo accounts in Alameda, we ascertained that the unique account number was generated automatically based on the data entered in KBD.	No exceptions noted
1.3	The functionality within Alameda automatically verifies the information (customer orders, memos) entered by an employee of the Operations Department.	We observed the automatic review procedures with respect to the information entered into Alameda/DPO by employees of the Operations Department. Based on the observation, we have ascertained that the system automatically notifies the employee of an error, requiring further actions where incorrect data are entered.	No exceptions noted
1.4	The controller (employee of the Operations Department) verifies whether the information entered into Alameda is matched to the hard copy of the customer order, and makes a review note in Alameda and on a paper order.	For a sample of executed customer and internal orders, we performed the review procedures and ensured that the executed orders and entered data were verified by authorised employees.	No exceptions noted
1.5	An Operations Department employee reviews whether the questionnaire entered into Alameda by an Operations Department employee is matched to the hard copy of such questionnaire and makes a review note on the paper questionnaire and in Alameda.	For a sample of customer questionnaires, we performed the verification procedures and ensured that the data entered into the system were reviewed by authorised employees.	No exceptions noted



Nº	Control procedure	Testing performed	Test results
1.6	An Operations Department employee reviews whether the questionnaire entered in KBD by a Client Relations Department employee is matched to the hard copy of such questionnaire and makes a review note on the paper questionnaire and in KBD.	We examined the sampled customer questionnaires. Based on the examination, we ascertained that the data entered into the system was reviewed by authorised employees.	No exceptions noted
1.7	Employees of the Client Relations Department verify that there are no balances on customers' depo accounts and no debt payable to NSD, and thereupon sign the order to close such depo accounts.	For a sample of closed depo accounts, we examined the documents on balances and debt payable to NSD. Based on the examination, we have ascertained that CRNMD employees review the balances on customers' accounts and debt payable to NSD prior to closing such depo accounts.	No exceptions noted
1.8	As part of the day closure procedures an Operations Department employee reviews the report on procedures completed in Alameda and makes a review note.	For a sample of days, we examined the review procedures performed by an Operations Department employee with respect to the "completed operations" report. Based on the examination, we ascertained that all actions required for initiating and closing a trading day were executed correctly.	No exceptions noted
1.9	Customers' documents are reviewed by authorised departments (Legal, Security and Internal Control Departments) prior to making bank account agreements. Subject to approval by the above departments, the Director of the Operations Department signs the agreement with the customer and makes an order to open the bank or trading account.	For a sample of open bank accounts, we examined the checklists. Based on the examination, we ascertained that the customers' documents were reviewed by authorised departments prior to signing the agreement and opening such bank or trading accounts.	No exceptions noted
1.10	The controller (second independent employee of the Accounts Department) reviews the package of documents, verifies the data entered into ASER against the customer's data and signs off the letters to the tax inspectorate and the customer, report to the accounting department and notice to the market.	For a sample of trading accounts, we ascertained that the customers' documents were reviewed by authorised employees prior to entering the data into ASER.	No exceptions noted

№	Control procedure	Testing performed	Test results
1.11	A 20-digit number is generated by ASER automatically based on the balance account number, currency, type of activity and form of ownership of an organisation, type of account, category of account and customer's ID entered by an Accounts Department employee.	We examined the process of bank account generation. Based on the examination, we ascertained that a new bank account is generated by ASER automatically based on the entered customer's data.	No exceptions noted
1.12	Based on the bank account closure application from a customer, the Head of the Operations Department signs off an agreement termination order.	For a sample of closed bank accounts, we have ascertained that before closing bank accounts, the Head of the Operation Department signed off termination orders and the related bank account closure applications from customers.	No exceptions noted

**Objective 2. Control procedures provide reasonable assurance that balances related to securities are recognized, written off and transferred between customer accounts in an accurate and timely manner, strictly in line with customer instructions and securities certificates (registering their movements) received from the registrars).**

№	Control procedure	Testing performed	Test results
2.1	An employee with the Registrar Relations Department sends requests on a daily basis, asking registrars to provide reasons where they have failed to submit reports with balances (reconciliation requests for balances) for specified issues of securities in nominee accounts with the central securities depository.	Based on the examination of the procedure for the interaction between the Company and the registrars, we have ascertained that the recent reconciliation with respect to the balances for securities in NSD's accounts has been completed. Where reconciliation information was not available, the list of securities issues and registrars was specified in electronic reports and letters with commentaries.	<p>We have made an observation that the results from the requests for reasons for unavailable documents were not always recorded on a formal basis during the audited period.</p> <p>Management response of National Settlement Depository:                      In accordance with the recommendation given by the external auditor about documenting the results of control procedures for verifying the availability of reconciliation inquiries for specific securities issues on the accounts of the nominee holder of the Central Depository, NSD plans to implement an additional journal for ongoing monitoring by means of the information system in order to control the aging of not submitted documents for reconciliation, and regular updating of information.</p>

№	Control procedure	Testing performed	Test results
2.2	The functionality within Alameda automatically generates a message to higher rank depositories and dispatches it via SWIFT while preventing manual changes to message properties.	Based on the observation of the procedure for generating and dispatching messages within Alameda, we have ascertained that Alameda prevents NSD employees from modifying properties of messages to higher rank depositories.	No exceptions noted
2.3	The functionality within Alameda automatically matches a customer order and a report for order execution from the higher rank depository, including booking, removing, or transferring securities between depositors' accounts. Customer orders for which data fails to match are transferred for manual matching.	Based on the observation of the matching process for customer orders, we have ascertained that the functionality within Alameda performs the matching process automatically. Customer orders that could not be matched automatically were matched manually by an employee from the Operation Settlement Department.	No exceptions noted
2.4	Alameda automatically generates a failure message where there is a refusal to proceed with a transaction from the higher rank depository. This message is then automatically sent to the customer while preventing manual corrections.	Based on the observation of the procedure for generating a message with the refusal to proceed with a transaction, we have ascertained that messages were sent automatically while preventing users from modifying message properties.	No exceptions noted
2.5	Messages for transactions in local markets are not sent to higher rank depositories until the Operations Department for Foreign Security Settlements or the Operations Department have checked that the information in a message is correct. Only employees from the Operations Department for Foreign Security Settlements or the Operations Department can access DPO and SWIFT to verify such messages.	We have examined a sample of orders received. Based on the examination, we have ascertained that data entered into DPO were verified by authorized employees from the Operations Department for Foreign Security Settlements. We examined user accounts of DPO and SWIFT system and ensured that only employees from the Operations Department for Foreign Security Settlements or the Operations Department can access DPO and SWIFT to verify such messages.	No exceptions noted

№	Control procedure	Testing performed	Test results
2.6	The Head of the Depository Operations Department checks (i) whether there is a memo from the issuer as regards the replacement of a registrar by the issuer and (ii) a customer order for registrar replacement. Following this, the Head of the Department for Depository Operations signs off the memo. Subject to the approval of a request, the Operations Department makes changes to KBD.	We used a sample of issuers to observe the procedure for the replacement of a registrar. Based on the observation, we have ascertained that the orders for registrar replacement and memos were authorized and prepared in an appropriate manner.	No exceptions noted
2.7	An employee from the Corporate Actions verifies the accuracy of a corporate action entered into KBD and makes a respective note on the paper copy of the questionnaire.	For a sample of corporate actions, we examined paper copies of questionnaires for corporate actions. Based on the examination, we have ascertained that the corporate action data inserted in KBD by the Corporate Actions was checked for accuracy.	No exceptions noted
2.8	KBD automatically generates ISIN codes for new securities, based on the information entered by employees from the Securities Services and Information Support Department.	We observed the procedure for generating and assigning ISIN codes for new securities. Based on the observation, we have ascertained that KBD automatically generates ISIN codes, based on the data entered.	No exceptions noted
2.9	The functionality within ASER prevents processing a payment order from the purchaser of securities unless there is a confirmation that a requested amount of securities has been locked in the depo of a seller.	We observed the procedure for processing payment orders from purchasers of securities. Based on the observation, we have ascertained that ASER prevents processing a payment order from the purchaser of securities unless there is a confirmation that a requested amount of securities has been locked in the depo account of a seller.	No exceptions noted
2.10	Alameda users (NSD employees) cannot access Alameda to modify parameters of the orders made by the depository customers and received via the EDM system.	We examined the lists of user accounts within Alameda. Based on the examination, we have ascertained that users who have the broadest scope of rights to access Alameda do not have an access to modify the parameters of the orders made by the depository customers and received via the EDM system.	No exceptions noted

Nº	Control procedure	Testing performed	Test results
2.11	When accepting securities the authorized employees from the Issuer Relations Department, the Operations Department and the Cash Department make a respective note on a memo order for asset acceptance.	For a sample of memo orders, we have examined the procedure for the acceptance of certificates for safekeeping. Based on the examination, we have ascertained that before accepting securities, the authorized employees verified the information received.	No exceptions noted
2.12	When releasing securities the authorized employees from the Issuer Relations Department, the Operations Department and the Cash Department make a note on a memo order for asset release.	For on a sample of memo orders, we have examined the procedure for releasing securities. Based on the examination, we have ascertained that before releasing securities, the authorized employees verified release documents.	No exceptions noted

**Objective 3. Control procedures provide reasonable assurance that payments are authorized, processed and recorded completely, accurately and on a timely basis.**

Nº	Control procedure	Testing performed	Test results
3.1	An employee (a controller) from the Tax Accounting and Reporting Department verifies a tax agent report generated by the preparer. Where the controller has no comments, he or she makes a respective note on a paper copy of the report.	For a sample of tax reports, we have ascertained that the tax reports were verified by the controller.	No exceptions noted
3.2	All internal instructions related to the process of obtaining tax benefits and withholding taxes must be approved in an appropriate manner.	For a sample of corporate actions, we have observed the process for performing corporate actions. Based on the observation, we have ascertained that the selected corporate actions were authorized and completed in an appropriate manner.	No exceptions noted
3.3	An authorized employee from the function responsible for income payments checks whether payment transactions for yields on securities are processed in full, in an appropriate and timely manner. Based on this check, the authorized employee makes a note on the report on the payments made.	For a sample of corporate actions, we examined reports on payments. Based on the examination, we have ascertained that the reports were appropriately authorized by the head of the income payments function.	No exceptions noted

№	Control procedure	Testing performed	Test results
3.4	An authorized employee from the Operations Departments reviews the document registry that is sent to the Bank of Russia. Subject to the absence of errors, the authorized employee signs off a paper copy of the report. Where the report has errors, the authorized employee looks into the cause of incorrect payments.	We selected dates and registers to examine the procedure for preparing and reviewing registers. Based on the examination, we have ascertained that the registers sent to the Bank of Russia were prepared in an appropriate manner and signed by the authorized employee.	No exceptions noted
3.5	Before entering into currency transactions, the Currency Control Department reviews payment documents and makes notes on the paper copies of payment documents, as well as in ASER.	We sampled payment orders to examine the process of reviewing customer documents. Based on the examination, we have ascertained that the documents were reviewed and authorized in an appropriate manner.	No exceptions noted
3.6	The Head of the Department for settlements in the national currency checks the receipt and processing status of files in ASER. Where files with errors are identified, the Department takes appropriate steps to correct errors by interacting with National Clearing Centre (hereinafter "NCC"), etc.	We sampled dates to examine the procedure of checking files from NCC. Based on the examination, we have ascertained that the files from NCC were checked and free of errors.	No exceptions noted
3.7	The functionality within ASER does not make any changes to amounts unless there is a confirmation from a clearing organization.	Based on the observation of the process for dynamic exchange, we have ascertained that the functionality within ASER cannot not make automatic changes to amounts unless a clearing organization provides a notification of the approval for trading accounts transactions.	No exceptions noted
3.8	The functionality within ASER permits processing an order for settlements under transactions subject to a sufficient balance (securities and funds) in customer accounts and nostro accounts.	We have examined the procedure for checking balances in customer and nostro accounts. Based on the examination, we have ascertained that ASER performs this check automatically.	No exceptions noted
3.9	ASER users cannot access ASER to modify parameters of payment documents within ASER.	Based on the observation of the settings in ASER, we have ascertained that ASER effectively prevents users from modifying parameters of payment documents from customers.	No exceptions noted

Nº	Control procedure	Testing performed	Test results
3.10	The accuracy of manual entries in ASER is checked by an independent employee (a controller) by reconciling primary documents to data in ASER. Subject to the absence of mismatches, the controller signs the document.	Based on a sample of manual entries in ASER, we have examined the data entered into ASER and ascertained that the data was checked by the authorized employees.	No exceptions noted
3.11	The controller uses the paper copy of an order with the quotation and value date to verify the data, with the Cash Settlement Department then generating entries for translation transactions in ASER.	Based on a sample of manual entries for translation transactions, we have examined the related data entered into ASER and ascertained that the data was verified by the authorized employees.	No exceptions noted

**Objective 4. Control procedures provide reasonable assurance that clearing transactions and transfer-agent services are performed in an accurate and timely manner.**

Nº	Control procedure	Testing performed	Test results
4.1	The functionality within Alameda prevents an individual employee from entering the parameters of an issuer and confirming that the data entered is correct.	Based on the observation of the procedure for entering the parameters of an issuer, we have ascertained that Alameda prevents an individual employee from entering the parameters of an issuer and confirming that the data entered is correct.	No exceptions noted
4.2	The functionality within Alameda and ASER does not allow executing matched clearing orders unless the accounts of counterparties have sufficient balances of securities and funds (based on terms DVP).	Based on the observation of the process for executing a matched clearing order, we have ascertained that Alameda executes matched clearing orders only provided that the accounts of counterparties have sufficient balances of securities and funds (based on terms DVP).	No exceptions noted
4.3	The functionality within Alameda automatically matches counter clearing orders: only clearing orders that have been matched are then transferred to the next stage (the balance sufficiency check).	Based on the observation of the process for matching counter clearing orders, we have ascertained that such clearing orders are automatically matched by Alameda.	No exceptions noted
4.4	A transaction that is not ready for processing due to an insufficient balance of securities in the accounts of the transacting counterparties is automatically excluded from the clearing pool.	Based on the observation of the procedure for generating a clearing pool, we have ascertained that transactions with the status "not ready for processing" are automatically excluded by Alameda from the clearing pool.	No exceptions noted



**Objective 5. Control procedures provide reasonable assurance that agreements concluded in the over-the-counter (OTC) market are completely and accurately recorded in the register in a timely manner and are only based on customer orders.**

<b>Nº</b>	<b>Control procedure</b>	<b>Testing performed</b>	<b>Test results</b>
5.1	The functionality within Repo-X automatically reviews orders for registration of master agreements. A master agreement is registered provided that it is free of errors.	Based on the observation of the process for registering master agreements, we have ascertained that Repo-X performs an automatic review of the information received.	No exceptions noted
5.2	An employee with the Repository Department regularly monitors the day closure procedure for correctness. Where errors are identified during a repository day closure, the employee looks into the cause of such errors.	Based on the examination of repository day closure reports, we have ascertained that the steps required for day closures were completed correctly for the period under review.	No exceptions noted
5.3	The functionality within Repo-X automatically assigns the "informing party" status to a new customer.	Based on the observation of the process for assigning the "informing party" status to a new customer, we have ascertained that Repo-X does this automatically.	No exceptions noted
5.4	Employees with the Repository Department review customer information entered into Repo-X and check the availability of the paper copies of questionnaires. The paper copy of a questionnaire is signed subject to the absence of discrepancies.	Based on a sample of customer questionnaires, we have ascertained that the data entered into Repo-X was reviewed by the authorized employees from the Repository Department.	No exceptions noted

**Objective 6. Control procedures provide reasonable assurance that changes to the existing systems and applications are authorized, tested, approved, properly implemented, and documented.**

<b>Nº</b>	<b>Control procedure</b>	<b>Testing performed</b>	<b>Test results</b>
6.1	The environments for development, testing and production of the information systems are separated.	Based on the observation of the development, testing and production environments, we have ascertained that these environments are separated.	No exceptions noted

No	Control procedure	Testing performed	Test results
6.2	Before being implemented, changes to the production environment are subject to an approval from the Change Committee. Changes to SWIFT are subject to an approval before the testing stage begins.	Based on a sample of changes and releases, we have examined change requests and ascertained that the production environments only contain changes and releases that have been approved.  Based on a sample of changes made to SWIFT, we have examined change test requests and ascertained that SWIFT's production environment only contains changes that have been approved and tested.	No exceptions noted
6.3	Only requests that have been included in a release for the Committee for Products and Projects may be transferred for further development and implementation.	Based on a sample of releases, we have examined the minutes of meetings from the Committee for Products and Projects and ascertained that the contents of the releases were approved by the Committee for Products and Projects.	No exceptions noted
6.4	Changes to the information systems other than SWIFT may only be implemented in a related production environment, subject to a successful test.	Based on a sample of changes and releases, we have examined the testing reports and ascertained that the changes were tested before their implementation in a related production environment.	No exceptions noted
6.5	Subject to a change approval from the Change Committee, the change to SWIFT is tested on a pilot server. It is then rolled out to other servers in the production environment provided that the change is free of errors.	Based on a sample of changes made to SWIFT, we have examined change implementation requests and ascertained that before being rolled out to the production servers, the changes had been tested on a pilot server.	No exceptions noted

**Objective 7. Control procedures provide reasonable assurance that logical access to business-critical systems and applications is restricted to authorised individuals.**

No.	Control procedure	Testing performed	Test results
7.1	System developers do not have access to implement changes in the production environments.	We have verified the lists of administrator accounts in the systems and ascertained that developers have no access to the production environments of the information systems of the Company.	No exceptions noted

No.	Control procedure	Testing performed	Test results
7.2	Access to the information systems is password-protected. All password settings are in line with the Company's internal policies.	We examined password settings in the systems and ensured that settings were set in accordance with the Company's Policy of password security for most systems.	<p>We have made an observation that the password settings within ASER, CFT and SWIFT were configured to meet requirements that are less stricter than those in the Policy of password security.</p> <p>We identified that a number of technical accounts and some user accounts at the level of the DBMS (Data base management system) do not meet the requirements of the Policy of password security in full.</p> <p>Management response of National Settlement Depository: The IT Support Department is working to bring all NSD systems into compliance with the requirements of the Policy in the field of password settings in accordance with the previously approved by IS Department plan.</p>

No.	Control procedure	Testing performed	Test results
7.3	Access requests are reviewed and approved by authorised employees before the access is granted.	For a sample of accounts, we have examined the access granting requests. Based on the examination, we have ascertained that such requests were correctly approved and rights, both the requested and granted ones, were consistent.	We could not ascertain whether the process for granting access involves a formal analysis of access rights for the purpose of segregation of duties.  Management response of National Settlement Depository: IS Department implements an automation system for granting access rights.
7.4	Administrative access to the information systems at the level of applications and DBMS is restricted and granted to employees performing administration functions. All administrator accounts are personalized.	We examined the lists of administrator accounts in the information systems and ensured that all administrator accounts are only assigned to employees responsible for administration functions.	No exceptions noted
7.5	User accounts of terminated employees are blocked by information system administrators based on requests from the HR.	We examined the lists of user accounts and ensured that all user accounts of terminated employees were blocked in all systems in a timely manner.	No exceptions noted
7.6	Electronic keys are provided based on relevant requests signed by the requesting employees and power of attorney signed by the Chairman of the Executive Board.	For a sample of employees, we examined the powers of attorney and applications for electronic signature verification key certificates and ensured that electronic keys were provided to employees based on the submitted applications for electronic signature verification key certificates and the powers of attorney signed in an appropriate manner.	No exceptions noted

**Objective 8. Control procedures provide reasonable assurance that business and information systems recovery plans are documented, approved, tested and maintained, day-to-day activities could be restored as required, critical data is regularly saved on back up servers.**

No.	Control procedure	Testing performed	Test results
8.1	Data backup is regularly monitored by information system administrators according to the schedule set in the system. The administrator takes actions to investigate the identified backups errors, if any.	We examined backup logs. Based on the examination, we have ascertained that the latest backups were made in accordance with the schedule.	<p>We identified that backup logs are not kept for the period under audit, and we could not ensure that backup procedures were performed in accordance with the schedule for such period.</p> <p>Management response of National Settlement Depository: Currently, backup logs are stored for a period sufficient to provide operational control of the availability of successfully taken backups. The retention period will be extended to allow for an audit over a long period.</p>
8.2	The Company has the Business Continuity and Disaster Recovery Plans based on which the Business Continuity Service performs regular testing of actions in case of emergency situation and prepares reports on test results and identified deficiencies.	<p>For a sample of testing of the Business Continuity and Disaster Recovery Plans, we examined test reports.</p> <p>We ensured that the Business Continuity and Disaster Recovery Plans are documented, approved and tested.</p>	No exceptions noted

**Objective 9. Control procedures provide reasonable assurance that Information Technology processing is authorised and scheduled appropriately and exceptions are identified and resolved in a timely manner.**

<b>No.</b>	<b>Control procedure</b>	<b>Testing performed</b>	<b>Test results</b>
9.1	Incident statistics and summary reports are prepared by SLA managers on a quarterly basis and approved by heads of relevant departments.	We have examined incident statistics reports. Based on the examination, we have ascertained that these reports are prepared and approved by relevant departments.	No exceptions noted
9.2	Data transfers between the systems are continuously monitored. All incidents are captured and resolved.	For a sample of incidents, we examined the error capturing procedure. Based on the examination, we ensured that all data transfers errors were identified and resolved.	No exceptions noted