

**SBERBANK OF RUSSIA**

---

APPROVED  
by the Supervisory Board  
of Sberbank  
Minutes No. 19 dated July 03, 2020

**Sberbank's Policy  
on Organization of Internal Control**

**MOSCOW, 2020**

## IRD Details

<b>IRD Name</b>	Sberbank's Policy on Organization of Internal Control
-----------------	---

**Table of Contents**

1. General Provisions .....4

2. Goals and Objectives of Internal Control .....4

3. Internal Control Organization Principles.....5

4. Internal Control System.....6

5. Final Provisions ..... 13

Appendix 1 ..... 15

Appendix 2 ..... 16

Appendix 3 ..... 17

## **1. General Provisions**

1.1. Sberbank's Policy on Organization of Internal Control (hereinafter, the Policy) establishes the goals, principles and approaches in accordance to which Sberbank (hereinafter, the Bank) builds its internal control system.

1.2. This Policy has been developed in accordance with the requirements of Federal Law No. 86-FZ dated 10.07.2002 On the Central Bank of the Russian Federation (the Bank of Russia) /1/, Federal Law No. 395-1 dated 02.12.1990 On Banks and Banking Activity /2/, Federal Law No. 208-FZ dated 26.12.1995 On Joint-Stock Companies /3/, Regulation of the Bank of Russia No. 242-P dated 16.12.2003 On Organization of Internal Control at Credit Institutions and Banking Groups /4/, Order of the Federal Tax Service of Russia No. MMV-7-15/509@ dated 16.06.2017 On Approval of Requirements for Organization of an Internal Control System /5/, other government regulations, the Bank's Charter /6/, resolutions of the Bank's Supervisory Board, Executive Bodies and Collegial Working Bodies, as well as the Bank's internal regulatory documents.

1.3. This Policy takes into account the requirements of supervisory and regulatory bodies to the extent of organization of internal controls at credit institutions as well as the principles of evaluation of banks' internal control systems established by the Basel Committee on Banking Supervision /7/.

1.4. This Policy is the main document that defines the internal control system and serves as a basis for organization of internal control at the Bank as well as for the development of the Bank's internal organizational and procedural regulatory documents.

1.5. This Policy is subject to updating to take account of any changes in the legislation of the Russian Federation or any other applicable legislation (hereinafter, the Applicable Legislation) and the emergence of new standards or tools in the area of internal control.

## **2. Goals and Objectives of Internal Control**

2.1. The Bank exercises internal control in order to:

- ensure orderly, effective and efficient conduct of financial and business activities while performing banking transactions and other deals (including the achievement of financial and operating performance indicators), efficient management of assets and liabilities, including the safeguarding of assets, and risk management
- ensure the correctness of calculation (withholding) and the completeness and timeliness of payment (transfer) of taxes, duties and insurance premiums
- ensure the accuracy, completeness, objectivity and timeliness of reporting of financial and business activity results, compilation and filing of financial, accounting, tax, statistic and other statements (for external and internal users), as well as data security (the security of the Bank's interests (objectives) in the information area)
- ensure compliance by all of the Bank's employees in the course of their professional activities with the requirements of any applicable laws, codes, standards, business ethic norms, the Bank's Charter or any other documents, including in the course of execution or planning of a deal (transaction) or a series of interconnected deals (transactions), as well as in any other instances of the Bank's business activity
- prevent any involvement of the Bank or its employees in any illegitimate activities, including legalization (laundering) of proceeds of crime and financing of terrorism, and timely submission of information to competent government bodies and to the Bank of Russia.

2.2. Based on the above goals, the main objectives of the Bank's internal control are as follows:

- compliance by the Bank with the requirements of the applicable legislation and regulations
- establishment of procedures and powers in internal regulations and compliance with them in the course of making decisions and executing processes, as well as monitoring the results thereof
- making timely decisions aimed at remedying any discovered flaws or violations in the Bank's

activities

- safeguarding the Bank’s assets (property)
- efficient interaction with external auditors and government control, regulatory and supervisory bodies.

The internal control goals established by this Policy are achieved through simultaneous operation of five interconnected components:

- control environment
- risk management system<sup>1</sup>
- control procedures
- information and communications, and
- monitoring and performance assessment of controls.

These internal control components are an integral part of the Bank’s corporate governance system. The efficiency of internal tax controls is achieved through integration of the above components with the Bank’s goals and organizational structure. Each component is disclosed in specific internal documents of the Bank.

### **3. Internal Control Organization Principles**

The Bank’s internal control is organized and operates based on the following principles:

#### **3.1. Top view. Management and control culture. Leadership engagement.**

The Bank’s management (Supervisory Board and Executive Bodies) is responsible for creating and operating an adequate and effective internal control system, including control of compliance with the ethics norms and standards of professional activities as part of the Bank’s corporate culture, creates an atmosphere of open communication, gives an example of impeccable behavior, and encourages integrity and loyalty among the Bank’s employees, commitment to the ethics principles, and professional and diligent attitude towards participation in the internal control system.

#### **3.2. Responsibility. Participation of each Bank employee in internal control**

All of the Bank’s business units and employees without exception participate in the internal control process to the extent of their functions.

All employees and managers at all levels are responsible for exercising internal control as part of their powers.

Employees’ personal responsibility for exercising control functions is established in each specific case and stipulated in employees’ job descriptions.

A substantial element of the internal control system consists in the recognition by all employees of the need to perform their duties efficiently and to inform management at an appropriate level of any operating issues, instances of non-compliance with the code of professional ethics, or any other violations of rules or abuse.

#### **3.3. Allocation of powers upon execution of deals and transactions**

Establishment of a control system that provides for allocation of powers upon execution of deals and transactions, setting of limits, establishment of a system of approvals for deals and transactions, and control by the Supervisory Board, the Bank’s Executive Bodies and heads of business units. The control system implies a clear division of duties among employees and exclusion of any situations where an employees’ area of activity would involve a conflict of interest.

#### **3.4. Risk recognition and measurement**

The Bank’s internal control system is aimed at detecting material risks that may affect the achievement of the Bank’s strategic goals, assessing and monitoring detected risks on an ongoing basis using specially developed tools, and preventing and mitigating any such risks.

---

<sup>1</sup> The risk management system is not subject to regulation by this Policy; it is established by other internal documents of the Bank

### **3.5. Comprehensive nature**

Internal control is exercised across all of the Bank's business areas and processes. The internal control procedures are governed by the Bank's internal documents.

### **3.6. Consistent methodology**

The internal control processes and procedures are carried out based on uniform requirements and approaches that apply across the Bank's business units and employees.

### **3.7. Optimal volume**

The volume of control procedures in effect at the Bank is necessary and sufficient for exercising internal control effectively and achieving the Bank's goals. Resources and expenditures spent on implementation and subsequent operation of control procedures do not exceed the consequences of realization of risks, while the aggregate level of any residual risk matches the Bank's risk appetite.

### **3.8. Continuity**

The Bank's internal control is exercised on an ongoing basis at all levels of management, enabling the Bank to timely detect any deviations in the internal control system and prevent their emergence in the future.

### **3.9. Independent assessment**

The overall efficiency of the Bank's internal control is subject to independent assessment on an ongoing basis.

## **4. Internal Control System**

The Bank's internal control system is an aggregate of internal control bodies and areas and is consistent with the specifics of the Bank's financial and business operations. The internal control system is a multi-level hierarchical system built at the Bank at different management levels taking into account the role of each level in the process of organizing and ensuring the functioning of this system.

The Bank's internal control is organized on the basis of a risk-oriented approach, which in practical terms is a mechanism limiting the Bank's risk appetite.

In accordance with the requirements of Articles 10 and 24, /2/ the Bank's Charter stipulates the Internal Control Bodies, including the procedure for their establishment and their powers. The Bank has distributed powers among the members of its Supervisory Board and Executive Board, defined the powers of the CEO, Chairman of the Executive Board, and set forth powers, accountability and responsibility for the Bank's employees. The Bank's organizational structure is consistent with the nature and scale of transactions performed and the level and combination of risks assumed by the Bank.

### **4.1. Internal control system participants**

Internal control at the Bank is exercised by:

- the Supervisory Board
- the Bank's Executive Bodies
- the Bank's Chief Accountant (and his/her deputies)
- accountants (and their deputies) at the Bank's branches
- the Internal Audit Service
- the Internal Control Service
- the Controller for Countering the Legalization (Laundering) of Proceeds of Crime and Financing of Terrorism
- the Controller of a Professional Securities Market Participant
- the Authorized Officer for Countering the Illegitimate Use of Insider Information
- the Authorized Officer for Countering the Illegitimate Market Manipulation
- Other management bodies, business units and employees of the Bank exercising internal control to the extent of their powers as defined by the Bank's Charter and internal documents.

#### 4.1.1. Supervisory Board

The Supervisory Board is responsible for setting forth the principles and approaches for organization of the internal control system at the Bank, and performs assessment and control of the reliability and efficiency of the internal control system.

Acting within its powers/ 6/, /8/, /9/, the Supervisory Board, among other things:

- determines the principles for and approaches to internal control organization
- considers the matters of internal control efficiency and measures aimed at its improvement
- timely reviews internal controls for conformity with the nature and scale of operations performed and the level and combination of risks assumed.

The Supervisory Board Audit Committee preliminarily considers and prepares recommendations in the area of internal control for the Supervisory Board and, according to its purview/10/, it, among other things:

- makes sure that internal control systems and processes encompass processes such as the procedure for compilation and filing of accounting (financial) and internal reporting statements, monitoring of compliance with the requirements of the applicable legislation and the Bank's internal documents, the efficiency of transactions and other deals, and safeguarding of assets
- monitors and analyzes the efficiency of the Internal Audit Service
- prepares recommendations on selection of the Bank's auditors.

The Supervisory Board Risk Management Committee prepares and submits recommendations in the area of the Bank's risk and capital adequacy management for the Supervisory Board and, according to its purview/10/, it, among other things:

- oversees the development of and preliminarily reviews matters pertaining to the Bank Group's risk and capital management
- reviews reporting statements, including as part of internal capital adequacy assessment procedures
- oversees compliance with the legislation of the Russian Federation in the area of risk management.

#### 4.1.2. The Bank's Executive Bodies (Executive Board and CEO, Chairman of the Executive Board)

The Executive Bodies ensure that an effective internal control and risk management system is created and maintained at the Bank on an ongoing basis, and that resolutions made by the Supervisory Board in the area of internal control organization are carried out /6/, /9/, /11/.

The Bank's Executive Board, according to its purview, among other things:

- implements the Bank's strategy and policy in the area of organizing and exercising internal control, reviews the state of accounting, reporting, materials and findings of regular assessments of the internal control efficiency at the Bank, and establishes a system of control over remedy of any discovered violations or flaws in the internal control and over measures undertaken to remedy them.
- oversees compliance with federal laws and other laws and regulations by the Bank's business units, reviews compliance of the Bank's activities with its internal documents, including those that determine the internal control procedure, and assesses whether their content fits the nature and scale of the Bank's operations.

The CEO, Chairman of the Executive Board, among other things:

- reviews reports, opinions, representations or any other documents prepared by the Bank's Internal Control Bodies and, if needed, makes decisions on implementation of urgent measures aimed at remedying any violations discovered by them and at implementing recommendations.

#### 4.1.3. Chief Accountant

The Bank's Chief Accountant is responsible for the development of the Bank's Accounting

Policy, record keeping, and timely filing full and accurate accounting (financial) statements.

All employees of the Bank's business units involved in accounting to the extent of performing accounting operations and record-keeping report to the Bank's Chief Accountant.

The Chief Accountant's requirements for documentary recording of operations and provision of the necessary documents and information to the Bank's business units responsible for accounting apply to all of the Bank's employees.

#### 4.1.4. Internal Audit Service

The Internal Audit Service (hereinafter also the IAS) is an aggregate of the Bank's structural business units (the Internal Audit Division at the Central Head Office and RB Internal Audit Divisions) that act in accordance with /6/, /12/.

The Internal Audit Service reports to the Bank's Supervisory Board and acts under its direct supervision, and submits to the Supervisory Board, among other things, information on any discovered flaws in the operation of the internal control and risk management systems, as well as on measures taken to remedy them.

The Head of the Internal Audit Service reports to the Bank's Supervisory Board.

The Internal Audit Service carries out its activities independently of other structural units of the Bank.

Approaches to organization of internal audit, including the goal, objectives, functions and powers of the IAS are stipulated in the Regulation on the Internal Audit Service approved by the Bank's Supervisory Board /12/.

#### 4.1.5. Internal Control Service

The Internal Control Service (hereinafter also the ICS) is a group of employees at the Bank's Compliance Division that are not part of a stand-alone business unit and whose job descriptions include the performance of ICS functions stipulated in the Regulation on the Internal Control Service /13/.

Employees of various structural units of the Bank whose job descriptions provide for tasks and functions related to internal control and regulatory risk management may perform the functions of the Internal Control Service. The division of duties between those structural units is established by the Bank's internal risk management regulations, the Regulation on the Internal Control Service /13/, and regulations on structural units, and it must exclude a conflict of interest and any conditions leading to it when internal control functions are combined with execution of bank transactions or other deals.

The Internal Control Service reports to the CEO, Chairman of the Executive Board of the Bank. Reports on ICS activities may be considered by the Bank's Supervisory Board and Executive Board in accordance with the purview of those management bodies of the Bank.

The main goal of the Internal Control Service's activity is to assist the Bank's Supervisory Board and Executive Bodies in making sure that the Bank's activities comply with the applicable legislation, the standards of self-regulating organizations, and the best practices, as well as to create and apply effective methods and mechanisms for regulatory risk management.

The main objective of the Internal Control Service is to provide the Bank's Supervisory Board and Executive Bodies with information on the level of regulatory risk at the Bank, assessment of the regulatory risk management system, and the Bank's areas of operation that are most vulnerable to regulatory risk.

The Internal Control Service's functions in accordance with the objectives set for it to the extent of managing the Bank's regulatory risk are stipulated in the Regulation on the Internal Control Service approved by the Bank's CEO, Chairman of the Executive Board /13/.

#### 4.1.6. Controller for Countering the Legalization (Laundering) of Proceeds of Crime and Financing of Terrorism

The Controller for Countering the Legalization (Laundering) of Proceeds of Crime and

Financing of Terrorism is a special officer responsible for internal control in order to counter the legalization (laundering) of proceeds of crime and financing of terrorism (hereinafter, the CLPOC/FT Controller) /6/, /14/.

The CLPOC/FT Controller is appointed by an order by the Bank's CEO, Chairman of the Executive Board.

The CLPOC/FT Controller acts independently of the Bank's customer service business units and reports to the Bank's CEO, Chairman of the Executive Board.

The CLPOC/FT Controller is responsible for implementation of the Rules of Internal Control for Countering the Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction (hereinafter, the CLPOC/FT Rules) /14/. The functions of the CLPOC/FT Controller are defined in the CLPOC/FT Rules.

#### 4.1.7. Controller of a Professional Securities Market Participant

The Controller of a Professional Securities Market Participant is an officer in charge of overseeing the Bank's activities as a professional securities market participant.

The duties of the Controller of a Professional Securities Market Participant (hereinafter, the Bank's Controller) are assigned to a full-time employee of the Bank's Compliance Division by an order by the Bank's CEO, Chairman of the Executive Board.

The Bank's Controller conducts his/her activities independently of other structural units of the Bank. The Bank's Supervisory Board oversees the activities of the Bank's Controller.

The activities of the Bank's Controller are governed by an instruction /15/ that stipulates the general procedure for organization and exercise of control over compliance of the Bank's activities with the requirements of the legislation of the Russian Federation on the securities market, including the Bank of Russia's regulations, and the legislation of the Russian Federation on the protection of rights and legitimate interests of investors on the securities market and on advertising, as well as over compliance with the Bank's internal rules and procedures related to activities on the securities market.

#### 4.1.8. Authorized Officer for Countering the Illegitimate Use of Insider Information and Authorized Officer for Countering the Illegitimate Market Manipulation

The Authorized Officer for Countering the Illegitimate Use of Insider Information and the Authorized Officer for Countering the Illegitimate Market Manipulation are officers in charge of overseeing on an ongoing basis the compliance by Bank, its officers, employees and customers with the requirements, restrictions and prohibitions stipulated in Federal Law No. 224-FZ dated 27.07.2010 On Countering the Illegitimate Use of Insider Information and Market Manipulation and Introducing Amendments to Certain Legislative Acts of the Russian Federation and the Bank's internal regulatory and organizational-administrative documents to the extent of countering illegitimate use of insider information and market manipulation, including by conducting the necessary inspections.

The Authorized Officer for Countering the Illegitimate Use of Insider Information and the Authorized Officer for Countering the Illegitimate Market Manipulation are appointed and removed by an order by the Bank's CEO, Chairman of the Executive Board.

#### 4.1.9. Other business units and employees performing internal control functions in accordance with their structural unit regulations and job descriptions.

### 4.2. Internal Control Organization Areas

The Bank's internal control system encompasses the following areas:

- control by the Bank's Supervisory Board and Executive Bodies over organization of the Bank's activities
- control over operation of the risk management system and risk assessment

- control over division of powers upon execution of bank transactions or other deals
- control over information flow management (information receipt and transfer) and information security
- control over the conduct of business activities and the correctness of calculation (withholding) and the completeness and timeliness of payment (transfer) of taxes, duties and insurance premiums
- ongoing observation of the operation of the Internal Control System to assess the extent to which it meets the Bank’s operating objectives, detect any flaws, develop recommendations and exercise control over implementation of decisions on how to enhance the Internal Control System.

#### 4.2.1. Control by the Supervisory Board and the Executive Bodies over organization of the Bank’s activities

The Bank’s Supervisory Board and Executive Bodies exercise control over the Bank’s activities in accordance with /2/, /3/, /6/, this Policy, and the Bank’s other internal documents.

#### 4.2.2. Control over operation of the risk management system and risk assessment

The Risk Management System is governed by Sberbank’s Risk and Capital Management Strategy /16/, as well as by individual risk management policies.

The Risk Management System is aimed at ensuring sustainable development of the Bank as part of implementation of Sberbank’s Development Strategy.

The Bank creates a risk management system, inter alia, through implementation of internal capital adequacy assessment procedures.

The risk management system used by the Bank has been developed in accordance with the requirements of the legislation of the Russian Federation and the Bank of Russia’s regulations with account taken of recommendations of the Basel Committee on Banking Supervision and the EU, and meets the requirements of the world’s best practices.

The main objectives of the integrated risk management system as an integral part of the Bank management process include the introduction of risk management standards, principles, limits and restrictions, monitoring of the level of risk and generation of risk reporting, ensuring that the level of assumed risks conforms to established risk appetite limits, and modeling and formation of a general risk profile.

To ensure effective planning and control of assumed risks, the risk management functions are distributed among the Supervisory Board, the Executive Bodies, the Collegial Working Bodies reporting to the Bank’s Executive Board, the head of the Risks Block (Head of the Bank’s Risk Management Service), Risks Block units, and other business units of the Bank.

The division of powers within the risk management system meets the requirements and recommendations of the Bank of Russia and international financial institutions.

#### 4.2.3. Control over division of powers upon execution of bank transactions or other deals

The procedure for division of powers among the Bank’s business units and employees upon execution of bank transaction or other deals is established by internal documents of the Bank and includes such types of control as:

- inspections conducted by the Supervisory Board and the Executive Bodies by requesting performance reports and information from structural units and explanations from managers of corresponding business units for the purpose of detecting any control flaws, violations or errors
- control exercised by business unit heads by reviewing reports from their subordinate employees (on a daily and (or) weekly and (or) monthly basis)
- material (physical) control exercised by reviewing restrictions on access to material valuables, recounting of material valuables (cash, documentary securities, etc.), division of responsibility for safeguarding and using material valuables, and securing premises where material valuables are kept
- review of compliance with the established limits on bank transactions or other deals by receiving corresponding reports and reconciling data with primary documents

–a system for coordination (approval) of transactions (deals) and division of powers upon execution of bank transactions or other deals exceeding the established limits that provides for timely informing of corresponding managers of the Bank (the Bank’s units) about such transactions (deals) or the existing situation, and their proper reflection in accounting records and reporting

–review of compliance with the procedure for executing bank transactions or other deals, reconciliation of accounts, and informing corresponding managers of the Bank (the Bank’s units) about any detected violations, errors or flaws.

The allocation of rights and duties among business units and employees is reflected in regulations on structural units established as part of the bank’s organizational structure and in job descriptions of employees participating in execution of bank transactions or other deals.

Job duties are allocated among employees so as to exclude any conflict of interest or any circumstances leading to it, and to prevent crime or any other illegitimate activities.

It is not allowed to authorize one and the same business unit or employee to:

- execute bank transactions or other deals and record and (or) reflect them in accounting records
- authorize a disbursement of funds and perform (make) actual disbursements
- execute transactions on accounts held by the Bank’s customers and accounts reflecting the Bank’s proprietary financial and business operations
- provide advisory or information services to the Bank’s customers and execute transactions with the same customers
- evaluate the authenticity and completeness of documents provided upon a loan application and monitor the borrower’s financial situation
- perform actions in any other areas where a conflict of interest may arise.

The Bank establishes in its internal documents the procedure for detecting and exercising control over potential conflict of interest areas and for reviewing employees’ official duties to eliminate any possibility for them to conceal illegitimate activity.

#### 4.2.4. Control over information flow management (information receipt and transfer) and information security

##### 4.2.4.1. Efficiency of information dissemination methods and completeness of information communicated to employees tasked with execution

The sheer scale of the Bank’s transactions and its extensive branch network mean it is critically important to have an efficient information transmission system in place and guarantee that information is properly transmitted to each employee that needs to know it. All the while, this information must meet the quality criteria (reliability, timeliness, accessibility, and correctness of format).

A full understanding by employees of the Bank’s strategy and operating plans, as well as policies, internal regulatory documents, directives and instructions that define their work and duties, is achieved through the following, among other things:

- top-down dissemination of management information
- information transmission using various communication channels, including the corporate intranet portal
- training courses with a knowledge testing system.

##### 4.2.4.2. Internal control over automated information systems and technical means

Control over automated information systems and technical means is exercised for compliance with the provisions of Sberbank’s Cybersecurity Policy /17/ and other internal regulatory documents of the Bank that are subordinate to it, and encompasses all operating areas, including the rules for software acquisition, development and maintenance, as well as the procedure for physical and logical access security control.

Internal control over automated information systems and technical means consists of general control and software control.

#### 4.2.4.3. General control

General control over automated information systems involves computer systems control (control over the computing complex, the client-server system, end-user workstations, etc.) exercised for the purpose of ensuring uninterrupted and continuous operation.

General control consists of control over data backup (copying) procedures and automated information system function recovery procedures, providing support throughout the useful life of automated information systems, including the establishment of rules governing software acquisition, development and maintenance (support), and of a procedure for control over physical access security.

#### 4.2.4.4. Software control

Software control is exercised through automated procedures built into application programs as well as through manual procedures that control the processing of bank transactions or other deals (monitoring of automated systems and operations, logical access control, internal data backup and recovery procedures, etc.).

Software control is used for access control, authorization and automated system user audit. Software control also includes control exercised by specialized software means of control, such as security scanners, firewalls, intrusion detection systems, network traffic control systems, antivirus control systems, email control systems, web resources use control systems, etc.

#### 4.2.4.5. Business continuity

The Bank has developed and is continuously updating action plans aimed at ensuring the continuity and (or) recovery of the Bank's operations in the event of non-standard or emergency situations that provide for a set of measures for prevention or timely elimination of consequences of a potential disruption of the Bank's day-to-day operations, including the use of backup premises maintained at the ready for use in an emergency, backup (reserve) automated systems and (or) devices, and recovery of mission-critical systems supported by an external service vendor (provider).

A procedure for testing for the possibility of carrying out an action plan aimed at securing business continuity and (or) recovery in an emergency is determined /4/, /18/.

4.2.5. Control over the conduct of business activities and the correctness of calculation (withholding) and the completeness and timeliness of payment (transfer) of taxes, duties and insurance premiums

The procedure for exercising control over the conduct of business activities and the correctness of calculation (withholding) and the completeness and timeliness of payment (transfer) of taxes, duties and insurance premiums (internal tax control) is established by this Policy, /19/ and other internal regulatory documents of the Bank.

The main goal of internal tax control is to ensure reasonable confidence on the part of the Bank's management, government supervisory bodies, investors and other users that all results of the Bank's financial and business activities are accurately, completely and timely recorded in tax statements and that any tax obligations are fulfilled timely and completely.

The key areas for implementation of internal tax control procedures at the Bank include:

- ensuring the quality of data used in computation of taxes and preparation of tax and insurance premium returns (calculations) (including the need for the data, and completeness and correct classification of information included in tax statements)

- control of compliance with the requirements of the tax legislation at all stages of the Bank's operations, starting with the stage of drafting and executing contract documentation through the generation of tax statements and payment of taxes

- timely and complete identification of material tax risks subject to mitigation through the establishment of proper controls, and detection of any flaws, deviations or violations in ongoing processes.

Implementation of internal tax control procedures takes place based on a process-driven and systemic approach. Tax control procedures are integrated into all business processes and management and decision-making levels of the Bank, thereby ensuring end-to-end tax support of the Bank's operations, i.e. from preliminary tax review of supposed transaction terms through to defense of the

Bank's interests before the tax authorities and in court.

#### 4.2.6. Internal Control System monitoring and assessment

Internal Control System monitoring is performed on an ongoing basis. The Bank takes the necessary steps to enhance internal control taking into account the changing internal and external environment.

The Internal Control System is monitored, to the extent of their respective powers, by the Bank's Supervisory Board, Executive Bodies, managers and employees of stand-alone structural units, including units executing bank transactions or other deals and recording them in accounting and tax records and reporting statements, as well as by the Internal Audit Service.

The frequency of monitoring of various types of the Bank's activities is determined based on the frequency and nature of changes taking place and associated risks.

The results of Internal Control System monitoring are documented and communicated to the relevant executives of the Bank and the Bank's business units.

The Bank assesses the Internal Control System on an ongoing basis to determine the level of its organization and develop an action plan for its development and enhancement.

The procedure for and frequency of assessment of the Internal Control System are determined based on the nature and scale of the Bank's activities and the overall level of development and reliability of the Internal Control System. Assessment of the Internal Control System is conducted taking into account the results of control procedures that are actually performed and documented.

Assessment of the Internal Control System includes verification of the operation of the Internal Control System in the course of the Bank's financial and business activities in order to timely inform the executives of any detected errors, contradictions or flaws so that remedial steps could be taken.

The Internal Control System operates at all level of process controls, including the following:

- before the actual start of a process to prevent or minimize an adverse impact of events or factors that may affect the accomplishment of the organization's goals
- over the course of a process to timely identify and promptly remedy any violations or deviations from set parameters arising during operations
- after a process is completed to establish the accuracy of reported data and check whether the results meet the set targets (plans).

The Bank's Internal Control System is built using the Three Lines of Defense model, where:

–The first line represents business units that are responsible for efficiently carrying out day-to-day internal control activities and undertaking ongoing measures to manage risks associated with their activities. Those measures are part of day-to-day activities of business units, therefore they ensure a continuous process of identifying, assessing, and controlling risks.

–The second line represents the Bank's business units responsible for developing and implementing internal control rules and procedures, setting risk management standards, principles, limits and restrictions, monitoring risk levels, producing reports, checking whether risk levels match the Bank's risk appetite, advising, modeling and aggregating a general risk profile.

–The third line represents the internal audit that is responsible for independent assessment of the efficiency of internal control and risk management systems.

Line and area managers as well as process owners determine internal control procedures at each line level. As part of this work, they ensure the development and implementation of control procedures, assess the impact of any discovered flaws on the current and long-term performance on the areas of the Bank's Internal Control System that they are in charge of, ensure measures are undertaken to develop and enhance those areas, determine whether existing internal controls provide reasonable confidence in that process goals will be accomplished, and take steps to enhance the internal control.

## 5. Final Provisions

5.1. Amendments and additions to this Policy are approved by the Bank's Supervisory Board.

5.2. If any provision of this Policy conflicts with any statutory laws or regulations, such provision is considered null and void, and pending introduction of amendments into this Policy employees must follow the statutory norms.

### Terms and Definitions

**The Bank** – Sberbank of Russia (Sberbank).

**The Bank's Executive Bodies** – the collegial executive body – the Executive Board of the Bank, the sole executive body – the CEO, Chairman of the Executive Board of the Bank.

**The Bank's Collegial Working Bodies** – collegial working bodies the formation of which falls within the purview of the Executive Board under the Bank's Charter.

**Internal Control Bodies** – an aggregate of Management Bodies as well as of the Bank's business units and employees performing functions as part of the Internal Control System.

**Regulatory Risk** – a risk of losses to be incurred by the Bank due to non-compliance with any applicable legislation, internal documents of the Bank, standards of self-regulatory organizations (if such standards or rules are mandatory for the Bank), as well as due to application of sanctions and (or) any other measures of impact by the supervisory government authorities.

**Internal Control System** – an aggregate of internal control bodies and areas ensuring compliance with the procedures for achieving and accomplishing the goals set by the legislation of the Russian Federation and the Bank's Charter and internal documents.

**Risk Management System** – a set of measures aimed at ensuring sustainable development of the Bank as part of implementing Sberbank's Development Strategy, and that enables the following:

- identification and assessment of the Bank's risk materiality
- assessment of material/substantial risks for the Bank
- aggregation of quantitative assessments of material/substantial risks for the Bank for the purpose of determining an aggregate volume of risk assumed by the Bank, and
- control over the volume of material/substantial risks for the Bank.

**Corporate Governance System** – a system of interrelations between the Bank's shareholders, Executive Bodies, Supervisory Board and other stakeholders.

### Abbreviations

**CLPOC/FT Controller** – Sberbank’s Controller for Countering the Legalization (Laundering) of Proceeds of Crime and Financing of Terrorism

**CLPOC/FT Rules** – Sberbank’s Rules of Internal Control for Countering the Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction

**IAS** – Sberbank’s Internal Audit Service

**ICS** – Sberbank’s Internal Control Service

**RB** – a regional bank of Sberbank

**CHO** – Sberbank’s Central Head Office

### References

1. Federal Law No. 86-FZ dated 10.07.2002 On the Central Bank of the Russian Federation (the Bank of Russia)
2. Federal Law No. 395-1 dated 02.12.1990 On Banks and Banking Activity
3. Federal Law No. 208-FZ dated 26.12.1995 On Joint-Stock Companies
4. The Bank of Russia's Regulation No. 242-P dated 16.12.2003 On Organization of Internal Control at Credit Institutions and Banking Groups
5. Order of the Federal Tax Service of Russia No. MMV-7-15/509@ dated 16.06.2017 On Approval of Requirements for Organization of an Internal Control System
6. The Charter of Sberbank
7. The Bank of Russia's Letter No. 87-T dated 10.07.2001 On the BCBS's Recommendations for a Framework for Internal Control Systems in Banking Organizations
8. Regulation on the Supervisory Board of Sberbank No. 1280 (as amended)
9. Sberbank's Corporate Governance Code (approved by the Supervisory Board, Minutes No. 19 dated 20.04.2015)
10. Regulation on the Committees of the Supervisory Board of Sberbank No. 3851 (as amended)
11. Regulation on the Executive Board of Sberbank No. 1279 (as amended)
12. Regulation on the Internal Audit Service of Sberbank No. 3502 (as amended)
13. Regulation on the Internal Control Service of Sberbank No. 3497 (as amended)
14. Rules of Internal Control for Countering the Legalization (Laundering) of Proceeds of Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction No. 881 (as amended)
15. Instruction on Internal Control of Sberbank's Activities as a Professional Securities Market Participant No. 2778 dated 18.12.2015 (as amended)
16. Sberbank's Risk and Capital Management Strategy No. 4973 dated 16.04.2019
17. Sberbank's Cybersecurity Policy No. 4660 dated 26.10.2018
18. Regulation on Securing Sberbank Business Continuity and Recovery in Emergencies No. 4406 dated 02.12.2016
19. Regulation on Sberbank's System of Internal Control over the Conduct of Business Activities and the Correctness of Calculation (Withholding) and the Completeness and Timeliness of Payment (Transfer) of Taxes, Duties and Insurance Premiums No. 4987 (as amended)
20. Sberbank's Corporate Ethics Code (approved by the Supervisory Board, Minutes No. 52 dated 29.10.2015)
21. Sberbank's Policy on Countering the Illegitimate Use of Insider Information and Market Manipulation No. 4757 (as amended)
22. Tax Code of the Russian Federation (Part One) No. 146-FZ dated 31.07.1998.