



**Independent Service Auditor's Assurance Report on
the Description of Controls, their Design and
Operating Effectiveness for National Settlement
Depository**

For the period from 01.01.2019 to 30.06.2019

**Prepared in accordance with
International Standard on Assurance
Engagements (ISAE) 3402 (type 2)**

October 02, 2019

Contents

- 1 Section I. Independent service auditor's report
- 2 Section II. Management statement provided by NSD
- 3 Section III. Description of internal controls system
- 4 Section IV. Control objectives, related controls and tests performed by the service auditor

**1 Section I.
Independent service auditor's report**



JSC "KPMG"
10, Presnenskaya Naberezhnaya
Moscow, Russia 123112

Tel. +7 (495) 937 4477
Fax +7 (495) 937 4400/99
Internet www.kpmg.ru

Independent Service Auditor's Assurance Report on the Description of Controls, their Design and Operating Effectiveness

To: Non-bank lending institution Joint Stock Company "National Settlement Depository"

Scope

We have been engaged by the non-bank lending institution Joint Stock Company "National Settlement Depository" (hereinafter referred to as "NSD" or the "Company") to report on NSD's Description of its services internal controls system throughout the period from 1 January 2019 to 30 June 2019 (hereinafter – "the Description") as presented in Section III of the Report on the Description of Controls, their Design and Operating Effectiveness for NSD services (hereinafter – "the Service Organization Control report"), and on the design and operation of controls related to the control objectives stated in the Description.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of NSD's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or the operating effectiveness of such complementary user entity controls.

NSD's Responsibilities

NSD is responsible for:

- preparing the Description (in Section III of the Service Organization Control report) and accompanying Statement (in Section II of the Service Organization Control report), including the completeness, accuracy and method of presentation of the Description and Statement;
- providing the services covered by the Description;
- stating the control objectives;
- and designing, implementing and effectively operating controls to achieve the stated control objectives.

Our Independence and Quality Control

We have complied with the independence and ethical requirements established by the *Rules on Independence of Auditors and Audit Firms* and the *Code of Professional Ethics for Auditors* approved by the Audit Council of the Ministry of Finance of the Russian Federation and by the *Code of Ethics for Professional Accountants (including International Independence Standards)* issued by the International Ethics Standards Board for Accountants, which are based on

Engaging entity: JSC "National Settlement Depository"
Registration No. in the Primary State Register Number 1027739132563
Moscow, Russia

Audit firm: JSC "KPMG", a company incorporated under the Laws of the Russian Federation, a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity.

Registration No. in the Primary State Register Number 1027700125628.

Member of the Self-regulated organization of auditors "Russian Union of auditors" (Association). The Principal Registration Number of the Entry in the Register of Auditors and Audit Organisations: No. 11603053203.



Independent Service Auditor's Assurance Report on the Description of Controls, their Design and Operating Effectiveness

fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

We apply the *International Standard on Quality Control 1* and apply accordingly a system of quality control that includes documented policies and procedures for compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on NSD's Description and on the design and operation of controls related to the control objectives stated in that Description, 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 comply with ethical requirements and we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the Description is fairly presented and the controls are suitably designed and operating effectively.

An assurance engagement to report on the Description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's Description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the Description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the Description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organization and described in Section II and III of the Service Organization Control report.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of Controls at a Service Organization

NSD's Description is prepared to meet the common needs of a broad range of user entities and their auditors and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in Section II of the Service Organization Control report. In our opinion, in all material respects:

- (a) The Description in Section III of the Service Organization Control report fairly presents the NSD's services internal controls system as designed and implemented throughout the period from 1 January 2019 to 30 June 2019;
- (b) The controls related to the control objectives stated in the Description were suitably designed throughout the period from 1 January 2019 to 30 June 2019; and



Independent Service Auditor’s Assurance Report on the Description of Controls, their Design and Operating Effectiveness

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the Description were achieved, operated effectively throughout the period 1 January 2019 to 30 June 2019.

Description of Tests of Controls

The specific controls listed in the Description and the nature, timing and results of those tests are presented in Section IV of the Service Organization Control report.

Intended Users and Purpose

This report and the Description of tests of controls in Section IV of the Service Organization Control report are intended only for user entities who have used NSD’s services internal controls system, and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by user entities themselves, when assessing the risks of material misstatements of user entities’ financial statements.

A handwritten signature in blue ink, appearing to read 'S. Zaitsev', with a large, stylized flourish extending from the end.

Stanislav Zaitsev
JSC “KPMG”
Moscow, Russian Federation
02 October 2019

**2 Section II.
Management statement provided by NSD**

Section II: Management statement

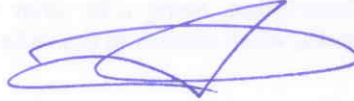
30 September 2019

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 at Section III of the current report fairly presents the internal control system for processing customers' transactions throughout the period **1 January to 30 June 2019**. 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; including, complementary customers' controls contemplated in the design of the service organization controls;
 - 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 **1 January to 30 June 2019**;
 - (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 **1 January to 30 June 2019**. 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; and

- (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 **1 January to 30 June 2019**.

Chairman of the Executive Board



E.V. Astanin

National Settlement Depository

30 September 2019

**3 Section III.
Description of internal controls system**

Section III: General information about National Settlement Depository submitted by the company's management

NSD is systemically important financial market infrastructure operating as central depository, systemically important settlement depository and repository, provider of systemically and nationally important payment system of NSD.

NSD (hereinafter - Company) is a part of the Moscow Exchange Group. NSD settles on-exchange trades and OTC transactions in all types of Russian issuers' securities, trades in mutual fund investment units and foreign issuers' securities, and also provides settlement banking services, including cash settlements on transactions of financial market participants, and clearing services.

NSD's key business areas:

Managing client accounts

1. Opening, maintaining, and closing securities accounts.

Managing client instructions

1. Debiting securities from/crediting securities to client securities accounts;
2. Interacting with trade and clearing accounts when conducting settlements on securities transactions;
3. Transferring securities between securities accounts with monitoring cash settlements;
4. Conducting DVP transactions in securities via international clearing and settlement centers and foreign depositories;
5. Interacting with the registrar when a client stops performing nominee functions.

Corporate actions (CAs) – Russian securities (mandatory and voluntary, including meetings)

1. Exchanging information about corporate actions with registrars/issuers/clients;
2. Recording corporate actions in the Company's systems, informing clients about upcoming CAs;
3. Promoting the exercise of the rights of securities holders related to voluntary CAs (processing client instructions);
4. Drawing up securities holder lists;
5. Distributing and transferring securities and cash based on the results of CAs (mandatory and voluntary ones);
6. Informing market participants about the results of CAs.

Corporate Actions – foreign securities

1. Accepting and processing incoming messages from upstream depositories and their agents;
2. Recording corporate actions in the Company's systems;
3. Informing depositors about upcoming CAs (voluntary and mandatory ones) involving foreign depository receipts, accounted on Company's accounts with superior depositories as a party acting in the interests of others.
4. Promoting the exercise of the rights of securities holders related to voluntary CAs (processing client instructions);
5. Distributing and transferring securities and cash based on the results of CAs (mandatory and voluntary ones);
6. Informing market participants about the results of CAs.

Managing reference data

1. Registering/amending forms of securities;
2. Registering/amending banking details.

Depository Operations

1. Opening/closing an active and passive account for safekeeping;
2. Operations on securities accounts (debiting and crediting, transfers of securities);
3. Moving securities;
4. Opening/closing a securities sub-account;

5. Performing regulatory transactions of the business day by the Operations Department: Closing a business day and generating daily documents;
6. Performing transactions when an issuer repurchase shares upon the request of a shareholder (the Company's client);
7. Conducting transactions related to selling/purchasing securities by the Company itself and at its own expense during the performance of treasury operations;
8. Seizing/releasing securities and other burdens;
9. Canceling a non-executed depository instruction;
10. Making corrective entries to correct errors made during inputting or the executing depository instructions;
11. Fixation of restriction / removal of restriction of disposal of securities;
12. Conducting information transactions;
13. Carrying out depository services provided as part of an IPO of Russian issuers' shares;
14. Accepting securities for safekeeping and/or record keeping;
15. Withdrawing securities from custody and/or record keeping;
16. Converting/speedily converting depository receipts.

Interactions with securities market participants (issuers and registrars)

1. Interacting with issuers, including the processes for concluding and terminating agreements with issuers and for exchanging documents:
 - 1.1 Interacting with bond issuers in regard to servicing bond issues kept in issuer accounts and treasury securities accounts of an issuer;
 - 1.2 Interacting with share issuers in regard to servicing share issues kept in the treasury securities accounts of an issuer;
 - 1.3 Interacting with bond issuers in regard to providing services related to conducting a general meeting of bond holders in the form of an absentee vote, including the performance of ballot committee functions, functions of the secretary of the meeting, and services of processing documents which do not meet ISO standards;
 - 1.4 Interacting with the issuers of commercial papers in regard to services for assigning an identification number to a commercial paper issue, a commercial paper program.
2. Interacting with registrars, including concluding agreements as part of information interchange with NSD or as part of the services provided.
3. Matching own and registrars' data.
4. Providing issuers with services related to shareholders' online voting at general meetings.

Payment system/Cash settlements

1. Conducting transactions via the Company's payment system;
2. Settling transactions on the exchange markets;
3. Settling transactions on the OTC markets;
4. Settling the Company's financial and economic transactions;
5. Opening/closing bank accounts;
6. Checking the sufficiency of funds;
7. Settling Bank of Russia transactions;
8. Exchanging information with clearing organizations, Bank of Russia and government agencies regarding issues related to the execution of agreements concluded and compliance with regulations during the opening/closing of accounts;
9. Performing functions of the currency control agent; Generating and submitting currency control reports;
10. Settling transactions with correspondent banks and foreign depositories and clearing organizations;
11. Conducting operations related to CSD functions;
12. Conducting ruble and foreign currency transactions in client bank accounts;
13. Performing regulatory transactions of the business day, generating business day documents;
14. Submitting information about banking transactions, including processing client requests, and preparing information for government agencies.

Clearing and tri-party services

1. Settling DVP trades;
2. Settling repos;
3. Servicing liabilities registered with the collateral management system.

Repository

1. Registering the participants of repository operations;
2. Maintaining a register of contracts to be reported to the repository;
3. Carrying out the procedure for opening/closing the repository's business day;
4. Generating and submitting repository reports;
5. Supporting repository clients.

Informing party's functions

Corporate Information Center and Valuation Center

1. Supporting basic infrastructural information services for the Company's clients;
2. Receiving information from registrars and issuers of securities and sending it to clients;
3. Developing commercial products in the corporate information sphere;
4. Developing a center for calculating the fair value of financial instruments;
5. Developing analytical products for financial information consumers;
6. Interacting with Russian and global information suppliers;
7. Supporting information provision services.

IT services

1. Connecting clients to NSD's IT services (SWIFT, EDI);
2. Supporting clients who use NSD's IT services;

As Russia's national numbering agency and the substitute numbering agency for the CIS, NSD is authorized to assign international ISIN, CFI and FISN codes. NSD has the status of a Local Operating Unit (LOU), which allows it to assign Legal Entity Identifiers (LEIs) to securities market participant. NSD is a direct participant in the Bank of Russia Real Time Gross Settlement System (BESP System). The company is a member of the Bank of Russia payment system.

Starting in 2017, the Company provides issuers with an E-voting service which allows them to vote at general meetings of shareholders by completing electronic ballots on the website.

The Company's clients include licensed professional and non-professional participants in the securities market (more than 1,500 major banks, investment companies, brokerage companies, etc.) and non-financial organizations.

Documents and licenses

The Company performs its operations in accordance with its Articles of Association. Information about the Company has been input into the USRL. The Company has a certificate of the state registration of a credit organization issued by the Central Bank of the Russian Federation (the Bank of Russia), holds a license for banking operations, a professional securities market participant license for depository operations, a license for clearing operations, a license for repository operations, and a license for information encryption services. The central securities depository status was assigned to NSD by the Russian Federal Financial Markets Services' Order No. 12-2761/PZ-I (dated 6 November 2012). Professional securities market participant license No. 045-12042-000100 for depository operations issued by the Russian Federal Financial Markets Services (19 February 2009). License No. 3294 for banking operations issued by the Central Bank of the Russian Federation (4 August 2016). License No. 045-00004-000010 for clearing activities issued by the Russian Federal Financial Markets Services (20 December 2012). License No. 045-01 for repository operations issued by the Bank of Russia (28 December 2016). License LSZ No. 0009523 for the provision of information encryption services issued by the Center for Licensing, Certification, and Protection of the State Secret of the FSS of Russia, registration number 13169 N (27 September 2013).

Organizational structure

Pursuant to the Company's Articles of Association, its governing bodies include:

- General meeting of shareholders (the supreme governing body). A meeting is conducted at least once every year;
- Supervisory Board - the supreme governing body between general meetings of shareholders. It is elected by the General meeting of shareholders for a 1-year term;
- Chairman of the Executive Board (the sole executive body). He/she is elected by the Company's Supervisory Board;
- Executive Board (the collegial executive body). It is appointed by the Company's Supervisory Board.

The Company's current organizational structure is presented below (Figure 1).

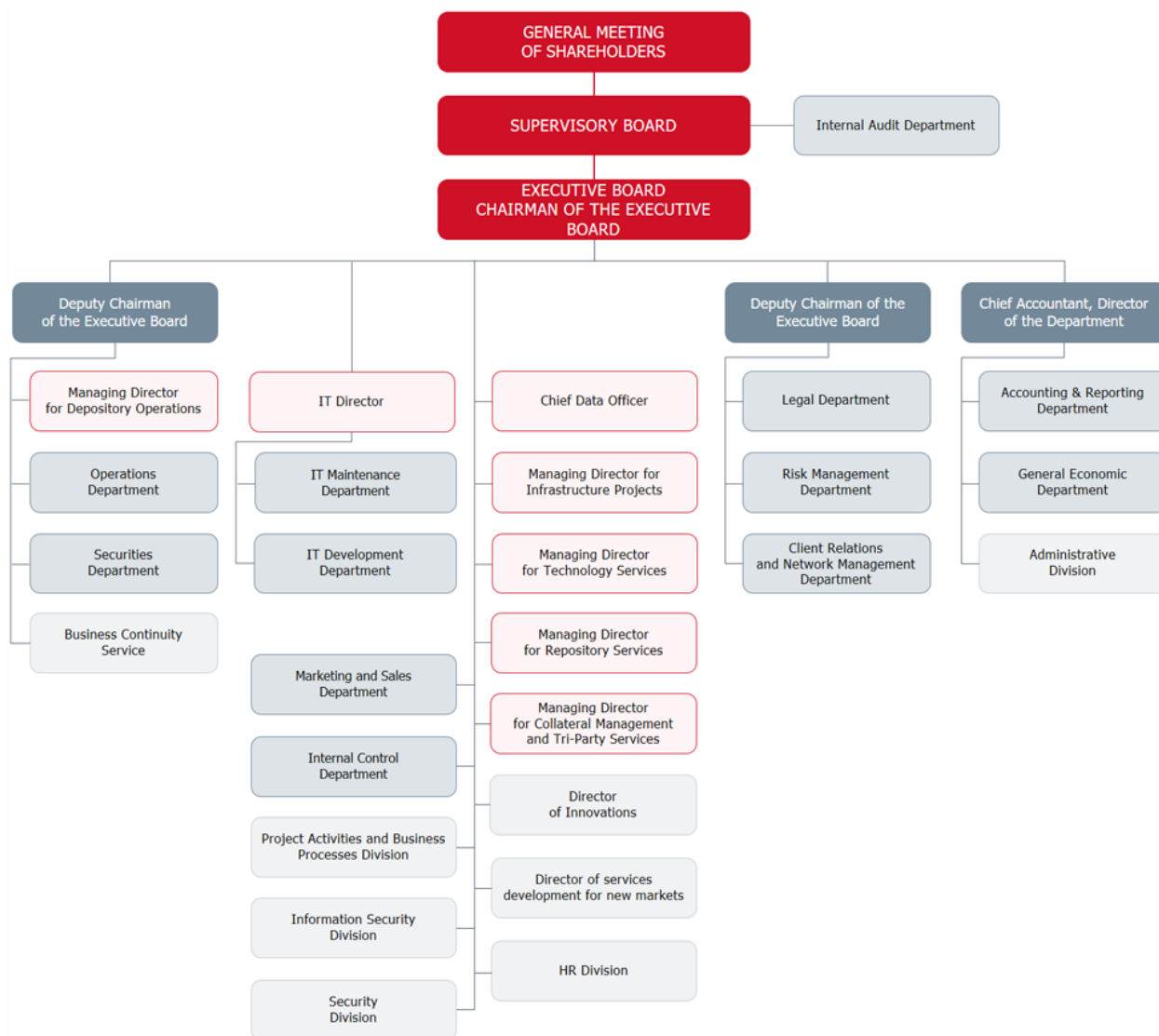


Figure 1. The Company's Organizational Structure

The Deputy Chairman of the Executive Board is responsible for the Company's day-to-day operations and supervises the activities of departments that conduct the Company's core operations. Pursuant to the organizational structure, key divisions responsible for the Company's operational processes include:

The Client Relations and Network Management Department (CRNMD). CRNMD employees are responsible for concluding contracts with clients, receiving client instructions, submitting reports on transactions and statements on securities accounts and bank accounts to the clients, and providing clients with consultations, as needed.

The Operations Department (OD) is responsible for:

- providing clients and the Company's internal divisions with corporate information (about issuers, registrars, securities, and corporate actions initiated by issuers);
- settling transactions in securities and cash following corporate action results;
- processing and executing instructions to debit and credit securities, and to process and execute global transactions;
- processing and executing clearing transactions;
- providing ruble and foreign currency settlements on the on-exchange and OTC markets;
- providing ruble and foreign currency settlements on its clients' DVP transactions in securities involving international settlement and clearing organizations (Euroclear and Clearstream);
- accepting and executing settlement documents denominated in rubles and foreign currency;

- monitoring cash flows into the Company's NOSTRO accounts in rubles and foreign currency;
- performing functions of the currency control agent for client transactions.

The Securities Department (SD) is responsible for:

- interacting with securities market participants;
- concluding contracts with issuers and registrars;
- servicing Russian and foreign issuers' securities issues;
- providing information support when servicing securities issues and processing CAs;
- providing services to process CAs;
- providing services to assign identification numbers to commercial papers.

The Repository Operations Division (ROD) is responsible for the repository's operations, including registering repository operation participants, repository operations, and generating and submitting repository reports.

The General Economic Department (GED). GED's Settlement Division employees are responsible for submitting invoices to clients and monitoring the payment of submitted invoices.

The IT Maintenance Department (ITMD) is responsible for the Company's operations with regard to using information technologies and systems. Given that a significant part of the Company's operations, including many Monitoring procedures as part of business processes, depend on information systems, this department is considered a key part of the organization that provides the working process along with operational units.

The IT Development Department (ITDD). The main functions of the department include the following:

- preparing and approving technical specifications;
- conducting work on software modification, testing, implementation, and maintenance;
- analyzing and containing emergency situations that happen during the use of the Company's software;
- planning the development of the Company's hardware and software systems, planning the budget and procurement of equipment and software;
- interacting with the Moscow Exchange Group with regard to the joint development of software.

The Company follows the principle of the division of responsibilities and authority of employees performing significant tasks as part of business processes. This principle has been formalized in the Company's regulations, including job descriptions, and is implemented as part of the procedures and the employees' rights to access information systems. The authority to perform the most important tasks is assigned to heads of relevant structural units. Compliance with the principle of the division of responsibilities and authority is monitored and analyzed against the observance of applicable laws and regulators' requirements by a unit that is independent from the Executive Board – the Company's Internal Audit Department. In addition to this, certain operations should be approved by the Legal Department, the Internal Control Department, and the Risk Management Department.

Corporate Governance

In accordance with the newest approaches to organizing corporate governance which are based on recent practice and meet Russian legal requirements, NSD's corporate governance is the general management of the Company's operations performed by the General meeting of shareholders and the Supervisory Board and incorporate relationships with the Company's executive bodies and other stakeholders (employees, clients, counterparties, banking regulators, supervisory agencies, and governmental agencies) with regard to:

- setting the Company's strategic goals and effective governance system;
- creating incentives that provide for implementation by the Company's executive bodies and employees all actions required to achieve the Company's strategic goals;
- maintaining the balance of interests of the Company's shareholders, members of the Supervisory Board and executive bodies, as well as other stakeholders;
- ensuring compliance with Russian laws, the Company's Articles of Association, and internal regulations.

The Company follows key corporate governance principles proposed by the Organization for Economic Cooperation and Development (OECD) which are reflected in the NSD shareholder agreement; in accordance with these principles, the Company's corporate governance structure should provide for:

- equal treatment of shareholders. All shareholders shall receive effective protection if their rights are violated;
- observance of the legally protected rights of stakeholders;

- timely and accurate disclosure of information related to all material issues related to the Company, including its financial status, performance, ownership, and management.
- strategic management, effective control over the Company's managers by the General meeting of shareholders and the Supervisory Board.

The Company's corporate governance structure is presented in Figure 2. The activity and the composition of structural units which are part of corporate governance are regulated by relevant provisions.

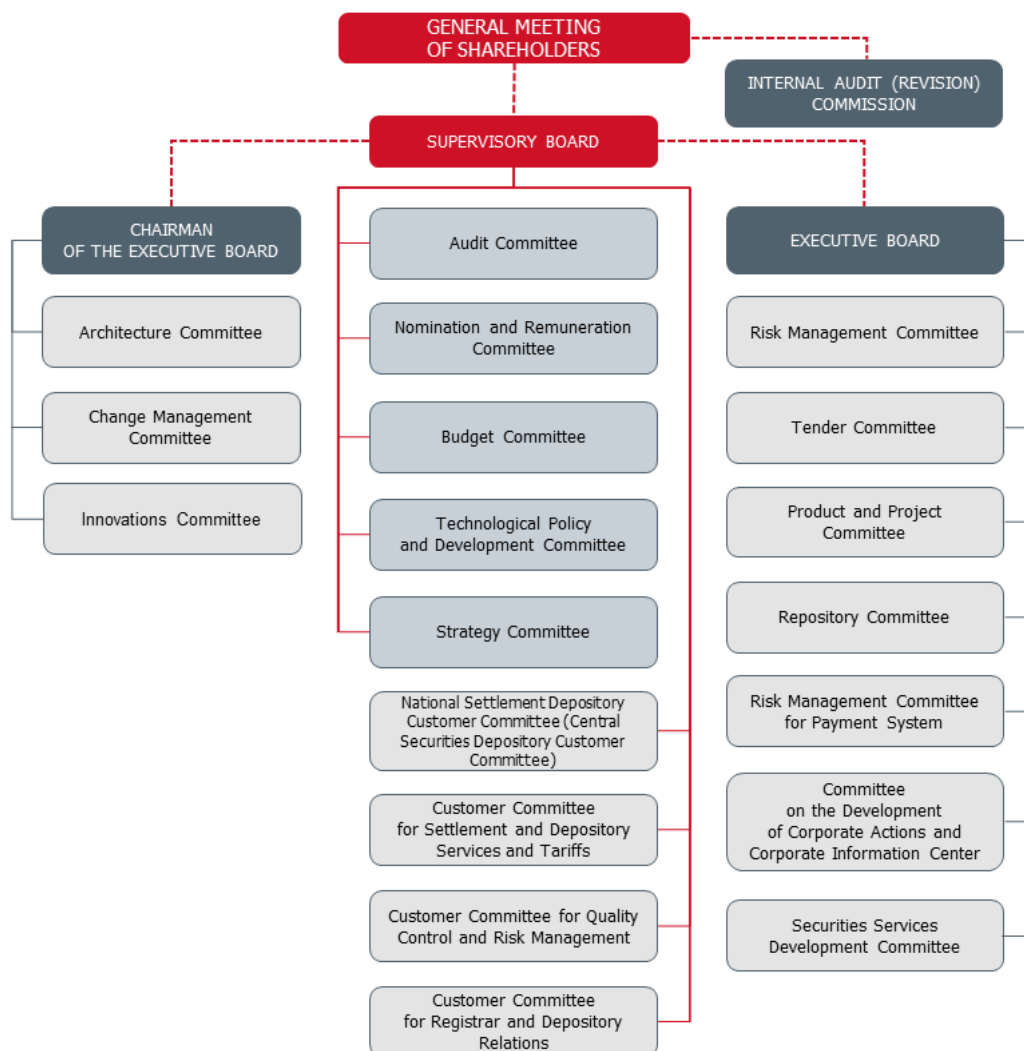


Figure 2. The Company's corporate governance structure

Risk Management

The Company's senior managers, its corporate governance bodies, and its stakeholders are involved in the risk management process; it is verified by relevant protocols. In particular, the Supervisory Board, the Audit Committee of the Supervisory Board, the Customer Committee for Quality Control and Risk Management, the Executive Board, the Risk Management Committee, and the Risk Management Committee for the Payment System of the Executive Board of NSD are involved in the risk management process. Functions of the management and the competence of corporate governance bodies related to risks and control are set in relevant internal regulations, including the Article of Association, regulations on commissions and committees, regulations on divisions, job descriptions, etc.

To provide the Company's sustainability and operating effectiveness, it conducts methodical work on the creation and operation of a risk management system that is relevant to the scale and nature of corporate operations, the profile of risks accepted by the Company, and that meets the requirements for further development of the Company's operations. The risk management system is designed to provide:

The identification, assessment, and limitation of risks accepted by the Company, as well as monitoring their volume and structure.

When managing risks, the Company follows international risk management standards, regulators' requirements and recommendations. In particular, the Company has implemented a model of three lines of defense:

- The first line (level) of defense is represented by all NSD employees. The functions and tasks of the representatives of the first line of defense with regard to the risk management system:
 - identifying, analyzing, and assessing risks in accordance with the procedure provided by NSD internal documents;
 - making management decisions regarding measures of responding to risks, including developing and implementing risk mitigation actions;
 - recording data on risks and risk events in the risk and risk event database;
 - developing separate plans for business process recovery that are included in NSD's unified business continuity and recovery plan; participating in recovery procedures when business continuity was violated; taking preventive measures;
 - implementing NSD executive bodies' resolutions related to risk management.
- The second line (level) of defense is represented by the Risk Management Department and other structural units: the Internal Control Department, the Legal Department, the Business Continuity Service, the Information Security Division, and the Security Division. The Risk Management Department is the center that provides a unified approach to NSD's risk management, that sets a methodology for managing risks and that controls the compliance of risk management processes with current methodology. The functions and tasks of the representatives of the second line of defense with regard to the risk management system:
 - preparing and implementing internal documents regulating the risk management process;
 - organizing and providing for the efficiency of the risk management process;
 - providing methodological support for first line representatives in all phases of the risk management process;
 - assessing risks and preparing proposals aimed at minimizing risk levels;
 - preparing reports on risk management issues.
- The third line (level) of defense is represented by the Internal Audit Department. The functions and tasks of the Internal Audit Department as part of the risk management system include auditing the fullness and effectiveness of the risk management system during audits conducted by the Internal Audit Department. Based on the results of the audits conducted, the Internal Audit Department prepares a report for the Supervisory Board and executive bodies of NSD, including recommendations on eliminating revealed shortcomings, if any.

The Risk Management Department covers three areas: financial risks, non-financial risks, and risk analysis and reports. Managing financial risks entails managing liquidity risk, market risk, and credit risk. Managing non-financial risks means managing operational, strategic, legal, and regulatory risks, as well as reputational risk. Risk analysis and reports is focused on optimizing and automating management and regulatory reports in the risk management field.

Business Continuity

One of key tasks of NSD management is ensuring the organization's high sustainability. In accordance with the Company's mission and its operational model, the business continuity management system (BCMS) covers all key corporate business areas.

To achieve the Company's business continuity goals, it uses the newest methodological developments of recognized international organizations and best foreign and domestic practices. When building the BCMS, the Company strives to comply with ISO 22301:2012 ("Societal security — Business continuity management systems — Requirements").

Key approaches to building the BCMS are approved by NSD's Supervisory Board. Work on providing critical process continuity is systemic and consistent. The Company manages continuity under the direct support of its senior managers and provides enough resources for that. To develop and support the BCMS, there is an independent division in the Company – the Business Continuity Service (BCS). The upper level document that describes the main approaches to the organization of the BCMS is the Business Continuity Policy which is upgraded at least annually or even more often if the Company modifies its HR structure or upgrades business processes.

Key business continuity tasks include:

- maintaining the Company's ability to fulfil its obligations to clients and partners, preventing possible violations of the Company's day-to-day operational mode;
- ensuring the compliance of all business continuity mechanisms with the requirements of Russian government organizations, regulations, and the Company's policies, procedures, and plans;
- minimizing the impact of violations of the Company's day-to-day operational mode (including the amount of material losses, information losses, and the loss of business reputation);
- recovering the Company's business processes within an established time period in emergency situations;
- drawing up a list of the Company's processes critical to interruption or violation;
- retaining the level of the Company's management which allows it to make well-grounded and optimum management decisions and to implement them fully and in a timely manner;
- providing favorable labor conditions and employee safety, as well as the safety of visitors on the Company's premises.

Fully-featured elements of the backup infrastructure function in NSD include the backup office and the backup data processing center which meet the requirements for such facilities.

The backup office was built based on the "hot functioning" principle. The backup office has the capacity to house the Company's critically important personnel and allows to implement key business processes. The backup office is located five kilometers from the main office. The doubled technical infrastructure of the backup office, electric power and telecommunications suppliers that are different from the ones used by the main office minimize main office technogenic risks.

The backup data processing center is located 16 kilometers from the main site. The main and backup data processing centers should meet higher standards based on the recommendations by the Uptime Institute (USA) were offered in the document named "Data Center Site Infrastructure Tier Standard: Topology."

Electric power is supplied via two independent channels to the main and backup office buildings. To provide uninterrupted supply of electric power in emergency situations, the electric power supply systems of both NSD offices have uninterrupted power supply sources (UPS) and diesel generator sets (DGS) that have programmed automatic operation with manual control as an option. Available fuel supply is sufficient for diesel generator plant operation for 8 hours, and an agreement for on current fuel supply concluded with the supplier ensures autonomous power supply for NSD for an indefinite term. Monthly technical maintenance of UPS and DGP, and regular automatic tests of DGP operation in the automatic mode guarantees the operability and fault tolerance of the Company's uninterrupted power supply system.

The Company developed and implemented BCR procedures and plans which are being regularly tested, reviewed, and upgraded. Results of the tests and internal and external checks and audits confirm the high level of the Company's readiness to address non-standard and emergency situations.

Risk insurance

On 20 January 2017, NSD and Ingosstrakh Insurance Joint Stock Company concluded an agreement for complex insurance of a professional securities market participant (Policy No. 433-003101/17) for a new term. Insurance period was from 31 January 2017 to 30 January 2018 inclusively.

On 18 December 2018, NSD and Ingosstrakh signed Additional Agreement No. 1 regarding a change in the insurance period. The new insurance period was from 31 January 2018 to 31 January 2019 inclusively. On 29 March 2019, NSD and Ingosstrakh Insurance Joint Stock Company concluded an agreement for complex insurance for a professional securities market participant (Policy No. 023051/19) for a new term – from 1 April 2019 to 31 March 2020 inclusively.

The insured amount under the agreement was USD 65 million for all insurance events and each insurance event during the effective period.

The insurance policy covers NSD's (the insured party) proprietary interests related to damage inflicted as a result of financial and electronic computer crimes (as a result of the insured party employees' and third parties' wilful activity) and NSD clients' proprietary interests related to losses resulting from the insured party's violations made when performing professional activities.

The policy covers the company's operations related to providing services to clients, in particular, within the framework of NSD's licenses, founding documents, and agreements.

Information security

The Company organized its activities focused on providing information security in accordance with Russian laws, Bank of Russia regulations, and a set of Bank of Russia documents related to the standard "Providing Information Security of the Organizations of the Banking System of the Russian Federation" (BR IBBS). The Company has an Information Security Policy that takes into account best practices and international standards. These activities are focused on providing for the security of client assets when providing them with Company services, as well as of the Company's banking, depository, settlement, and information automated sets. Tasks related to the effective risk management of IS violation risk in the Company were imposed on the Information Security Division (the IS Division) which works to combat possible threats. Pursuant to BR IBBS and Bank of Russia regulations, the IS Division actively participates in the development of technical specifications, implementation of hardware and software systems, evaluates the contractual base, regulates the processes for segregating user access, sets and maintains information protection means, distributes access rights and keeps key information, and checks protection levels.

To maintain and increase the IS level, the Company develops information protection means used when operating automated systems. The Company continues to expand the coverage of the automated system to record access rights and the power of the centralized system users via the IDM (Identity Management) access; a system to protect against the leaking of confidential information was set and is being amended with new rules. The Company is implementing a project focused on mitigating the risks of the use of "zero day" threats by intruders and targeted attacks. The Company is also implementing a program to increase personnel awareness of the newest threats and methods to prevent them. These developments allow NSD to effectively manage risks that emerge when using IT systems. The Company also conducts regular events aimed at preventing unauthorized access to confidential information. Reports on the results of the implementation of these measures and control procedures are prepared; they are submitted to stakeholders and NSD committees, including the Executive Board and the Supervisory Board, and are used as the basis for correcting measures focused on confidential information protection. The IS Division continues to improve the methodological system: legislative and regulatory changes are analyzed on a permanent basis; based on analysis results, internal regulations are amended; if the legislation has significant changes, or new Bank of Russia information security regulations and standards are put into effect, the Company initiates projects to bring internal documents into conformance with new requirements.

HR policy

As part of HR policy, the Company implements the following functional activities:

- designing organizational and staff structure, personnel organization;
- managing the career growth system and remuneration system;
- managing the system of material and non-material incentives;
- managing operational effectiveness;
- designing and developing the corporate training system;
- recruiting personnel;
- implementing corporate culture development projects;
- conducting HR management.

HR Division activities are established and regulated with regard to HR management, recruitment, effective management, incentivization, social policy, and functional and official hierarchy. The Company has a Code of Professional Conduct, which was approved by NSD's Supervisory Board 15 September 2016.

Employees who are hired sign their Job descriptions, read the Internal Labor Conduct Code, the Regulation on Labor Safety, the Regulation on Bonuses, the Regulation on the Remuneration System, the Regulation on Corporate Social Support, the Regulation on Handling Personal Data, the Regulation on Handling Confidential Information, the Instruction on Compliance with the Information Security Regime, the Memo for Responding to Information Security Incidents, the Regulation on Combating Commercial Bribery and Corruption, documents related to compliance and other internal documents, and sign the Confidentiality agreement, and the Consent to Personal Data Processing, attend initial training on risk management, business continuity, information security, and compliance; they take the insider information course, labor safety course, and a course focused on anti-money laundering, combating the financing of terrorism and the financing of the proliferation of weapons of mass destruction.

The Company supports initiatives related to personnel training and development. The Company's employees actively participate in international and Russian forums and conferences, attend workshops and trainings related to their professional sphere, participate in internships, and receive required professional certificates. The effectiveness of activities is assessed based on corporate and personal goals. Goals are set and effectiveness is evaluated every year. Along with assessing the achievement of these goals, the Company takes into account if an employee meets corporate competence and value system requirements. Candidates to fill the vacancies are selected based on established requirements for a position approved by the heads of structural units and Bank of Russia requirements.

Internal Control System

The Company's Internal Control System is a combination of the system of internal control bodies and directions that provides for compliance with the procedure for achieving goals established by Russian laws, Bank of Russia regulations, and the Company's founding and internal documents. The Company's Internal Control System is developed in accordance with the scale and nature of operations conducted by the Company as a non-banking credit organization, a central securities depository, a professional securities market participant, a clearing organization, and a repository.

The Company implements internal control to provide:

- the effectiveness and successful performance of the Company's financial and economic operations when conducting banking and other transactions, the effective asset and liability management (including asset safety provision), and the management of banking risks;
- the reliability, fullness, objectivity and timeliness of financial, accounting, statistical and other statements (for internal and external users), and of information security (protection of the Company's interests (goals) in the information sphere which represents a combination of information, information infrastructure, subjects that collect, generate, distribute and use information, as well as the system for regulating relations that emerge in the course of these activities);
- compliance with regulations, standards of self-regulatory organizations, and the Company's founding and internal documents;
- prevention of the Company's involvement and its employees' participation in criminal activities, including money laundering, the financing of terrorism and the financing of the proliferation of weapons of mass destruction, as well as the timely submission of information to governmental organizations and the Bank of Russia in accordance with Russian laws. To observe Regulation No. 242-P "On the Organization of Internal Control in Credit Organizations and Banking Groups" (approved by the Bank of Russia 16 December 2003), the Internal Control Department and the Internal Audit Department perform their functions in the Company on a permanent basis.

Information systems

To perform depository, clearing, repository, and settlement operations, the Company uses a few information systems. Given that the Company mainly handles non-documentary securities, the role of information systems in the Company's business is significantly increasing. The Company's key information systems are located in the data processing center of the Moscow Exchange. Information systems have backup versions in the Moscow Exchange's backup data processing center. The Company and the Moscow Exchange concluded an agreement to provide information and technological services which set the Moscow Exchange's responsibility and obligations to maintain the level of services rendered to the Company.

Office systems and systems that perform auxiliary functions for the Company's basic systems are located in the server room on the Company's premises.

As part of the BCMS, the Company conducts regular tests of its information resource recovery plan, including in the backup data processing center, including tests that assume employee transfer to the backup office.

The Company uses the following information systems:

- Alameda, the Company's depository and clearing accounting system;
- DPO, an addition to Alameda that includes depository, clearing, and repository functionality;
- ASSES, the Company's main hardware and software system which functions online and automates the cash settlement process;
- CFT, the Company's information accounting system that prepares mandatory and internal reports, it includes the billing module designed to generate settlement documents for submitting invoices for services to clients;
- CBD, the corporate database;
- The Repository, NSD's main repository system;

- LUCH (EDI), a hardware and software system which is a part of the workstation of the Company's electronic interchange (EDI) system and provides information interactions between the Participant and the Company via the Company's EDI systems using email and/or Web service;
- E-voting - NSD's software solution consisted of specialized website for organization and implementation of electronic voting at annual general shareholders meetings and internal system, integrated with various NSD's systems, USAA service, EDI services and providing integration with systems of registrar meetings conduction;
- Web-offices, electronic accounts allowing clients to access NSD services;
- Delo, the EDI system;
- SWIFT, the international interbank system for transmitting information and conducting payments;
- IAS ROP, the system for monitoring the Company's business processes;
- RedMine, the system for registering and managing information system upgrades based on requests, including on incidents and errors;
- OmniTracker, the system for processing telephone and email requests in the Help Desk mode for NSD clients and employees.

Complementary procedures for monitoring NSD clients

Internal control environment aspects, such as provisions and Monitoring procedures presented in this report, cover the general structure of the internal control environment of each client with regard to the Company's services. It is necessary to consider the presence of internal control elements that certain Company clients have, along with the organization of general Monitoring procedures in the Company, as well as the presented Monitoring procedures implemented in the Company.

The Company also believes that clients should be responsible for the presence of their own monitoring procedures that are necessary to provide effective, accurate and well-managed interactions with the Company. The Company believes that clients should have such monitoring procedures, and, accordingly, the Company developed most internal procedures based on the assumption that clients also monitor interactions with the Company. Each Client should independently evaluate its internal control environment to determine the presence of proposed monitoring procedures. The presented list of monitoring procedures shows only those measures that relate to information exchange between the client's personnel and the Company. Thus, the list below should not be perceived as a full list of all possible monitoring procedures. The list of monitoring procedures on the client's side which independent auditors should take note when reviewing the general internal control organization on the client's side, includes the following procedures:

- Clients implement terms and control compliance with the Company's terms and conditions of depository operations. Information provided by the Company's clients corresponds with the terms of depository, clearing, and other services agreements concluded by the Company and clients. Clients inform the Company about any changes in their bank account details, addresses and telephone numbers in timely manner.
- Clients implement appropriate Monitoring procedures to ensure that the Company receives notices of crediting securities in the Company's account on time.
- Clients inform the Company about all amendments related to their professional licenses, lists of persons authorized to send and receive instructions from the Company.
- Clients control the process of sending and receiving messages via digital communications channels, protecting information and systems from unauthorized access or impact.
- Reports on securities flows and balances, instruction status reports, notices of securities income payments, and notices of debiting funds as payment for cash and settlement services provided by the Company should be reviewed by clients in a timely manner. Clients will send to the Company a written notice of any discrepancy found in a timely manner.
- Instructions to process issuers' corporate actions should be sent to the Company in a timely manner.
- Based on contractual obligations, clients should view the content on the Company's Website on a daily basis to check the presence of issuers' and registrars' information requests and submit the required information in a timely manner.

The scope of the work of the organization's auditor providing services does not cover the Company's Monitoring procedures used to check the efficiency of the counterparty's monitoring procedures that may include the analysis of the conclusion that provides the Company with reassurance regarding the counterparty's monitoring procedures, as the Company does not use counterparties within the framework of services listed in the Description.

Summary of control objectives

In this section, NSD has specified the control objectives that it believes are relevant to its clients and their independent auditors, and has identified the related controls in place to achieve those objectives.

Control Objective 1: Controls provide reasonable assurance that account opening and managing is performed in compliance with existing agreements and legislation.

- 1.1. Depo account, bank account or issuer account could be opened based on concluded agreement with a client, or a client's written request to open account within the terms of the agreement.
- 1.2. An Operation Department employee (checker) checks whether the questionnaire entered into Alameda system by an Operations Department employee (maker) is matched to the hard copy of such questionnaire and makes a review note in Alameda.
- 1.3. Depo account, bank account or issuer account can be closed based on respective client's instructions within termination of contract, account closure client's instructions or liquidation of legal entity.
- 1.4. Unique account numbers are automatically generated by Alameda for depo accounts based on the order entered by an employee in CDB system.
- 1.5. Employees of the Client Relations Department verify that there are no balances on clients' depo accounts and debts and after that sign the order to close such depo accounts.
- 1.6. After account opening an employee of the Accounts Department (a controller) signs a notification to tax authorities, prepares a notification to client and to a respective market (for trading accounts only).
- 1.7. The 20-digit account number is automatically generated by the ASER information system based on the currency, activity type and ownership of the organization, type of account, and client ID entered by the employee of the account opening and maintenance department.
- 1.8. ASER prevents bank account closure with non-zero balance.
- 1.9. When accepting securities certificates, securities are placed on the issuer account based on a signed deed of transfer under the "double data entry" control by the Operation Department staff.

Control Objective 2: Controls provide reasonable assurance that deposits, writing off, transferring securities balances on/ from clients' accounts are performed correctly, in timely manner and are based on client instructions or certificates from Registrars.

- 2.1. In case of absence of a daily reconciliation with Registrars for any securities emissions, a responsible employee from Registrar Relations Department investigates reasons why Registrars have failed to submit reports with balances (reconciliation requests) for specified issues of securities on NSD nominee accounts. The reasons of the lack of reconciliation are recorded.
- 2.2. Reconciliation with Foreign Depositories is based on the balances reports and performed on a daily basis. Any discrepancies are identified automatically, analysed and resolved (if any).
- 2.3. The Alameda functionality automatically verifies the information (client's depo instructions, internal notes) entered by an Operation Department employee.
- 2.4. An Operations Department employee (a checker) reviews the information entered into the Alameda system by the Operation Department employee (a maker) for compliance with the paper form of a client's instruction and drops a checking mark in the Alameda system.
- 2.5. Alameda users (NSD employees) do not have access to change the parameters of client instructions received through the EDI system.
- 2.6. Alameda functionality does not allow client instructions processing without a confirmation that required for the transaction amount of securities has been blocked on an account.
- 2.7. Alameda functionality automatically generates a message to Foreign Depositories and proceeds it via SWIFT (for foreign securities) and to the Registers via the EDI system (for Russian securities) preventing manual changes of messages.
- 2.8. Alameda functionality automatically matches a client depo instruction and an execution report from the Foreign Depository, and performs charging, writing-off, or securities transferring between clients' accounts. Client instructions for which data does not match are transferred for manual matching.
- 2.9. Alameda functionality automatically generates a message about a transaction processing refusal obtained from a Foreign Depository. Further, this message is automatically sent to a client preventing manual corrections.

- 2.10. SWIFT messages for transactions with foreign securities in local markets (with "Domestic" tag) are sent to Foreign Depositories only after a checking of correctness by two independent employees ("four-eye" control).
- 2.11. As part of the day-closure procedures, an Operation Department employee reviews the procedures completed report and drops a mark of the performed review.
- 2.12. For variety of mandatory corporate actions (SPLF, MRGR, DVCA, SPLR, SOFF, CAPG, CAPD, DVSE) with foreign securities which have one storage location, an initial message registration, a corporate action forming and generation of an instruction to inform clients are done in the CDB system automatically upon receiving a message from upstream storage.
- 2.13. Notification about a corporate action (Russian and foreign securities) is sent to NSD clients by the Alameda system automatically through the NSD's EDI channels based on a list of securities holders formed in the CDB system.
- 2.14. Instructions for participation in a corporate action (Russian and foreign securities) are registered in the system automatically. Information about errors in instructions processing is communicated to responsible employees via the department's corporate mailbox.
- 2.15. The e-voting system does not allow NSD's employees making changes in an established shareholder meeting, as well as in a list of the meeting's participants.
- 2.16. NSD employees monitor the main statuses of a shareholder meeting (voting opened/ registration opened/ voting completed/ meeting ended) via automatic system notifications. In case of any malfunctions of the system, the reasons are investigated and resolved.
- 2.17. NSD, as a National Numbering Agency, assigns ISIN codes for financial instruments automatically in the CDB system without modifiability.

Control Objective 3: Controls provide reasonable assurance that payments made based on clients' instructions for the transfer of funds authorized, processed and recognized completely, accurately, and in a timely manner.

- 3.1. Entering and changing of tax rates in the reference directory of Alameda system is possible only with verification by a second employee.
- 3.2. When calculating tax payments, the tax rate is applied automatically based on electronic client disclosures using electronic tax rate reference directories. A tax agent report is generated automatically in the Alameda system.
- 3.3. Alameda automatically creates a list of recipients of cash income payments based on the client's securities balance at holder-of-record date.
- 3.4. The distribution of income payments is proceed automatically in the DPO system only after checking of received funds completeness.
- 3.5. An authorized employee of the income payment department checks the correctness of automatically generated payment orders and sends them to the ASER system for execution with preventing manual corrections.
- 3.6. An authorized employee from the Operation Department reviews a register of documents that is sent to the Bank of Russia. In case of error absence, the authorized employee signs paper copies of the documents. If the Bank of Russia declines payment orders, the authorized employee investigates causes of rejection.
- 3.7. Before currency transactions processing, the Currency Control Department employees review payment documents and drop a mark in ASER system.
- 3.8. On a daily basis, an authorized employee of the Operation Department of payment in a national currency processes files received from NCC (National Clearing Centre) in the ASER system. If files with errors are detected, the department employees take the necessary actions to resolve them (interaction with NCC, etc.).
- 3.9. The ASER functionality automatically makes changes on client's trading accounts only after relevant confirmation from a NCC.
- 3.10. The ASER functionality permits processing settlement instructions only with sufficient cash balances on client's accounts and nostro account.
- 3.11. ASER users do not have an access to modify parameters of payment documents within ASER system.

- 3.12. The correctness of manual entries in ASER system is checked by an independent employee of Operation Department (a checker) within reconciling original documents to data in ASER. In case of mismatches absence, the employee (a checker) signs the document.
- 3.13. An employee of the Operation Department (a checker) reviews the correctness of entered data in the ASER system for compliance with an exchange rate and date of valuation of currencies specified in a paper document. The posting of entries for conversion transactions in the ASER information system is performed automatically.
- 3.14. On a monthly basis, the responsible employee starts the automatic procedure for calculating service fees and generating payment documents (service payment invoice, protocol of provision of services, statement of settlement services) in the CFT-Bank system (the module "Billing"). Any changes (if necessary) in calculated services (making adjustments, service cancellation) require confirmation by the second user (a checker).
- 3.15. For calculating fees for agent services and providing technical access to SWIFT services, as well as for generating payment documents (service payment invoice, protocol of provision of services, statement of settlement services) in the CFT-Bank system (the module "Billing") information is entered manually into the system under the double data entry control.

Control Objective 4: Controls provide reasonable assurance that clearing operations and transfer-agency services are provided correctly and in a timely manner.

- 4.1. Alameda functionality prevents an individual employee from entering the parameters of an issuer and confirming that the data entered is correct.
- 4.2. Data transmission through a secure communication channel is automatic. In case of errors, NSD informs the client with automatic notification.
- 4.3. Alameda functionality allows executing of matched clearing instructions only in case when counterparties accounts have sufficient balances of securities or funds (based on terms DVP - Delivery Versus Payment).
- 4.4. Alameda functionality automatically matches counter clearing instructions and transfers to the next stage (awaiting for the sufficient balance) only matched instructions.
- 4.5. A transaction that is not ready for processing due to an insufficient balance of securities or funds on accounts are automatically excluded from the clearing pool.

Control Objective 5: Controls provide reasonable assurance that the accounting of agreements and contracts concluded on the third market, in the register there are taken place timely, correctly and only based on instructions from clients.

- 5.1. Repository functionality automatically checks incoming instructions for registration of general agreements/ contracts. In case of errors absence, general agreements/ contracts are registered automatically.
- 5.2. The sequence and execution of scheduled procedures in a frame of Repository operation day closure process is monitored automatically on a daily basis. The correctness of executing procedures and operation day closure is additionally checked by an employee of the Repository Operation Department. In case of errors in the Repository operation day closure process, reasons are investigated, incidents are recorded and their resolution is monitored, if any.
- 5.3. Repository functionality automatically appoints a new client as a reporting agent.
- 5.4. In case of submitting a questionnaire (an instruction) by a client in paper form, employees of the Repository Operation Department check the information entered into the Operator's Workstation (Repository web-cabinet) for compliance with the paper version of the questionnaire. In case of discrepancies absence, the questionnaire is signed and sent to register in the Repository system.

Control Objective 6: Controls provide reasonable assurance that the changes to existing systems, applications and programs, as well as the development and implementation of new systems, applications and programs, are carried out by authorized employees with the required approval, testing, implementation and documentation procedures.

- 6.1. There are separate segments of information systems for the development, testing and production implementation.
- 6.2. Prior to installation in a production environment, all changes are approved by the Change Committee. Changes to the SWIFT system are approved before testing phases.
- 6.3. Only those change requests that were included in the release to the Products and Projects Committee proceed with development and can be implemented.
- 6.4. Changes into information systems (except for the SWIFT system) are installed in production environments only after successful testing.
- 6.5. After a change of the SWIFT system has been approved by the Change Committee, the testing is performed on the pilot server and, if there are no errors, it is installed on the other servers of the production environment.

Control Objective 7: Controls provide reasonable assurance that the issue of logical access rights to information systems and data is carried out only by authorized persons.

- 7.1. Developers do not have access to install updates in the productive environments of information systems.
- 7.2. Access to information systems is password protected, all password protection settings in the systems comply with the policies of NSD.
- 7.3. Access rights requests obtain all necessary approvals.
- 7.4. Administrative access to information systems at the application and database level is limited and granted to employees who perform the functions of administering information systems.
- 7.5. Information system administrators block accounts of dismissed employees based on a request from the HR department.
- 7.6. Electronic keys are provided on the basis of a request signed by the employee for whom the key will be made, and a power of attorney signed by the Chairman of the Executive Board.

Control Objective 8: Controls provide reasonable assurance that plans for the restoration of information systems and business activities are documented, approved, tested and maintained, if necessary, daily activities can be restored, critical data is stored on backup servers on a regular basis.

- 8.1. Information system administrators monitor performing of scheduled backups. In case of errors, administrators will investigate reasons of backup errors.
- 8.2. The Company has Business Continuity Plans for ensuring continuity and restoration of activity based on which, on a regular basis, employees of the business continuity service perform testing of Disaster Recovery Plans and report results of testing and identified deficiencies.

Control Objective 9: Controls provide reasonable assurance that the processing of operations in the field of information technology is authorized and carried out according to the schedule, and errors / failures are detected and resolved.

- 9.1. Managers responsible for the service level agreement periodically issue summary reports of incident statistics and coordinate with the heads of the respective departments.
- 9.2. In the Company there is monitoring of data transmission between systems. All failures and incidents are recorded and resolved.
- 9.3. On a daily basis, employees of the Information Products and Services Department check the availability and correctness of updated data in information products via automatic and manual tests. Based on test results, a relevant report is communicated to the management.
- 9.4. After the completion of planned updates and in case of any malfunction of the NSD's information site, responsible IT and Information Products and Services Department staff are notified by automatic notifications via e-mail.

**4 Section IV.
Control objectives, related controls and tests
performed by the service auditor**



Testing approach

Our tests of the control environment included the following procedures, to the extent we considered necessary:

- reviews of NSD's organizational structure including the segregation of functional responsibilities, policy statements, accounting and processing manuals, human resource policies and the corporate audit and compliance units' policies, procedures and reports;
- inquiring management and responsible personnel on developing, ensuring adherence to, and applying controls;
- observations of personnel in the performance of their assigned duties;
- inspection of documentation subject to the control;
- re-performance the operation of a control to ascertain that it was performed correctly.

The control environment was considered in determining the nature, timing and extent of the testing of controls relevant to achievement of the control objectives.

Testing of relevant system generated reports was performed to ensure accuracy and completeness of reports used in evaluating controls measures required to achieve controls objectives.

To assess operational effectiveness of automatic controls for which it was not possible to test these controls over the audited period, we tested the operational effectiveness of the main IT controls (i.e. information systems change management), that significantly affect the automatic component of control.

Test procedures were performed for the period 01.01.2019 - 30.06.2019 ("audited period").



Control objectives, related controls and tests performed by the service auditor

The following tables set out the control objectives and control procedures identified by NSD's management and the tests which KPMG have undertaken and the results of those tests. In addition, exceptions to those control procedures identified by KPMG within the Independent Service Auditor's Report are annotated alongside the appropriate control procedure.

Control Objective 1:

Controls provide reasonable assurance that account opening and managing is performed in compliance with existing agreements and legislation

Controls Specified by NSD	Test Performed by KPMG	Result of Testing
Contracts concluding and managing of client's questionnaires		
1.1 Depo account, bank account or issuer account could be opened based on concluded agreement with a client, or a client's written request to open account within the terms of the agreement.	For haphazardly selected accounts opened during the audited period, we inspected confirmation documents for opening them. We noted that the selected accounts were opened on the basis of a new agreement or a request from the client within the terms of the relevant previously concluded agreement.	No exceptions noted
1.2 An Operation Department employee (checker) checks whether the questionnaire entered into Alameda system by an Operations Department employee (maker) is matched to the hard copy of such questionnaire and makes a review note in Alameda.	We inspected the entire population of questionnaires in the Alameda system and noted that all questionnaires were entered and checked for compliance with the paper version of the questionnaire by different employees of the Operations department.	No exceptions noted
1.3 Depo account, bank account or issuer account can be closed based on respective client's instructions within termination of contract, account closure client's instructions or liquidation of legal entity.	For haphazardly selected accounts closed during the audited period, we inspected confirmation documents for their closure. We noted that all selected accounts were closed on the basis of termination of the contract, the client's instruction to close the account or due to the liquidation of the legal entity.	No exceptions noted



Controls Specified by NSD		Test Performed by KPMG	Result of Testing
Depo accounts management			
1.4	Unique account numbers are automatically generated by Alameda for depo accounts based on the order entered by an employee in CDB system.	We re-performed the procedure for opening a depo account in the Alameda system and noted that an account's number was generated automatically without modifiability.	No exceptions noted
1.5	Employees of the Client Relations Department verify that there are no balances on clients' depo accounts and debts and after that sign the order to close such depo accounts.	For haphazardly selected accounts, we inspected requests to the operations department for balances checking before the accounts were closed. We noted that all selected accounts were closed after confirmation from the operations department that there were no balances on the selected accounts.	No exceptions noted
Bank accounts management			
1.6	After account opening an employee of the Accounts Department (a controller) signs a notification to tax authorities, prepares a notification to client and to a respective market (for trading accounts only).	For haphazardly selected bank accounts opened in the audited period, we inspected generated notifications to tax authorities, to clients, and to relevant markets (for trading accounts). We noted that for all selected accounts necessary documents were generated and signed by the controller.	No exceptions noted
1.7	The 20-digit account number is automatically generated by the ASER information system based on the currency, activity type and ownership of the organization, type of account, and customer ID entered by the employee of the account opening and maintenance department.	We re-performed the procedure for opening a bank account in the ASER system and noted that an account number was automatically generated based on the data entered by the employee of the opening and maintaining accounts department.	No exceptions noted
1.8	ASER prevents bank account closure with non-zero balance.	We re-performed the procedure a bank account closure with a non-zero balance in the ASER system and noted that the system did not allow closing the bank account with a non-zero balance.	No exceptions noted



Controls Specified by NSD	Test Performed by KPMG	Result of Testing
Issuer accounts management		
1.9 When accepting securities certificates, securities are placed on the issuer account based on a signed deed of transfer under the "double data entry" control by the Operation Department staff.	For haphazardly selected "Acceptance of Securities for Storage and / or Accounting" instructions executed during the audited period, we inspected the deeds of transfer / electronic certificates, on the basis of which placing was made. We noted that all selected instructions were proceeded in a timely manner and under the "double data entry" control.	No exceptions noted



Control Objective 2:

Controls provide reasonable assurance that deposits, writing off, transferring securities balances on/ from clients' accounts are performed correctly, in timely manner and are based on client instruction or certificates from Registrars.

Controls Specified by NSD	Test Performed by KPMG	Result of Testing
Reconciliations		
2.1 In case of absence of a daily reconciliation with Registrars for any securities emissions, a responsible employee from Registrar Relations Department investigates reasons why Registrars have failed to submit reports with balances (reconciliation requests) for specified issues of securities on NSD nominee accounts. The reasons of the lack of reconciliation are recorded.	For haphazardly selected dates from the audited period, we inspected the reconciliations with the Registrars. We noted that in case of absence of a daily reconciliation for any securities emissions, an employee of the department recorded this fact and investigated reasons of the lack of reconciliation.	No exceptions noted
2.2 Reconciliation with Foreign Depositories is based on the balances reports and performed on a daily basis. Any discrepancies are identified automatically, analysed and resolved (if any).	For haphazardly selected dates from the audited period, we inspected reconciliations with Foreign Depositories. We noted that for selected dates there were no discrepancies in reconciliations.	No exceptions noted
Client's instructions management		
2.3 The Alameda functionality automatically verifies the information (client's depo instructions, internal notes) entered by an Operation Department employee.	We re-performed the procedure for an instruction entering into the Alameda system and noted that the system's functionality automatically verified the information entered by the Operations department employee.	No exceptions noted
2.4 An Operation Department employee (a checker) reviews the information entered into the Alameda system by the Operations Department employee (a maker) for compliance with the paper form of a client's instruction and drops a checking mark in the Alameda system.	For haphazardly selected instructions received in paper form during the audited period we inspected and noted that all selected instructions were entered into the system correctly in accordance with the paper form of received instructions and under the "maker/checker" control.	No exceptions noted



Controls Specified by NSD	Test Performed by KPMG	Result of Testing
2.5 Alameda users (NSD employees) do not have access to change the parameters of client instructions received through the EDI system.	We examined the Alameda system functionality and noted that NSD employees do not have ability to edit instructions after they were accepted for execution.	No exceptions noted
2.6 Alameda functionality does not allow client instructions processing without a confirmation that required for the transaction amount of securities has been blocked on an account.	For a haphazardly selected client instruction we inspected the instruction execution process. We noted that the process was suspended due to insufficient amount of securities on a client's account. Once a sufficient number of securities appeared on the account, they were blocked and the instruction was executed.	No exceptions noted
2.7 Alameda functionality automatically generates a message to Foreign Depositories and proceeds it via SWIFT (for foreign securities) and to the Registers via the EDI system (for Russian securities) preventing manual changes of messages.	For a haphazardly selected client instruction we inspected that the message to the Depository was generated on the basis of the original instruction and was automatically sent without modifiability.	No exceptions noted
2.8 Alameda functionality automatically matches a client depo instruction and an execution report from the Foreign Depository, and performs charging, writing-off, or securities transferring between clients' accounts. Client instructions for which data does not match are transferred for manual matching.	For a haphazardly selected client instruction, we inspected that it was executed automatically based on the confirmation of successful settlement received from a Foreign Depository.	No exceptions noted
2.9 Alameda functionality automatically generates a message about a transaction processing refusal obtained from a Foreign Depository. Further, this message is automatically sent to a client preventing manual corrections.	For a haphazardly selected client instruction that was not executed, we noted that on the basis of a transaction processing refusal obtained from a Foreign Depository via SWIFT, a notification to a client was automatically generated and sent without modifiability.	No exceptions noted
2.10 SWIFT messages for transactions with foreign securities in local markets (with "Domestic" tag) are sent to Foreign	For haphazardly selected transactions with foreign securities conducted in local markets during the audited period, we inspected SWIFT messages sent to Foreign Depositories.	No exceptions noted



Controls Specified by NSD	Test Performed by KPMG	Result of Testing
Depositories only after a checking of correctness by two independent employees (“four-eye” control).	We noted that for all selected transactions, SWIFT messages were checked by a second employee.	
2.11 As part of the day-closure procedures an Operation Department employee reviews the procedures completed report and drops a mark of the performed review.	For haphazardly selected dates from the audited period, we inspected an operation day closing. We noted that all selected operation days were successfully closed.	No exceptions noted



Control Objective 3:

Controls provide reasonable assurance that payments made based on clients' instructions for the transfer of funds authorized, processed and recognized completely, accurately, and in a timely manner.

Controls Specified by NSD	Test Performed by KPMG	Result of Testing
Tax rates management		
3.1 Entering and changing of tax rates in the reference directory of Alameda system is possible only with verification by a second employee.	We inspected the entire population of tax rates entered / changed for the audited period and noted that they were entered and checked by two employees with subsequent verification by a head of the Tax Accounting and Reporting department.	No exceptions noted
3.2 When calculating tax payments, the tax rate is applied automatically based on electronic client disclosures using electronic tax rate reference directories. A tax agent report is generated automatically in the Alameda system.	For a haphazardly selected client disclosure, we noted that the tax rate from the tax disclosure matched with the data from the electronic tax rate reference directories. We also noted that the tax agent report contained a correct tax rate.	No exceptions noted
Income payments		
3.3 Alameda automatically creates a list of recipients of cash income payments based on the client's securities balance at holder-of-record date.	For a haphazardly selected corporate action for the payment of annual dividends, we inspected and noted that the list of holders and their balances in the DPO system corresponds to the data from the Alameda system at holder-of-record date. We also verified that the client securities balances in the Alameda system at holder-of-record date matched with securities balances in the corporate action for the income payment registered in the DPO system.	No exceptions noted
3.4 The distribution of income payments is proceed automatically in the DPO system only after checking of received funds completeness.	We re-performed the procedure of generating payment documents to depo clients in the DPO system.	No exceptions noted



Controls Specified by NSD	Test Performed by KPMG	Result of Testing
	We noted that in case when the amount of payments calculated in the DPO system did not match with the amount of the received funds, income payments processing is not possible.	
3.5 An authorized employee of the income payment department checks the correctness of automatically generated payment orders and sends them to the ASER system for execution with preventing manual corrections.	We examined the functionality of the DPO system and noted that employees do not have the ability to make changes in generated payment orders for the income payment.	No exceptions noted
Communication with Central Bank		
3.6 An authorized employee from the Operation Department reviews a register of documents that is sent to the Bank of Russia. In case of error absence, the authorized employee signs paper copies of the documents. If the Bank of Russia declines payment orders, the authorized employee investigates causes of rejection.	For haphazardly selected dates from the audited period, we inspected a checker's signature on paper versions of the documents for that day, as well as the Central Bank's answers. We noted that for all the selected dates there were signatures of makers and checkers on paper versions of the documents. We noted that when the client's order was rejected by the Central Bank, the client received a notification.	No exceptions noted
Payment transactions		
3.7 Before currency transactions processing, the Currency Control Department employees review payment documents and drop a mark in ASER system.	We inspected the entire population of payment documents that underwent the stage of currency control and noted that for all documents there were check marks made by an employee of the Currency Control Department.	No exceptions noted
3.8 On a daily basis, an authorized employee of the Operation Department of payment in a national currency processes files received from NCC (National Clearing Centre) in the ASER system. If files with errors are detected, the department	For haphazardly selected dates from the audited period, we received a status of requests from NCC. We noted that for selected dates all requests were in the status "Processed without errors".	No exceptions noted



Controls Specified by NSD	Test Performed by KPMG	Result of Testing
employees take the necessary actions to resolve them (interaction with NCC, etc.).		
3.9 The ASER functionality automatically makes changes on client's trading accounts only after relevant confirmation from a NCC.	For haphazardly selected instructions (to increase/ decrease cash positions), we observed and noted the transactions on trading accounts was performed automatically after receiving relevant confirmations from a NCC.	No exceptions noted
3.10 The ASER functionality permits processing settlement instructions only with sufficient cash balances on client's accounts and nostro account.	For a haphazardly selected instruction, we inspected that before the settlement instruction processing, the ASER system automatically checked the availability of a sufficient amount of funds on the client's accounts and blocked the necessary amount. We noted that only after blocking the necessary amount of funds, the settlement instruction was automatically transferred to the next stage of execution.	No exceptions noted
3.11 ASER users do not have an access to modify parameters of payment documents within ASER system.	We inspected ASER system functionality and noted that users did not have the ability to modify payment documents after accepting them for execution.	No exceptions noted
3.12 The correctness of manual entries in ASER system is checked by an independent employee of Operation Department (a checker) within reconciling original documents to data in ASER. In case of mismatches absence, the employee (a checker) signs the document.	For haphazardly selected payment orders received on paper during the audited period, we inspected and noted that all selected documents were entered into the system correctly and checked by an independent employee of the Operations Department.	No exceptions noted
3.13 An employee of the Operation Department (a checker) reviews the correctness of entered data in the ASER system for compliance with an exchange rate and date of valuation of currencies specified in a paper document. The posting of entries for conversion transactions in the ASER information system is performed automatically.	We noted that there were no conversion operations received in paper form during the audited period. For a haphazardly selected payment document, we inspected and noted that the entry were generated in the ASER system automatically and in accordance with the data in the electronic payment order.	No exceptions noted



Control Objective 4:

Controls provide reasonable assurance that clearing operations and transfer-agency services are provided correctly and in a timely manner.

Controls Specified by NSD	Test Performed by KPMG	Result of Testing
Transfer-agency services		
<p>4.1 Alameda functionality prevents an individual employee from entering the parameters of an issuer and confirming that the data entered is correct.</p>	<p>We re-performed the procedure of creating a new issuer in Alameda system and noted that:</p> <ul style="list-style-type: none"> – Data was not displayed in the system till double data entry control had been performed; – In case of discrepancies under double data entry control an error message was generated by the system indicating the fields with errors. 	<p>No exceptions noted</p>
<p>4.2 Data transmission through a secure communication channel is automatic. In case of errors, NSD informs the client with automatic notification.</p>	<p>We inspected the data transfer process during one day (18.06.19) and, using the example of one failure (“Refusal of transit”) for a haphazardly selected sender, we inspected automatic notifications.</p> <p>We noted that the system registered an error (a problem with the user's certificate) and automatically generated a notification to the user. Once the problem was resolved, an automatic notification about the successful message transit was generated and sent to the user.</p>	<p>No exceptions noted</p>
Automatic check of clearing transactions		
<p>4.3 Alameda functionality allows executing of matched clearing instructions only in case when counterparties accounts have sufficient balances of securities or funds (based on terms DVP - Delivery Versus Payment).</p>	<p>For a haphazardly selected client’s instruction, we inspected the clearing processing.</p> <p>We inspected that all stages of the instruction execution were completed automatically. We noted that the instruction was correctly automatically matched with a counter instruction. The client was notified in a timely manner; the notification indicated the main transaction information.</p>	<p>No exceptions noted</p>



Controls Specified by NSD	Test Performed by KPMG	Result of Testing
4.4 Alameda functionality automatically matches counter clearing instructions and transfers to the next stage (awaiting for the sufficient balance) only matched instructions.	For a haphazardly selected client's instruction, we inspected the clearing processing. We inspected that all stages of the instruction execution were completed automatically. We noted that the instruction was transferred to the status "Waiting for the execution of the main (counter) instruction due to insufficient balance of securities on the counterparty's account". At the same time, the client was automatically notified about the stop of the instruction processing. Once sufficient balance of securities has appeared on the counterparty's account, the instruction had been executed, and the clearing participants were notified accordingly.	No exceptions noted
4.5 A transaction that is not ready for processing due to an insufficient balance of securities or funds on accounts are automatically excluded from the clearing pool.	For a haphazardly selected client's instruction, we inspected the clearing processing. We inspected that all stages of the instruction execution were completed automatically. We noted that the instruction was transferred to the status "Waiting for the execution of the main (counter) instruction due to insufficient number of securities on the counterparty's account" and was excluded from clearing pool. At the same time, the client was automatically notified about the stop of the instruction processing. Once sufficient balance of securities had appeared on the counterparty's account, the instruction was returned to the clearing pool and executed, and the clearing participants have been notified accordingly.	No exceptions noted



Control Objective 5:

Controls provide reasonable assurance that the accounting of agreements and contracts concluded on the third market, in the register there are taken place timely, correctly and only based on instructions from clients.

Controls Specified by NSD	Test Performed by KPMG	Result of Testing
<p>5.1 Repository functionality automatically checks incoming instructions for registration of general agreements/ contracts. In case of errors absence, general agreements/ contracts are registered automatically.</p>	<p>We inspected Repository functionality and the registration of general agreements/ contracts process.</p> <p>For a haphazardly selected general agreement, we noted that the system automatically checked the incoming instruction, automatically registered it (assigned a number) and generated a notification to the client about successful registration.</p> <p>For a haphazardly selected contract, we noted that the verification, registration and a registration number assignment also was performed automatically.</p>	<p>No exceptions noted</p>
<p>5.2 The sequence and execution of scheduled procedures in a frame of Repository operation day closure process is monitored automatically on a daily basis. The correctness of executing procedures and operation day closure is additionally checked by an employee of the Repository Operation Department. In case of errors in the Repository operation day closure process, reasons are investigated, incidents are recorded and their resolution is monitored, if any.</p>	<p>For haphazardly selected dates from the audited period, we inspected the Repository operation day closure.</p> <p>We noted that for selected dates, the Repository operation days were successfully closed automatically.</p>	<p>No exceptions noted</p>
<p>5.3 Repository functionality automatically appoints a new client as a reporting agent.</p>	<p>We inspected Repository functionality and the process of reporting agent appointing.</p> <p>For a haphazardly selected client, we re-performed the procedure for registering a new client and noted that the system automatically appointed this client as a reporting agent for itself.</p>	<p>No exceptions noted</p>
<p>5.4 In case of submitting a questionnaire (an instruction) by a client in paper form, employees of the Repository Operation</p>	<p>For haphazardly selected questionnaires (instructions) submitted by clients in paper form during the audited period, we inspected and</p>	<p>No exceptions noted</p>



Controls Specified by NSD	Test Performed by KPMG	Result of Testing
<p>Department check the information entered into the Operator's Workstation (Repository web-cabinet) for compliance with the paper version of the questionnaire. In case of discrepancies absence, the questionnaire is signed and sent to register in the Repository system.</p>	<p>noted that they were entered into the Operator's workstation system (Repository web-cabinet) after correctness checking performed by the second user for compliance with the paper version.</p>	



Control Objective 6:

Controls provide reasonable assurance that the changes to existing systems, applications and programs, as well as the development and implementation of new systems, applications and programs, are carried out by authorized employees with the required approval, testing, implementation and documentation procedures.

Controls Specified by NSD	Test Performed by KPMG	Result of Testing
6.1 There are separate segments of information systems for the development, testing and production implementation.	We inspected the NSD's network topology and noted that there are separate segments of information systems for the development, testing and production implementation.	No exceptions noted
6.2 Prior to installation in a production environment, all changes are approved by the Change Committee. Changes to the SWIFT system are approved before testing phases.	For haphazardly selected changes into information systems (Alameda, DPO, ASER, CDB, Repository, CFT "Billing", e-voting) installed during the audited period, we noted that all of them were previously approved by the Change Committee.	No exceptions noted
6.3 Only those change requests that were included in the release to the Products and Projects Committee proceed with development and can be implemented.	For haphazardly selected changes into information systems installed during the audited period, we inspected change requests and noted that prior development and implementing all of them were approved and included in the release to the Products and Projects Committee.	No exceptions noted
6.4 Changes into information systems (except for the SWIFT system) are installed in production environments only after successful testing.	For haphazardly selected changes into information systems (except for SWIFT) installed during the audited period, we noted that all of them were previously successfully tested.	No exceptions noted
6.5 After a change of the SWIFT system has been approved by the Change Committee, the testing is performed on the pilot server and, if there are no errors, it is installed on the other servers of the production environment.	For entire population of changes into the SWIFT system installed during the audited period, we inspected requests and noted that they were approved by the Change Committee and successfully tested.	No exceptions noted



Control Objective 7:

Controls provide reasonable assurance that the issue of logical access rights to information systems and data is carried out only by authorized persons.

Controls Specified by NSD	Test Performed by KPMG	Result of Testing
7.1 Developers do not have access to install updates in the productive environments of information systems.	We inspected the list of administrative accounts in information systems and noted that developers do not have access to install updates to the productive environments of the NSD information systems.	No exceptions noted
7.2 Access to information systems is password protected, all password protection settings in the systems comply with the policies of NSD.	We inspected the NSD's internal policy governing password settings. We inspected password settings in information systems (Alameda, ASER, CDB, Repository, CFT, SWIFT, e-voting) at the application, database and operating system levels.	We noted that the password settings at the application level for the Alameda and ASER systems for NSD's users and privilege administrative access were less strict than NSD's policies requirements; however, such settings met "ГОСТ Р ИСО/МЭК 27002-2012" recommendations. We noted that the password settings at the database level for the Alameda, ASER, Repository, CFT systems for the privileged administrative access were less strict than NSD's policies requirements; however, such settings met "ГОСТ Р ИСО/МЭК 27002-2012" recommendations. Management response of National Settlement Depository:



Controls Specified by NSD	Test Performed by KPMG	Result of Testing
		<p>Alameda, ASER, Repository, CFT (DBMS level) - the accounts used by the OAAA employees to access database objects do not have high privileges, nevertheless, they will be transferred to the profile with password requirements for administrators.</p> <p>ALAMEDA, ASER (application level) – password settings are completed.</p>
<p>7.3 Access rights requests obtain all necessary approvals.</p>	<p>For haphazardly selected access rights to information systems (Alameda, ASER, CDB, Repository, CFT, SWIFT, e-voting) provided during the audited period, we inspected requests and noted that all of them obtained necessary approvals.</p>	<p>No exceptions noted</p>
<p>7.4 Administrative access to information systems at the application and database level is limited and granted to employees who perform the functions of administering information systems.</p>	<p>We inspected the lists of administrative accounts in information systems (Alameda, ASER, CDB, Repository, CFT, SWIFT, e-voting) at the application and database level and noted that administrative access rights were granted only to employees performing the functions of administering information systems.</p>	<p>No exceptions noted</p>
<p>7.5 Information system administrators block accounts of dismissed employees based on a request from the HR department.</p>	<p>For haphazardly selected employees dismissed during the audited period we inspected requests of blocking access and noted that for all selected employees the HR requests were formed.</p> <p>We inspected the full population of accounts in systems (Alameda, ASER, CDB, Repository, CFT, SWIFT, e-voting) at the application, database, operation system and network level</p>	<p>We noted that there were two administrative accounts of dismissed employees not blocked at the database level for the Alameda, ASER, CFT, Repository systems; however these accounts were blocked on the network level that mitigated a risk of unauthorized access of</p>



Controls Specified by NSD	Test Performed by KPMG	Result of Testing
	<p>for inspecting whether accounts of dismissed employees were blocked.</p>	<p>dismissed employees to databases.</p> <p>Management response of National Settlement Depository:</p> <p>Unblocked accounts of two dismissed employees relate only to individual DBMS accounts, they are currently locked. The identified accounts were created before the implementation of the automated process for managing access rights. Regular reconciliation of such accounts is in process.</p> <p>All other employee data accounts were blocked upon dismissal, which does not allow usage of DBMS accounts remotely or locally.</p> <p>All new accounts are created in accordance with the new process, therefore, they are deleted upon dismissal by the system request, or automatically.</p>
<p>7.6 Electronic keys are provided on the basis of a request signed by the employee for whom the key will be made, and a power of attorney signed by the Chairman of the Executive Board.</p>	<p>For haphazardly selected electronic keys provided during the audited period, we inspected requests and powers of attorney and noted that the keys were provided to employees on the basis of the duly signed request and the power of attorney.</p>	<p>No exceptions noted</p>



Control Objective 8:

Controls provide reasonable assurance that plans for the restoration of information systems and business activities are documented, approved, tested and maintained, if necessary, daily activities can be restored, critical data is stored on backup servers on a regular basis.

Controls Specified by NSD	Test Performed by KPMG	Result of Testing
<p>8.1 Information system administrators monitor performing of scheduled backups. In case of errors, administrators will investigate reasons of backup errors.</p>	<p>We interviewed administrators of information systems and noted that the process of monitoring of backups was developed and implemented.</p> <p>For haphazardly selected dates from the audited period, we inspected backup completions.</p> <p>We noted that for selected dates, the backups were completed in accordance with the schedule, and in case of errors, the reasons were investigated and eliminated in a timely manner.</p>	<p>No exceptions noted</p>
<p>8.2 The Company has Business Continuity Plans for ensuring continuity and restoration of activity based on which, on a regular basis, employees of the business continuity service perform testing of Disaster Recovery Plans and report results of testing and identified deficiencies.</p>	<p>We inspected the Business Continuity and Disaster Recovery Plans and noted that they were duly approved by the NSD's management and heads of relevant business units.</p> <p>We inspected testing protocols of Disaster Recovery Plans and relevant reports with the results of performed tests for the audited period.</p> <p>We noted that Business Continuity and Disaster Recovery plans were documented, approved and tested.</p>	<p>No exceptions noted</p>



Control Objective 9:

Controls provide reasonable assurance that the processing of operations in the field of information technology is authorized and carried out according to the schedule, and errors / failures are detected and resolved.

Controls Specified by NSD	Test Performed by KPMG	Result of Testing
9.1 Managers responsible for the service level agreement periodically issue summary reports of incident statistics and coordinate with the heads of the respective departments.	We inspected full population of reports of incident statistics issued during the audited period, and noted that reports were approved by heads of the relevant business units.	No exceptions noted
9.2 In the Company there is monitoring of data transmission between systems. All failures and incidents are recorded and resolved.	We inspected the functionality of a system designed to monitor data transmission between systems. We noted that failures and incidents were recorded, and responsible business and IT department employees were informed.	No exceptions noted
9.3 On a daily basis, employees of the Information Products and Services Department check the availability and correctness of updated data in information products via automatic and manual tests. Based on test results, a relevant report is communicated to the management.	For haphazardly selected dates from the audited period, we inspected performed tests of the availability and correctness of the updated data in information products. We noted that for all selected dates, employees of the responsible Department performed tests of the availability and correctness of updated data in information products. Based on test results, reports were sent to management.	No exceptions noted
9.4 After the completion of planned updates and in case of any malfunction of the NSD's information site, responsible IT and Information Products and Services Department staff are notified by automatic notifications via e-mail.	We interviewed responsible incident management employees about matters of NSD's information site malfunctions and noted that the process of incident management was developed and implemented. We noted that in case of any incidents with the information site, the responsible employees of IT and Information Products and Services Department are informed by automatic notifications via e-mail.	No exceptions noted



Controls not directly designed for achieving of Control objectives specified in Section III “General information about National Settlement Depository” provided by Management and tests performed by the service auditor

The following tables set out additional control procedures identified by NSD’s management that are not directly connected to specified Control objectives and the tests which KPMG have undertaken and the results of those tests. In addition, exceptions to those control procedures identified by KPMG within the Independent Service Auditors’ Report are annotated alongside the appropriate control procedure.

Corporate actions management			
1	For variety of mandatory corporate actions (SPLF, MRGR, DVCA, SPLR, SOFF, CAPG, CAPD, DVSE) with foreign securities which have one storage location, an initial message registration, a corporate action forming and generation of an instruction to inform clients are done in the CDB system automatically upon receiving a message from upstream storage.	For a haphazardly selected corporate action (DVCA), we inspected and noted that the initial message registration, the corporate action forming and the generation of instruction to inform clients occurred in the CDB system automatically based on the message received from an upstream storage.	No exceptions noted
2	Notification about a corporate action (Russian and foreign securities) is sent to NSD clients by the Alameda system automatically through the NSD’s EDI channels based on a list of securities holders formed in the CDB system.	For a haphazardly selected corporate action (DVCA), we inspected and noted that in the Alameda system corporate action notifications were generated and sent to all holders of a relevant security.	No exceptions noted
3	Instructions for participation in a corporate action (Russian and foreign securities) are registered in the system automatically. Information about errors in instructions processing is communicated to responsible employees via the department’s corporate mailbox.	For a haphazardly selected corporate action, we inspected and noted that instructions for participation in the corporate action were registered in the system automatically.	No exceptions noted



E-voting			
4	The e-voting system does not allow NSD's employees making changes in an established shareholder meeting, as well as in a list of the meeting's participants.	For a haphazardly selected shareholder meeting, we inspected and noted that the system does not allow NSD's employees making changes to the established meeting, as well as in the list of the meeting's participants.	No exceptions noted
5	NSD employees monitor the main statuses of a shareholder meeting (voting opened/ registration opened/ voting completed/ meeting ended) via automatic system notifications. In case of any malfunctions of the system, the reasons are investigated and resolved.	For a haphazardly selected shareholder meeting, we inspected that automatic notifications were sent by the system to NSD's employees. We noted that the NSD's employees were informed about the main statuses of the shareholder meeting.	No exceptions noted
Securities maintenance			
6	NSD, as a National Numbering Agency, assigns ISIN codes for financial instruments automatically in the CDB system without modifiability.	<p>We re-performed the process of assigning the ISIN code in the CDB system for one financial instrument.</p> <p>We inspected that after entering information about a financial instrument in the CDB system the ISIN code was generated automatically without modifiability.</p> <p>We also noted that at the same day information about the ISIN code assignment for this financial instrument was published on the website of NSD.</p>	No exceptions noted
Billing			
7	On a monthly basis, the responsible employee starts the automatic procedure for calculating service fees and generating payment documents (service payment invoice, protocol of provision of services, statement of settlement services) in the CFT-Bank system (the module "Billing"). Any changes (if necessary) in calculated services (making adjustments, service	We inspected the entire population of adjustments and service cancellations made into the CFT-Bank system (the module "Billing") for the audited period and noted that they were entered into the system under the control of a second user (a checker).	We noted that a log of the "maker/checker" control has been maintained since June 01, 2019. It is not possible to test the operational



cancellation) require confirmation by the second user (a checker).

effectiveness of the control over the entire audited period due to lack of the audit trail.

8	For calculating fees for agent services and providing technical access to SWIFT services, as well as for generating payment documents (service payment invoice, protocol of provision of services, statement of settlement services) in the CFT-Bank system (the module "Billing") information is entered manually into the system under the double data entry control.	We inspected the entire population of manually entered documents about the provided agent services and providing technical access to SWIFT services. We noted that all documents were entered into the system under the double data entry control by two users.	No exceptions noted
---	---	--	---------------------
