**SBERBANK**
**OF RUSSIA**

APPROVED
by the Resolution of the Supervisory
Board of Sberbank
dated “7” December 2021 No. 35§2

**“7” December 2021** **No. 3960-5**

# SBERBANK GROUP RISK AND CAPITAL STRATEGY

(Version 5)

MOSCOW
2021

# IRD details

| | | | | |
|---|---|---|---|---|
| **IRD title** | Sberbank Group Risk and Capital Strategy | | | |
| **IRD developed by (unit)** | Integrated Risk Management Department | | | |
| **IRD prepared by, telephone number** | V. Narozhnaya, tel. 8 (495) 665 56 00, ext. 16-539 | | | |
| **IRD type / category** | Basic IRD / Documents approved by the supreme management body and regulating activities of the supreme management body | | | |
| **Customer journey number / process code** | -/П815, П812, П838, П810, П2395, П1652 (Р815, Р812, Р838, Р810, Р2395, Р1652) | | | |
| **IRD applies to the following units** | **X** | Central Head Office | **X** | Centrally subordinated units |
| | **X** | Regional banks | **X** | Internal structural units |
| | **X** | Bank branches | **X** | Sberbank Group |
| | **X** | Foreign branches | | |
| **IRD for upper-level process** | | | | |

***IRD history***

| **Revision No.** | **Details of the administrative document approving this IRD / amendments to this IRD, date, and position of the approving officer** |
|---|---|
| 1 | Resolution of the Supervisory Board of Sberbank, Minutes No.42 dated 15/09/2015 |
| 2 | Resolution of the Supervisory Board of Sberbank, Minutes No.17 dated 20 /04/2017 |
| 3 | Resolution of the Supervisory Board of Sberbank, Minutes No.10 dated 17/04/2018 |
| 4 | Resolution of the Supervisory Board of Sberbank, Minutes No.11 dated 16/04/2019 |
| 5 | Resolution of the Supervisory Board of Sberbank, Minutes No.35 dated 07/12/2021 |

***IRDs ceasing to be effective after this IRD comes into force***

Sberbank Group Risk and Capital Strategy No. 3960-4 dated 16/04/2019

Sberbank Risk and Capital Strategy No. 4973 dated 16/04/2019

| ***IRD effective date*** | ***IRD validity period*** |
|---|---|
| From the date of approval | |

**Information on crowdsourcing-driven expert review**

| | |
|---|---|
| | |

# Table of Contents

## 1. General Provisions

1.1. The Sberbank Group Risk and Capital Strategy (hereinafter the Strategy) specifies the basic principles used to form the risk and capital management system in Sberbank Group (hereinafter the Group).

1.2. The Strategy has been developed in compliance with the requirements of the Bank of Russia and the regulations of the Russian Federation /1-9/, with due regard to the guidelines of the Basel Committee on Banking Supervision (hereinafter BCBS) /10-13/ and the European Union /14, 15/.

1.3. The risk and capital management system is a part of the general corporate governance system of the Group and is aimed at ensuring sustainable development of Sberbank (hereinafter the Bank) and the Group members in the course of implementation of the Development Strategy of Sberbank (hereinafter the Development Strategy) approved by the Supervisory Board of the Bank.

1.4. The Bank shall create the risk and capital management system of the Group, in particular, through the implementation of internal capital adequacy assessment procedures (hereinafter referred to as the ICAAP).

1.5. The Group's ICAAP shall take into account risks of the Bank and the Group members[1], information on which is included in the calculation of capital adequacy ratios on a consolidated basis according to the requirements of /9/.

1.6. ICAAP implementation is driven by the need to:

- comply with the requirements of the Bank of Russia;
- satisfy the expectations of shareholders interested in long-term development of the Group with a view to ensure the returns on investments;
- ensure the efficient operation of the risk and capital management system enhancing the Group's reliability for all the stakeholders, namely, customers and creditors of the Group, its employees and regulatory bodies.

1.7. The provisions of this Strategy serve as the basis for organization of work aimed to manage the risks and capital adequacy in the Group, among others, for development of the regulatory documents of the Bank and the Group members on risk and capital management.

1.8. The Strategy also describes the risk management procedure, in particular, allocation of the risk and capital management functions among the Supervisory Board, the Executive Board, collegial working bodies of the Bank, business units of the Bank, and the Group members performing the risk management and risk taking functions, as well as methods used for risk assessment, containment and mitigation.

1.9. Deviations from the Strategy requirements shall be possible for the Group members being out of the jurisdiction of the Russian Federation as agreed upon with the Bank if these requirements are in conflict with local laws in countries of the Group members' operation.

1.10. The Strategy requirements shall be mandatory for the Bank being the parent credit institution of the banking group, and for the Group members for which substantial[2]/material risks are identified. Other Group members may also be guided by the Strategy provisions while building their risk management systems.

[1]The Bank if necessary may extend the perimeter of Group's ICAAP.

[2] The term 'substantial risk' corresponds to the term 'significant risk' in /4/.

1.11. When developing the Strategy, the Bank shall be guided by the approach ensuring the going concern in the longer term. The financial stability of the Group shall be ensured by timely identification of potential risks arising, in particular, while revising the Development Strategy, and by management of substantial/material risks.

## 2. Goals and objectives

**The goals of risk and capital management are:**

- to ensure/maintain the acceptable risk level within the risk appetite[3] and/or other limits and containments;
- to ensure capital adequacy to cover substantial/material risks;
- to ensure the financial stability of the Group and minimize possible financial losses caused by risks taken by the Group within the risk appetite established in accordance with the Development Strategy;
- to ensure the efficient resource allocation for optimization of the risk-return ratio of the Group;
- to ensure the going concern and plan the optimal management of the Group's business with due regard to possible stress conditions;
- to comply with requirements of government authorities of the Russian Federation regulating the activities of the Group as a whole and of specific members of the Group, as well as requirements of government authorities in countries of the Group members' operation.

**The objectives of the risk and capital management system are:**

- Risk identification and assessment of risk significance;
- to estimate and forecast the risk levels;
- to set risk limits and containments;
- to monitor and control the volume of the risk taken, implement measures aimed at mitigation of the level of the risk taken by the Group with a view to keep it within the set external and internal containments;
- to comply with the mandatory ratios and restrictions established by the Bank of Russia;
- to assess the adequacy of available financial resources (hereinafter AFR) for covering substantial/material risks for which the capital requirements are determined, including those in case of stress conditions;
- to plan the capital by reference to the results of the comprehensive risk assessment, testing of the Group's stability against internal and external risk factors, the Development Strategy targets, and capital adequacy requirements of the Bank of Russia;

[3]The term 'risk appetite' corresponds to the term 'risk tolerance' in /4/.

- to develop preventive and remedial actions aimed at maintenance of capital adequacy and prevention/reduction of the Group's losses in case of stress conditions;
- to carry out strategic planning with due regard to the level of accepted risk;
- to keep the Supervisory Board of the Bank, the Executive Board of the Bank, collegial working bodies of the Bank and business units of the Bank performing the risk management and risk taking functions, informed about substantial/material risks and capital adequacy;
- to ensure the uniform understanding of risks at the Group's level;
- to develop the risk culture and risk management competencies in the Group with due regard to the best international practices.

## 3. Classification of Risk and Capital Management Objects

Risk is defined as the Group's inherent possibility of events resulting in financial losses and/or negatively affecting the Group's reputation and/or liquidity position. The risk management means a complex of measures to identify, assess, and aggregate all substantial/material risks, monitor, constrain, and control the amount of taken risks, plan the risk level, implement the measures to mitigate the risk level in order to keep the amount of taken risks within the set external and internal limits in the course of implementation of the Development Strategy.

Under ICAAP, capital shall be assessed as adequate, if AFR (disposable capital) exceed the overall economic capital (i.e. required capital). It shall be established for each risk, whether the capital for its coverage shall be specified, and if the need for capital allocation is determined, it shall be specified whether the capital will be allocated on an individual or aggregate basis. The capital adequacy ratio shall be calculated as a ratio of available capital to the overall amount of accepted and potential risks.

With a view to control the capital adequacy (equity/ AFR), the Bank and the Group members shall establish the capital allocation procedures through a system of limits/containments for substantial/material risks and for business areas/units performing the risk taking functions, if applicable.

For risk and capital management purposes, there are six categories of the Group members, for whom the minimum ICAAP requirements vary in accordance with the principle of proportionality specified in Appendix 4. The organization of interaction in the Group for building the risk management system is given in Appendix 5.

## 4. General Principles of Risk and Capital Management

### 4.1. Risk awareness

Decisions to conduct any operations shall be made only after the analysis of risks arising as a result of such an operation. All operations shall be conducted in compliance with the internal regulatory and/or organizational-administrative documents. No new transactions exposed to substantial/material risks shall be allowed, in case internal regulations, organizational and administrative documents, or relevant resolutions of collegial bodies regulating the procedure for their performance are non-existent.

### 4.2. Risk-adjusted operations management

The Group shall assess the adequacy of disposable (available) capital by implementation of ICAAP.

While making decisions on business development (elaboration of the Development Strategy), the Group shall rely on the ICAAP results as a basis for evaluation of the capital amount needed to cover the accepted and potential risks.

The Group shall select top-priority areas of development and capital allocation using the analysis of risk-adjusted performance indicators for particular business units and lines of business.

### 4.3. Involvement of top management

The Supervisory Board, CEO, the Chairman of the Executive Board, the Executive Board, and other collegial bodies of the Bank, as well as supervisory boards/ boards of directors/ executive and collegial bodies of the Group members shall approve IRDs specifying the risk management approaches, set the limits and containments, review the information about the level of accepted risks and capital adequacy, as well as about violations of established risk management procedures, limits and containments on a regular basis, and adopt other resolutions with regard to risk and capital management.

### 4.4. Principle of proportionality

While building the risk and capital management system, the Bank and the Group members shall be guided by the principle of proportionality, which means that the requirements to implementation of the risk and capital management system in the Group member shall depend on the nature and scope of its operations as well as on the level and combination of risks[4].

### 4.5. Risk Containment

The Group applies a system of limits and containments allowing to ensure the acceptable risk level.

The Group's system of limits has a multi-level structure[5]:

- risk appetite (including that of the Group and the Bank) approved at the level of the Bank's Supervisory Board;
- risk appetite approved at the level of the Group member's Board of Directors, including risk limits cascaded from the Group level;
- risk appetite (including that of the Group, the Bank, the Group member) approved at the level of collegial working bodies, including limits for the Group members, structural units of the Bank and the Group members performing substantial/material risk taking functions, as well as for the extent of transactions conducted with one counterparty, group of counterparties connected by certain features, for the extent of transactions conducted with financial instruments, etc.
- other risk containments necessary to efficiently manage substantial/material risks.

[4]In accordance with Appendix 4.

[5] The structure of limits/containments for each particular risk shall be represented in IRDs of the Bank / the Group member, describing the management of such risk.

### 4.6. Segregation of functions

For the purposes of efficient risk management and taking into account the need to minimize the conflict of interest between risk taking, risk level limitation and control, as well as the audit of risk and capital management system, the organizational structure of the Bank and the Group members shall be formed with due regard to the necessity for allocation of functions and responsibility among business units of the Bank/ the Group members in accordance with the '3 lines of defense' principle. The functions indicated for each line of defense may be performed not by one structural unit, but by several business units of the Bank/ the Group member:

| **1st line of defense** | |
|---|---|
| **Goal** | Risk level management within the set containments |
| **Functions** | – Risk identification<br>– Identification and primary assessment of the risks arising from performing operations and concluding transactions, including when launching new products and/or entering into new markets<br>– Monitoring and forecasting the level of risks related to positions / portfolios managed on a consolidated basis, modelling the customer behavior, balance sheet items, financial results, pricing, products, including for the purposes of analysis, assessment and forecasting of risk levels, etc.[6]<br>– Development of the [7]risk management and assessment methodology<br>– Development of models required to perform the 1st line of defense functions.<br>– Ensuring that the accepted risk complies with the set limits and containments.<br>– Development and implementation of measures required to comply with the set limits<br>– Performing the functions related to risk taking while conducting operations and entering into transactions (active risk taking) or through consolidation of positions exposed to risk (passive risk taking as a result of risk transfer) within the set regulatory and internal containments on risk (risk appetite, other limits and mandatory ratios, other restrictions)<br>– Risk taking as a result of performing/failing to perform functions associated with the risks other than those related to execution of operations or conclusion of transactions, by participants of the risk and capital management system (Subclause 5.3) |

| **2nd line of defense** | |
|---|---|
| **Goal** | Independent risk assessment and control |
| **Functions** | – Risk identification and materiality assessment<br>– Provision of the expertise within own competences in identification of the risks arising when launching new products and/or entering into new markets[8] |

[6]For liquidity risk, interest rate risk and currency risk in the banking book.
[7] If the business unit responsible for the risk (see Subclause 5.3.14) is a unit performing the 1st line of defense functions.
[8] This process is under development for particular risks.

| | |
|---|---|
| | – Development[9] / approval of the risk management and assessment methodology<br>– Development of models required to perform the 2nd line of defense functions.<br>– Assessment of aggregated (overall) actual risk level<br>– Forecasting[10] and monitoring the risk level<br>– Development of a system for limitation of risk levels (including development of risk appetite limits and/or other risk limits structure and values and/or other qualitative restrictions proposed for approval)<br>– Assessment of risk level, control over the correspondence of actual and anticipated risk levels to the set risk containments (development of escalation procedures and control over implementation of measures to eliminate violations), irrespective of the 1st line<br>– Control of the compliance with regulatory ratios / indicators, if applicable<br>– Organization/implementation of stress testing procedures<br>– Development and approval of risk level mitigation measures in case of violation of the set limitations on actual data by the 1st line of defense<br>– Generation of reports[11] on risks and their communication to the management and collegial bodies<br>– Testing and validation of risk assessment models (this function shall be performed by a business unit independent of business units developing models and assessing risks with the use of such models)<br>– Development of risk culture |
| **3rd line of defense** | |
| **Goals** | Independent assessment of the risk and capital management system performance and its compliance with internal and external requirements |
| **Functions** | – Assessment of the efficiency of the risk and capital management system, including verification of the efficiency of the risk assessment methodology and risk management procedures established by IRDs of the Bank / the Group members, as well as whether the above mentioned documents are applied in full<br>– Notifying the management of deficiencies identified in the risk and capital management system<br>– Control over elimination of deficiencies identified in the risk and capital management system |

Specification of functions performed by the 1st and 2nd lines of defense shall be determined in IRDs[12] on management of substantial/material risks and may deviate from the above list, if there are any specific functions for such risk.

[9] If the business unit responsible for the risk (see Subclause 5.3.14) is a unit performing the 2nd line of defense functions.
[10] For liquidity risk, interest rate and currency risks in the banking book, the function shall be performed by a unit responsible for the risk (see Subclause 5.3.14) performing the 1st line of defense functions, which does not contain the possibility for forecasting conducted by a unit performing the 2nd line of defense functions.
[11] With the exception of the financial reporting, the responsibility for formation of which is assigned to Accounting and Reporting Department and Financial Reporting Center in Saint Petersburg, including for calculation of actual values of mandatory ratios set by the Bank of Russia.
[12] For substantial risks, shall be developed the risk management policy by a unit responsible for the risk.

The 4th line of defense shall be represented by the regulators, as well as external auditors who, despite being external organizations in relation to the Bank/ the Group member, nevertheless constitute an important mechanism not only for the risk and capital management system, but for the corporate governance of the Group as a whole as well.

### 4.7. Centralized and decentralized approaches

The Group shall apply the combination of centralized and decentralized approaches to risk and capital management in order to ensure the best practice efficiency. The Bank's authorized bodies shall manage risks and capital of the Bank and the Group as a whole, as well as set the requirements for organization of the risk and capital management system at the level of specific members of the Group (including pursuant to the structure of limits and restrictions, applied methodology and other aspects). The Group members shall manage risks and capital at the local level within the set limits and powers and develop IRDs in accordance with requirements set forth in the Group standards with due regard to local specifics.

Decentralization of functions shall enable the prompt response to changes of risk levels in the Group members.

### 4.8. Information technology and data quality

Risk and capital management shall be based on using the advanced information technology allowing to enhance the quality and promptness of decision-making.

For example, for credit risks, with a view to minimize the requirements to customers with regard to presentation of personal data in order to make decisions in real time, and also to increase the level of risk assessment, the Bank/ the Group members seek to automated aggregation of customer data. The Goal of the Bank / the Group members is to automate making of standard decisions and involvement of risk manager's expert knowledge only in non-standard complex transactions. In order to make decisions on transactions, the Bank/ the Group members may use the artificial intelligence (including that implemented with the use of approaches based on neural networks). The Bank/ the Group members shall work towards automation of credit risk management processes by using the advanced technology for digitalization of the tools and models.

Data quality, completeness and availability are critically important factors for ensuring the reliability and accuracy of risk calculation and assessment.

The Group shall work towards maximum automation of the processes of data collection, storage and processing.

Risk management takes into account risks associated with the implementation of advanced information technology and caused by disruptions in the work of automated systems and in the information protection of systems of the Bank and the Group members.

### 4.9. Perfection of methods

The risk and capital management methods shall be continuously updated: procedures, technology and information systems shall be improved with due regard to strategic tasks, changes in the external and internal environment, as well as innovations in the international practice.

### 4.10. Risk culture

Risk culture develops such values as transparency, trust, quick response, responsibility, and involvement.

With a view to ensure the stable and efficient functioning of the entire risk management system, the Group shall take actions aimed at the development of risk culture with the following main tasks:

- acquisition of knowledge and skills by employees of the Bank and the Group members in the field of risk management through regular training;
- correct use of risk management tools by executives and employees in their day-to-day activity;
- development of employees' skills of correct and timely using of risk management tools;
- open and active communications within the Group regarding the risk culture values and principles.

The Group applies the following risk culture rules:

- I see – I speak out;
- I hear – I correct;
- I make an error – I report.

Therefore, the risk culture develops the atmosphere of transparency, proper attitude to risks, and, generally, mature organization.

### 4.11. Risk-based incentive system

The Group's remuneration system shall be built with due regard to the nature and scope of operations conducted, operating results, level and combination of accepted risks.

The risk-adjusted incentive system is implemented in the Bank in accordance with requirements set forth by the Bank of Russia /22/.

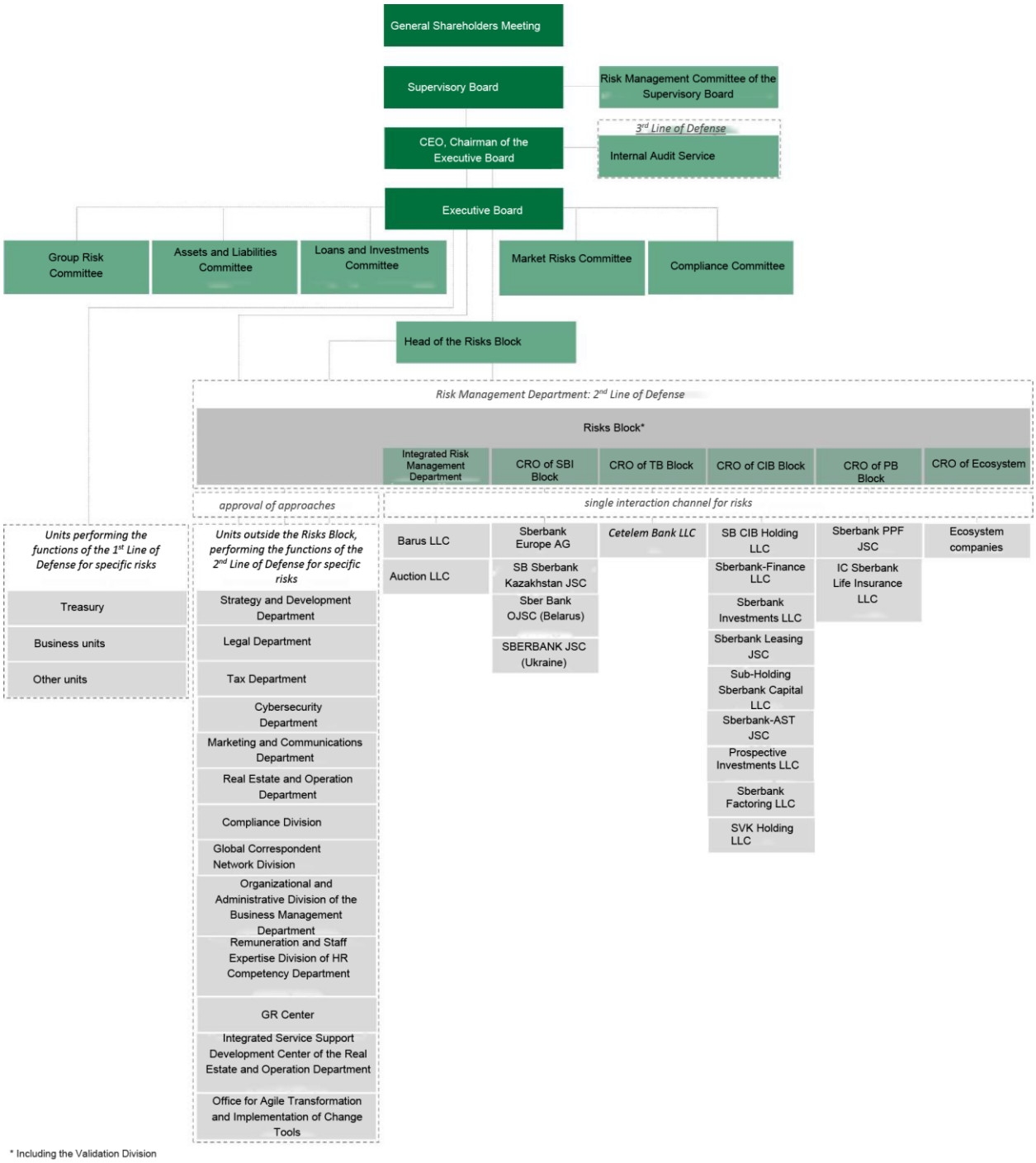
### 4.12. Information disclosure

All risk and capital adequacy management information needed according to the regulators' requirements shall be disclosed. Composition and periodicity of risk reporting shall comply with the requirements of the Bank of Russia /8/, the requirements to management accounts, and the requirements to disclosure of information on risks for any stakeholders in accordance with the principles of transparency, completeness, etc., as per Subclause 6.5.

# 5. Key Participants of the Risk and Capital Management System

## 5.1. Organization of Risk and Capital Management of the Group

The organization of risk and capital management of the Group is presented in Scheme[13].




[13] This scheme shows the Group members to be included in the ICAAP perimeter of the Group according to Subclause 1.3 /4/. Here are management companies of sub-holdings and controlled subsidiaries of the Bank outside sub-holdings. Sberbank Europe AG, Sberbank JSC (Belarus), Sberbank Capital LLC sub-holdings are included in the ICAAP perimeter of the Group in full. SB CIB Holding LLC sub-holding is included in the ICAAP perimeter of the Group in part, including Sberbank Switzerland AG, Sberbank CIB JSC, SBGB CYPRUS LIMITED, SB Finance Holding LLC. Sberbank Investments LLC, Sberbank Leasing JSC,Sberbank AST JSC are only included in the ICAAP perimeter of the Group at the level of the sub-holding's parent company.

## 5.2. Risk Management Department of the Bank

Risk management at the Group's level is performed by the Bank's Risk Management Department represented by the Risks Block of the Bank. The Risk Management Department of the Bank is functionally and administratively accountable to CEO, the Chairman of the Executive Board. The Head and employees of the Risk Management Department of the Bank are staff members of the Bank.

In its work, the Risk Management Department of the Bank shall be guided by the applicable laws of the Russian Federation, regulations of the Bank of Russia, the Bank's Charter, this Strategy, resolutions of the Bank's management bodies, and other IRDs or OADs of the Bank. In order to ensure the integrated risk management within the Group, the Risk Management Department shall take into account the requirements of local regulators in countries of the Group members' operation.

The Risk Management Department of the Bank shall perform its functions on a continuous basis. The Risk Management Department shall perform the functions of the 2nd line of defense. For some risks, certain functions of the 2nd line of defense may be performed by business units outside the Risks Block, which have necessary competence and resources and which are interested in mitigation of the level of the risk taken by the Bank with a view to compliance with the risk appetite limits and other containments. Negotiation of the policies and regulations for management of substantial/material risks with the Risks Block shall be mandatory. Business units outside the Risks Block shall not be a part of the Risk Management Department.

The Head of the Risk Management Department of the Bank shall be the Head of the Risks Block[14] accountable to CEO, the Chairman of the Executive Board of the Bank. The Head of the Risks Block shall control the work of the business units of the Risks Block and shall be a member of the Bank's committees for management of substantial/material risks[15].

The Head of the Risk Management Department of the Bank shall comply with the qualification and business reputation requirements set by the legislation and regulations of the Bank of Russia[16].

The function of risk management in the Group members has been organized and operates in accordance with the requirements of local regulators and the approaches to risk management organization established in the Group, and with due regard the organizational structure of the Group members.

[14] Or any designated substitute.

[15] Personal participation in the committees for management of substantial/material risks, or participation of a representative of the Risk Management Department.

[16]Qualifying requirements are set by the Bank of Russia Ordinance dated 25/12/2017 No. 4662-У (4664-U) "On the Qualification Requirements for the Head of Risk Management, Internal Controls and Internal Audit of a Credit Institution; for the Risk Management Officer and Controller of a Non-governmental Pension Fund, and the Auditor of an Insurance Company; on the Procedure for Informing the Bank of Russia about the Appointment to (Termination of) these Positions (Except for the Controller of a Non-governmental Pension Fund) and the Position of Special Officers Responsible for the Implementation of Internal Controls Rules Aimed at Countering the Legalization (Laundering) of Criminally Obtained Incomes and the Financing of Terrorism of Credit Institutions, Non-governmental Pension Funds, Insurance Companies, Management Companies of Investment Funds, Unit Investment Funds and Non-governmental Pension Funds, and Microfinance Companies; of an Internal Control Officer of a Management Company of Investment Funds, Unit Investment Funds and Non-governmental Pension Funds; and on the Procedure for the Bank of Russia to Assess the Compliance of These Persons (Except for the Controller of a Non-governmental Pension Fund) with Qualification and Business Reputation Requirements" The business reputation requirements are set by Clause 1 of Part 1 of Article 16 of the Federal Law dated 02/12/1990 No. 395-1 'On Banks and Banking'.

### 5.3. Division of functions and powers

Key functions of the risk and capital management system participants are described below[17]. In addition to these functions, the Bank's management bodies and collegial working bodies shall review the reports generated within ICAAP in accordance with Appendix 6, as well as approval of IRDs in accordance with Appendix 7.

CRO of the Group, CRO curator of the Group member, CRO of the ecosystem also serve as the risk and capital management system participants and perform the risk management functions, including, but not limited to responsibility for building the risk management system in the Group / the Bank / the Group members, organization of risk management within their areas of responsibility through interaction with the Bank's business units and the Group members, and control implementation of the risk management targets in the Group / the Bank / the Group members.

#### 5.3.1. The General Shareholders' Meeting of the Bank shall:

- adopt resolutions on increase/decrease of the charter capital, split-up/consolidation of shares, issue/conversion of bonds or other issue-grade securities convertible into ordinary shares, in cases provided for in /16/;
- make decision on dividend payment (declaration) in accordance with /16/;
- make decision on consent to conclusion or approval of major transactions / related party transactions, in cases and in the manner specified in /16/.

#### 5.3.2. The Supervisory Board of the Bank

- approve the Risk and Capital Management Strategy of the Group, including the procedure for management of material risks of the Group[18];
- approve the risk appetite at the Supervisory Board level and target risk levels of the Group;
- approve the planned capital adequacy level, planned capital level and planned capital structure of the Group;
- approve the Regulation on the Dividend Policy of the Bank;
- give recommendations for the amount of dividends on shares and for determination of the date on which the persons having the dividend rights are identified;
- adopt resolutions on changes in capital in accordance with the powers specified in /16/;
- approve the stress testing scenarios for the Group;
- approve the financial stability recovery plan of the Group (hereinafter the FSR plan);
- approve the key documents for the purposes of regulatory assessment of capital adequacy in accordance with /29/;
- approve the documents specifying approaches to accounting of risks in the remuneration system in accordance with /22/;

[17] The complete list of functions of the Supervisory Board, the Executive Board, and collegial working bodies of the Bank shall be established in the respective Regulations.

[18] The procedure for management of substantial risks is described in Appendix 8. In terms of liquidity risk, the Supervisory Board shall approve the Liquidity Risk Management Policy of the Group.

- control the implementation of the Risk and Capital Management Strategy of the Group, including the procedure for management of material risks of the Group[15];
- control the compliance with risk appetite approved at the Supervisory Board level and be informed about compliance with mandatory ratios[19] / indicators set by the Group / the Bank / the Group member;
- at least once a year, consider the need for making amendments in the documents developed under ICAAP, within its competence;
- control the efficiency of the risk and capital management system by reviewing, among others, the opinions of the Internal Audit Service (hereinafter INAS);
- make decision on consent to conclusion or approval of major transactions / related party transactions, in cases and in the manner specified in /16/.

### 5.3.3. The Risk Management Committee of the Supervisory Board shall:

- conduct preliminary review of all issues concerning risk and capital management of the Group within the competences of the Supervisory Board, including:
  - approval of the Risk and Capital Management Strategy, including the procedure for management of material risks of the Group[15];
  - approval of the risk appetite at the Supervisory Board level and target risk levels of the Group;
  - control of the compliance with risk appetite at the Supervisory Board level;
  - approval of the planned capital adequacy level, planned capital level and planned capital structure of the Group;
  - approval of stress testing scenarios for the Group;
  - approval of the FSR plan for the Group;
  - approval of key documents for the purposes of regular assessment of capital adequacy in accordance with /29/;
  - approval of documents specifying approaches to accounting of risks in the remuneration system in accordance with /22/;
- review of matters related to management of certain material /substantial risks, including social and environmental risk (ESG risk) and technology risk;
- control the compliance with Russian laws regarding risk and capital management;
- interact with other committees of the Supervisory Board on issues of risk management.

[19] With regard to the Group and the Bank, in terms of the Bank of Russia – mandatory ratios in accordance with Instruction of the Bank of Russia dated 29/11/2019 No. 199-*И* (199-I) "On Mandatory Ratios and Premiums to Capital Adequacy Ratios of the Banks with a General License".

### 5.3.4. Bank Executive Board

- adopt resolutions on establishment and termination of collegial working bodies of the Bank, approve the regulations on them, and stipulate their functions;
- approve the Group's business plan and monitor its implementation;
- approve the Group's IRDs regulating risk and capital management[20];
- at least once a year, consider the need for making amendments in the documents developed under ICAAP, within its competence.

### 5.3.5. The Group Risk Committee of the Bank shall:

- manage the overall risk of the Group within the powers, requirements and restrictions approved by resolutions of the Supervisory Board and the Executive Board of the Bank;
- approve the report on identification and materiality assessment of the Group's risks:
    - approve the list of risks considered material/substantial for the Group/ the Group members;
    - determine the Bank's collegial bodies responsible for management of particular risks, and the business units responsible for formation of the system of management of particular risks at the Group's level (hereinafter the business units responsible for risks);
    - adopt resolutions on incorporation of the Group members into sub-holdings and establish a management company for each sub-holding in order to organize integrated risk management;
- conduct preliminary review and approval of the Risk and Capital Strategy, including the procedure for management of material risks of the Group, for subsequent approval by the Supervisory Board;
- conduct preliminary review and approval of risk appetite to be approved at the level of the Bank's Supervisory Board and target risk levels of the Group;
- approve, within its powers, cascading of the risk appetite to be approved at the level of the Bank's Supervisory Board;
- adopt resolutions on inclusion / updating of risk appetite indicators of the Group members and on values of the set risk appetite limits of the Group members, with regard to risks, for which it serves as a responsible collegial working body;
- control, within its powers, the compliance with risk appetite limits and with regulatory ratios / indicators and requirements in the Bank and the Group members being subsidiary banks;
- approve and control risk appetite at the level of the Bank's collegial working bodies with regard to risks managed by the Committee;
- approve and control limits and other containments for risks managed by the Committee;
- adopt resolutions, within its powers, aimed at compliance with the established containments and eliminating violations of risk appetite and other risk limits;

[20] In accordance with Appendix 7.

- control, within its powers, implementation of measures aimed at eliminating violations of risk appetite and other risk limits;
- conduct preliminary review and approval of the Group's FSR plan;
- determine the need for and initiate unscheduled updating of the Group's FSR plan with due regard to stress testing scenarios and results;
- perform other functions on organizing and improving the integrated risk management system of the Group.

In addition, the Bank's Group Risk Committee (hereinafter GRC) shall perform functions of the risk management committee according to Subclause 5.3.7 with regard to substantial/material risks reserved for GRC.

### 5.3.6. The Assets and Liabilities Management Committee of the Bank shall

- approve the Group's standards for capital adequacy management processes and approaches, and requirements to the regulatory documents of the Group members, describing internal capital adequacy management methods and procedures;
- conduct preliminary review and approval of risk appetite of the Group to be approved at the level of the Bank's Supervisory Board for risks managed by the Committee;
- establish the architecture (system) and values for limits that constrain the capital adequacy level for the Group and the Bank with due regard to risk appetite containments approved at the level of the Bank's Supervisory Board;
- establish limits with regard to capital adequacy and with regard to risks managed by the Committee, for the Group members for further approval by their collegial bodies (except the limits to be established by GRC);
- establish the alert limits on mandatory capital adequacy ratios of the Bank and the Group, as established by the Bank of Russia;
- organize the compliance with mandatory and other adequacy ratios for the Group as a whole and for the Bank, and adopt resolutions on management of mandatory and other adequacy ratios of the Group and the Bank as established by the Bank of Russia;
- adopt resolutions aimed at eliminating violations of risk appetite limits of the Group and the Bank in terms of capital adequacy;
- conduct preliminary review of activity plans aimed at liquidity and capital adequacy management in the Group in crisis conditions for further approval by the Bank's Supervisory Board.

In addition, the Bank's Assets and Liabilities Committee (hereinafter ALC) shall perform functions of the risk management committee according to Subclause 5.3.7 with regard to substantial/material risks reserved for ALC.

### 5.3.7. Bank's Committee for Management of Substantial/Material Risks[21]

The Bank's Committee for Management of Substantial/Material Risks shall adopt the complete range of resolutions necessary to comply with the requirements established by the Bank's management bodies and the requirements of regulators, and shall perform the following functions in relation to the relevant risks:

- manage the substantial/material risks of the Group within the powers, requirements and containments approved by the Executive Board of the Bank;
- conduct preliminary review and approval of risk appetite of the Group to be approved at the level of the Bank's Supervisory Board for risks managed by the Committee;
- approve the architecture (system) and limit values[22] within the established risk appetite of the Group approved at the level of the Bank's Supervisory Board as proposed by a business unit of the 2nd line of defense;
- approve risk appetite limits cascaded to the level of Group members with regard to risks managed by the Committee;
- approve other risk containments, including those based on qualitative indicators, according to the proposal of a business unit of the 2nd line of defense;
- control the compliance with limits and/or other restrictions based on qualitative indicators;
- adopt resolutions, within its powers, on management of particular risks, aimed at compliance with the established containments, and approve the measures to settle violations of the established risk appetite limits of the Group and the Bank and other containments;
- review and approve the policies for management of substantial/material[23] risks of the Group as related to the line of activity of this committee[24], for further approval by the Bank's Executive Board or Supervisory Board in accordance with the requirements set forth by regulators;
- approve other IRDs regulating the processes of management of particular risks in accordance with /17/;
- control the activities of accountable committees[25].

### 5.3.8. The Integrated Risk Management Department of the Bank shall:

- develop, support and improve the Risk and Capital Management Strategy of the Group on a consolidated basis, and ensure its compliance with the Development Strategy, requirements and recommendations of the Bank of Russia, the BCBS recommendations, and best world practices;
- organize the process of risk identification and materiality assessment in the Group;

[21]The list of the Bank's committees for management of substantial/material risks shall be approved within annual identification and materiality assessment of risks.
[22] The approval level of limits and containments may differ and be specified in IRDs for particular risks.
[23] If any policies for management of substantial risks are available.
[24] If provided for in the Regulation on the respective Bank's Committee for Management of Substantial/Material Risks.
[25] The term 'accountable committees' means the list of committees and functions delegated to them within the system of management of substantial/material risks of the Group.

- cause generation of the following reports in accordance with Appendix 6:
  - on results of Group's ICAAP implementation;
  - on stress testing results for the Group;
  - on organization of Group's ICAAP and their results according to the form stated by the Bank of Russia /4/;
  - aggregated reports at the level of substantial/material risks with a view to presentation of information to the Supervisory Board, the Executive Board, and collegial working bodies of the Bank, which manage the Group's risks, in accordance with the requirements set forth in Subclause 6.5 of this Strategy;
- inform the Bank's Executive Board and the Bank's Supervisory Board about violations of the established risk appetite and regulatory ratios by the Group / the Group member upon identification[26];
- coordinate the process for establishing and controlling the risk appetite of the Group and the Bank;
- generate the proposals on the risk appetite values of the Group and the Bank, on inclusion of indicators in the risk appetite of the Group members, on proposed limits as approved by the Treasury (with regard to mandatory and other capital ratios) and business units of the 2nd line of defense;
- perform the aggregated assessment and forecasting of the aggregate level of the Group's substantial/material risks, as well as monitor and control the aggregate level of the risk taken;
- develop the stress testing schedule (program) for the Group;
- coordinate the interaction of business units when elaborating scenarios and performing stress testing of the Group as part of ICAAP;
- perform stress testing of substantial risks of the Group;
- coordinate and organize development of the Group's FSR plan;
- consolidate information about risks for the purposes of disclosure in accordance with the requirements of the Bank of Russia /28/;
- ensure the development of methodology and internal documents regulating the credit risk management in the Group(upper-level group requirements);
- ensure the methodological support on compliance of the systems of management of substantial/material risks with the risk management requirements in the Group and with the requirements of the Bank of Russia;
- negotiate the policies and regulations for management of substantial/material[17] risks;
- maintain the register of IRDs on integrated risk management and general issues of management of substantial/material risks;
- perform other functions within integrated risk management.

[26] The notification procedure is specified in other IRDs of the Bank.

### 5.3.9. The Bank's Treasury shall:

- develop the proposals concerning the list of indicators[27] and their thresholds with regard to capital adequacy for their inclusion in the risk appetite of the Group;
- distribute and control the implementation of the group standards of capital adequacy management at the level of the Group members;
- develop the capital adequacy management plan of within the business planning procedure of the Group as a whole, and the capital adequacy management plan of the Group in crisis conditions;
- carry out regular forecasting of capital adequacy ratios for the Group and develop the forecasting techniques;
- monitor the compliance with the risk appetite with regard to capital adequacy ratios and other internal limits for actual and anticipated values of capital adequacy ratios;
- develop the proposals and measures for capital adequacy management, submit those for consideration of an authorized collegial body of the Bank, and coordinate their implementation;
- take part in stress testing of the Group within ICAAP;
- take part in development of the FSR plan of the Group, within its competence;
- perform other functions on capital adequacy management in accordance with /25/.

### 5.3.10. The Bank's Finance Department shall:

- determine the business planning principles and develop (coordinate development of) respective methodologies/regulations;
- develop the financial structure of the Group, including the perimeter of and criteria for consolidation of companies in order to generate the business plan and the proposals for formulation of business plan targets;
- prepare the consolidated business plan and the mechanism to control the compliance with indicators of the Group's business plan;
- consolidate the financial statements of the Group for the purposes of management statements.

### 5.3.11. The Bank's business units performing the functions of the 1st line of defense

are specified in IRDs on management of substantial/material risks.

### 5.3.12. The Bank's business units performing the functions of the 2nd line of defense

are specified in IRDs on management of substantial/material risks.

The functions of the Bank's units performing functions of the 1st and 2nd lines of defense within the system of management of substantial/material risks are described in IRDs on management of respective risks.

[27] The term 'indicator' corresponds to the term 'risk metric'.

### 5.3.13. The Validation Division of the Bank shall:[28]

- validate all Sberbank Group's models compliant with requirements according to /37/.

### 5.3.14. The Bank's business unit responsible for risk

For each risk (substantial/material risk), GRC shall specify, by its resolution, one business unit (or special employee) of the Bank[29], which shall:

- develop, support and improve the substantial/material risk management system at the Group's level with possible involvement of other business units of the Bank and/or outside organizations, including:
  - IRDs[30] specifying the methodology for management and assessment of a substantial/material[31];
  - risk assessment models;
  - management processes and procedures;
  - requirements to division of powers;
- generate standards and requirements for the methods and processes of management of substantial/material risk for the Bank and/or the Group members;
- interact with the Risk Management Department[32] within the risk and capital management system;
- organize the substantial/material risk management system in the Bank and/or the Group.[33]

Depending on specifics of particular risks, the business unit responsible for risk may be that outside the Risks Block, if it has the required competencies and resources to generate the efficient risk management system. As a rule, the business unit responsible for risk is that performing the functions of the 2nd line of defense. In specific cases, the business unit responsible for risk may be that performing the functions of the 1st line of defense. In this case, the policies and regulations for management of substantial/material risks shall be agreed upon with the business unit performing the functions of the 2nd line of defense.

### 5.3.15. The Internal Audit Service of the Bank shall:

- perform the functions of the 3rd line of defense, namely:
  - assess the efficiency of the risk and capital management system, in particular, verify the efficiency of the risk assessment methodology and risk management procedures

[28] The Validation Division is a part of the Risks Block, and it is functionally independent of business units developing and using risk assessment models.
[29] With due regard to the organizational structure of the Bank/ the Group member, several business units (or employees) may be determined by business segment, line of business, etc., with clear differentiation of the areas of responsibility, within the system of management of a particular risk.
[30] Developed IRDs shall be approved in accordance with requirements set forth in /17/.
[31] The business unit responsible for risk may engage other business units of the Bank and/or external organizations for performing the above functions.
[32] For the business units outside the Risks Block.
[33] The list of substantial/material risks is defined in the annual Report on the identification and assessment of the materiality of risks of the Sberbank Group.

established by IRDs of the Bank and the Group members, as well as whether the above mentioned documents are applied in full;

- inform the Supervisory Board and the executive bodies of the Bank about deficiencies identified in operation of the risk and capital management system, as well as about actions taken to eliminate them;

- generate the requirements to organization of internal audit in the Group members with regard to efficiency assessment of the risk and capital management system.

#### 5.3.16. The Group members – management companies of sub-holdings shall:[34]

- organize the risk and capital adequacy management process at the sub-holding level according to the principles determined by this Strategy, the group documents, and with due regard to the requirements of local regulators in the countries of operation of the Group members;

- provide the Bank with the information required for integrated risk management and management of substantial/material risks.

#### 5.3.17. The Group members beyond sub-holdings shall:

- organize risk and capital adequacy management at their levels in accordance with principles specified in this Strategy, group documents and with due regard to requirements set forth by local regulators in countries of Group members' presence, as well as with standards and requirements to methods and processes for substantial/material risk management developed by units responsible for risks;

- provide the Bank with the information required for integrated risk management and management of substantial/material risks.

Risk and capital management functions in the Group members should be organized in accordance with the requirements set forth by local regulators and the approaches to risk management organization established in the Group, and with due regard to the organizational structure of the Group members.

## 6. Organization of the Risk and Capital Management System

The integrated risk management process shall include 5 stages. The risk management system shall be created for all substantial/material risks in accordance with the requirements of Subclause 6.2. The procedure for management of substantial risks is given in Appendix 8.

### 6.1. Integrated Risk Management Process

#### 6.1.1. Identification and Materiality Assessment of the Group's Risks

The approach to identification of the Group risks applied by the Group shall depend on the risk identification perimeter:

- regulatory perimeter;

- ecosystem perimeter.[35]

[34] With due regard to specifics, nature and scope of the Group member activities.

[35] The ecosystem perimeter does not stand out in the Group's members, since the Bank builds the risk management system in the ecosystem companies.

*Regulatory perimeter*

The following Group members shall be included in the regulatory risk identification perimeter of the Group:

- the Bank;
- the Group members whose risks are recognized within ICAAP of the Group according to the requirements of /4/;
- the Group members for which the requirements of local regulators are established in terms of risk management, and whose risks are not recognized within ICAAP of the Group according to the requirements of /4/;
- other Group members who may bear high risks for the Group.

Scheduled risk identification and materiality assessment in regulatory perimeter companies shall be conducted once a year and completed before the start of the annual business planning cycle. In case of any significant changes in the external environment and/or within the Group that may affect the risk level of the Group, unscheduled risk identification and materiality assessment may be performed.

The Bank shall assess risk materiality at the level of the Bank/ the Group members and the Group as a whole. The Group members also shall assess risk materiality at the local level if the local regulator and/or the Bank require(s) that.

All potential risks of the Group according to the world practice and recommendations of regulatory authorities and BCBS shall be included in the list of risks for their materiality assessment.

Risks, in respect of which the Bank of Russia establishes mandatory ratios for credit institutions/ banking groups and/or which are taken into account in the calculation of adequate regulatory capital of credit institutions/ banking groups, shall be recognized, by default, as material for the Bank / the Group.

Risks that are subject to annual materiality assessment shall be assessed on the basis of established quantitative criteria or expert estimates. Criteria for risk materiality at the Group level shall be specified in accordance with the internal methodology in effect at the date of identification.

At the Group level, risks may be classified as material, substantial, and non-material. At the Bank / Group member level, risks may be classified as material, substantial, non-material, non-relevant. The risk may be recognized as substantial/material for the Group member, but non-material for the Group as a whole. During materiality assessment, the Group members shall rely on the standards approved in the Group with due regard to the requirements of local regulators.

The list of Group / Bank / Group member risks with specification of their materiality shall be approved by GRC. Requirements to the capital for coverage of every substantial/material[36] risk shall be established on an individual or aggregated basis.

Depending on whether the risk as classified as material, substantial, non-material, non-relevant, different requirements shall be specified for generation of the system to manage this risk (for more details see Subclause 6.2).

*Ecosystem perimeter*

[36] Except liquidity risk.

In addition to the regulatory perimeter of risk identification, the Group shall identify risks in ecosystem companies. The ecosystem parameter of risk identification includes all ecosystem companies except for those included in the regulatory perimeter[37].

Requirements to identification of risks characteristic for companies from the ecosystem perimeter are based on principles set forth in this Strategy, but make allowance for specifics of ecosystem companies and the absence of regulatory requirements to them.

Companies from the ecosystem perimeter belong to Category 6 of the Group members, in accordance with which requirements to substantial/material risks of such companies shall be specified by units responsible for risks, and requirements to ICAAP shall not be imposed (see Appendix 4). If there is a new risk identified in an ecosystem company, for which the Bank does not have an approved unit responsible for the risk, due to the limited and specific nature determining the risk inherence only to this company, a decision on materiality of such risk and the need for arranging work with it shall be made by the International Business and Ecosystem Risks Division, together with other units of the Bank, where applicable.

*Risk identification in other companies*

Units responsible for risks[38] may identify and assess materiality of respective risks in the Group companies not included in the regulatory and ecosystem perimeters. In such a case, the approach to risk identification and materiality assessment shall be specified by units responsible for risks.

### 6.1.2. Aggregated Assessment of Risks and Overall Capital

The methodology for aggregated risk assessment shall be determined for the substantial/material risks for which the capital requirements are established. In order to ensure the possibility of aggregating data for the purpose of determining the overall capital required to cover losses should the risk realize, the required capital calculation approaches applied by the Group members shall be agreed with the Bank.

As a rule, for any substantial/material risks with no quantitative models for estimating the required capital, the necessary capital amount is allocated to cover these risks and it is determined by judgement in accordance with the approved inside methodology.

The required capital amount also may be allocated to cover the risks arising from business development measures provided for by the Development Strategy of Sberbank or the development strategy of the Group member, as well as the risks which may not be shared among structural units of the Bank or the Group member or such sharing is difficult.

The assessment models of the required capital (economic capital) used in ICAAP are subject to annual validation procedure.

Risks for which the capital requirements are not established (e.g. liquidity risk) shall be assessed with the use of different methods.

[37] For such companies, in addition to the risk identification procedure according to the criteria of the regulatory perimeter, according to the decision of the ecosystem CRO, risk identification can be carried out using the criteria of the ecosystem perimeter.

[38] If the division responsible for the risk is not a division of the 2nd line of protection, identification and development of an approach to it is carried out with the involvement of the division of the 2nd line of protection.

### 6.1.3. Determination of the Risk Appetite of the Group/ the Bank/ the Group Member

Risk appetite means the aggregate maximum risk level of the Group/ the Bank/ the Group member that the Group/ the Bank/ the Group member is ready to accept in the course of creating shareholder value and achieving established strategic goals.

The risk appetite shall be established in accordance with the following principles:

- The Group provides a complete range of banking services, so the Group's risk appetite contains limitations on all substantial/material risks inherent in banking, among others, through allocation of the required capital amount.

- The Group's risk appetite excludes the targets for return or administrative and management expenses which are set under business planning. The risk appetite does not duplicate, but complements the Development Strategy and business plans through determining the maximum permissible level of risks.

- The risk appetite contains signal and limit values (limits). For each indicator of risk appetite, two boundaries are defined: the limit of the "yellow zone" and the limit of the "red zone" of risk appetite or equivalent concepts adopted by the relevant collegial working body. The limit of the "yellow zone" means the limit, the excess of which should signal the need to take / initiate management measures aimed at preventing violations of the limit of the "red zone". The limit of the "red zone" of risk appetite means the final limit, the value of which should not be violated. Target risk levels are understood as forecast values of the indicator that do not violate the border of the "yellow zone" of risk appetite over the entire planning horizon. The risk appetite is developed in accordance with the Development Strategy and with due regard to the stress testing results.

Risk appetite shall be developed taking into account the Development Strategy and taking into account the results of stress testing.

When determining the indicators to be included in the risk appetite, the following requirements and containments shall be taken into account:

- effectiveness of indicators as a risk containment measure with due regard to their historical dynamics;

- sufficiency of coverage of the Group's substantial/material risks revealed in the course of risk identification and materiality assessment;

- conformance of the indicators to existing and prospective regulatory requirements.

The Group's risk appetite shall be established for all substantial/material risks of the Group for the strategic planning horizon. The risk appetite shall be approved by a separate resolution of the Supervisory Board of the Bank and shall be an integral part of this Strategy. The risk appetite for particular risks can be established in the form of aggregated indicators for several risks. Qualitative indicators of risk appetite shall be determined as risk management principles and the target rating. Risk containments approved by the Bank's Supervisory Board shall be communicated to the operational management level of the Bank and Group members through the limit cascading system and establishing the risk appetite of Group members at the local level with a view to control substantial/material risks taken by the Bank and Group members.

The Bank's Supervisory Board shall consider the issue of the necessity to change the Group's risk appetite at least once a year. Particular values of the risk appetite may be updated during a financial

year in case of changes in the economic situation and/or alteration of the requirements for credit institutions and/or banking groups (alteration of the existing ratios and/or introduction of new ratios).

The risk appetite implies the set of indicators. The following risk appetite levels shall be distinguished:

- Level A – key indicators for the Group, including capital adequacy, portfolio quality, liquidity metrics, as well as for substantial risks for the Group to be approved at the level of the Bank's Supervisory Board;
- Level B – capital allocation limits and metrics for particular risks to be approved at the level of the Bank's collegial working bodies;
- Level C – metrics for the Group member to be approved by its Board of Directors (Supervisory Board);
- Level D – Group member's risk limits that are not included in the local risk appetite at the level of the Board of Directors (Supervisory Board) of the Group member;[39]

In order to ensure control of risk appetite at the level of Group members and their divisions, the above limits are translated into a system of operational limits (level D limits) approved by authorized collegial bodies, divisions and managers of a Group member. As part of the Group's risk appetite, the target risk structure is approved in order to monitor the amounts of substantial/material risks accepted by the Bank and the Group members. The target risk structure for the risks for which capital requirements are determined is the distribution of substantial/material risks in the form of their share in the AFR.

The risk appetite of the Bank and the Group members shall be set with due regard to the risk appetite of the Group.

### 6.1.4. Risk Exposure Planning

The Group's risk exposure shall be planned within annual business planning process in the Group according to top-down principle: firstly, high level target indicators are determined for the Group, then they are specified for specific business lines, Group members, structural units of the Group, etc.

While planning[40] activities of the Group, one shall use the indicators that characterize (or recognize) the level of losses from risk realization in projected scenarios in both normal operations (business plan) and stress conditions. Compliance with the Group's risk appetite shall be assessed in projected scenarios.

### 6.1.5. Management of Overall Risk Exposure of the Group

The management of the Group's overall risk exposure shall comprise:

- calculation of factors characterizing a consolidated level of overall risk of the Group based on assessments of substantial/material risks, with due regard to risk correlations;
- assessment of deviation of the Group risk exposure from the levels set by the consolidated business plan of the Group;

[39] Including Sberbank

[40] As part of development of the business plan and the financial stability recovery plan.

- assessment of the compliance of risk exposure of the Group with the approved risk appetite of the Group;
- forecasting factors characterizing a consolidated level of overall risk of the Group;
- generation of the reports according to Appendix 6;
- making decisions on establishing/changing risk limits, or other decisions aimed to optimize the risk level of the Group (including risk mitigation measures) based on the information contained in the reports prepared in accordance with Appendix 6, and control over execution of such decisions;
- control over execution of risk mitigation measures in case of risk appetite limits violation.

### 6.2. Formation and Improvement of the Risk Management System

Following the procedure of identification of the Group's risks, each risk of the Group/ the Bank/ the Group member shall be classified in one of the categories listed in Subclause 6.1.1.

For each risk recognized as substantial/material, GRC shall adopt a resolution to assign the following for the Group / the Bank[41]:

- a collegial body of the Bank to manage the risk;
- a unit responsible for risk, with specification of the line of defense[42].

The functions of the business unit responsible for risk are specified in 5.3.14.

The system for managing the risk that is recognized as substantial/material for the Group shall cover the Bank and all Group members, where this risk is recognized as substantial/material[43], while requirements to the system for managing risks in a particular Group member shall be specified with due regard to the proportionality principle described, inter alia, in Appendix 4. If the risk is recognized as substantial/material only at the Bank's level, the system for managing this risk shall be created at the Bank's level. If the risk is recognized as substantial/material only at the Group member's level, the local system for managing this risk shall be created. In this case, the Group member shall independently determine risk management approaches, establish and control risk limits and risk targets, and control the efficiency of management of this risk. If there is a service level agreement (SLA) for managing the Group member's risks is concluded between the Group member and the Bank, the Report on Identification and Materiality Assessment of Group Risks shall specify the Bank's unit responsible for managing such risk in the Group member, with specification of the line of defense.

For each risk classified as substantial/material, it is necessary to:

- determine the structural units performing the functions of the 1st and 2nd lines of defense;
- establish, if necessary, the accountable committees (i.e. the list of committees and functions delegated to them within the risk management system);

[41] For the Group member, a collegial body for risk management or a business unit responsible for risk shall be assigned in accordance with the local procedures accepted by the Group member.
[42] If the business unit responsible for risk is from the 1st line of defense.
[43] In such case, IRD on management of a substantial/material risk shall apply to the Group as a whole, and no development of specific IRDs at the Bank's level is required.

- develop and approve IRDs that determine the procedure[44] for operation of the risk management system.

The risk management system shall ensure performance of the following functions:

- risk identification;
- risk assessment with using quantitative and/or qualitative methods;
- determination of risk management approaches and methods, as well as the list of risk mitigation measures (use of collateral, etc.);
- determination of limits and other containments on risk level, as well as target values, the achievement of which signals the need to implement risk mitigation measures;
- control over volumes of accepted risks, escalation of violating stated risk limits and/or containments;
- generation of reports at the level of accepted risk and on results of efficiency assessment of applied risk management methods.

The requirements for building the risk management system shall depend on whether the risk is classified as substantial or material:

- **substantial risks**: the risk management system shall comply in full with Subclause 6.2 of this Strategy, as well as with the regulatory requirements as part of building the risk management system, including /4, 7/;
- **material risks**: for risks classified as material, only minimum mandatory requirements shall be specified:
  - available approach to risk assessment by a quantitative and/or qualitative (expert) method;
  - available system of limits and/or restrictions, which may be based on expert estimates;
  - taking into account these risks in the risk appetite by providing the required capital amount to cover these risks on an aggregate basis;
  - available reporting system which allows to control the level of accepted risk (completeness and periodicity of management reports are determined by a business unit responsible for risks);
  - periodicity for assessment of quality and efficiency of the system for managing these risk shall be determined according to INAS inspection schedules;
- **non-material**[45] **risks** and **risks that are non-relevant**[46] **to an organization**: the risk management system is not required.

While determining an approach to build the risk management system, it is necessary to be commuted to the principle of proportionality regarding economic efficiency of building the risk

[44] One document may be developed for several risks.
[45] The division responsible for risk may impose additional requirements on a Group member in relation to non-material risks, including requirements regarding the provision of necessary information for consolidated financial statements.
[46] The concept of "non-relevant risks" applies only to the Bank and the Group members, but not to the Group as a whole.

management system in Group members where the risk is considered as substantial/material. Delegation of risk management functions from one Group member to another or the Bank is allowed, excluding[47] the functions of the board of directors (the supervisory board) / executive bodies / the head of the risk management department.

### 6.3. Capital Adequacy Management

The process of the capital structure and adequacy management of the Group is centralized. The Bank's Treasury is a business unit responsible for organization of capital adequacy management in the Group and the Bank. To implement an efficient process of capital structure and adequacy management, the Bank's Treasury develops necessary procedures, regulations for cooperation between business units, methods and group standards, and also controls the organization of the process in the Group members.

Capital adequacy management shall be in place in each member of the Group subject to the mandatory capital adequacy requirements set by regulators, or the requirements for risk appetite as related to capital adequacy approved by the Bank's competent collegial body, as well as in other members of the Group stipulated by a specific resolution of ALMC. The Group members shall organize capital adequacy management according to principles stipulated in the Capital Adequacy Management Policy of the Group[48] /25/ and other Group standards. The following key tools are used for capital adequacy management:

- business planning and a capital adequacy management plan;
- planning of dividends and capitalization of subsidiaries;
- system of capital adequacy ratio limits;
- capital adequacy management plan in case of a crisis situation /26/.

### 6.4. Stress testing

The stress testing is an analytical tool for assessment of a potential impact of preset risk factor changes on financial position, capital adequacy and liquidity of the Group based on scenario analysis and analysis of credit institution sensitivity to changes in risk factors.

The stress testing covers all substantial/material risks of the Group. One shall apply a combination of centralized and decentralized approaches to stress testing at the Group's level. In case of the decentralized approach local stress testing results received based on the overall group stress scenario shall be aggregated from the level of sub-holdings and the Group members beyond sub-holdings. The Bank shall assess regularly considered stress scenarios, as well as quality of used data and assumptions of stress testing.

Stress scenarios of the Group shall be approved by the Bank's Supervisory Board and shall be an integral part of the Strategy. The reports on stress testing results shall be provided to GRC, the Executive Board and the Supervisory Board of the Bank.

Stress testing results shall be taken into account while establishing risk appetite of the Group, developing the capital adequacy management plan (preventive measures as part of a business plan) and the financial stability recovery plan of the Group .

[47] The exception is not applicable to non-financial institutions.

[48] This Policy applies to the Group as a whole, Sberbank, and the Group members in respect of which the Group may exercise control over operating and financial activities.

The Group members develop their own stress testing procedures which shall be agreed upon with the Bank.

### 6.5. Reports

The Group shall abide by the following main principles in reports preparation:

- Rationality: Reports preparation shall focus on achieving maximum efficiency of the reporting system by ensuring the availability of all necessary information meeting the regulators' requirements and allowing to make management decisions.
- Understandability: The reports shall be understandable for the target audience in terms of the level of detail and scope of information contained therein.
- Transparency: The risk reports shall contain correct, comparable and accurate data.
- Comprehensiveness: The reports shall include information on all substantial/material risks, as well as information on compliance with the regulatory requirements. The reports shall contain a comparison of the accepted risks against available capital to cover accepted risks.
- Comparability and aggregability: The format of reports shall allow to aggregate information on various substantial/material risks and units to ensure complete representation of the risk profile at the Group's level.
- Match: The risk reports shall be comparable with previous periods. All decisions on changes in reports shall be disclosed, and data for past comparable periods shall be calculated[49] according to accepted changes.
- Timelines: The reporting system shall be organized in a way, that, in case of crisis conditions, would allow to shift to prompt provision of data on actual and target risk level and structure in order to timely take management measures.
- Integrity: the reports shall be prepared with an established frequency and the contents of reports shall be provided in a structured form.

The Group has in place the process of collection, verification and consolidation of data provided by the Group members in order to calculate capital value, mandatory ratios and other risk factors.

The risk level of the Group shall be disclosed in accordance with Appendix 6.

### 6.6. Audit of the Risk and Capital Management System at the Group's Level

The effectiveness of the internal risk management and capital adequacy assessment systems (hereinafter the audit of the risk and capital management system) at the level of the Bank/ the Group shall be inspected annually in accordance with the requirements of the Bank of Russia /4/ and as per INAS inspection schedules. The risk and capital management system shall be audited with due regard to the principle of proportionality and limited resources.

The Head of INAS of the Bank shall communicate the information on identified deficiencies in the risk and capital management system of the Bank/ the Group, and on actions taken to eliminate them to the Supervisory Board and the Executive Board of the Bank at least once a year as part of the reports submitted by INAS to the Supervisory Board and the Executive Board.

[49] If available.

## 7. Final Provisions

This Strategy shall be approved by the Bank's Supervisory Board and be revised as the requirements of state regulatory authorities change and new effective risk management methods and tools emerge in accordance with the best international practice, but at least once a year.

**APPENDIX 1. List**

## List of Terms and Definitions

**CRO of the Bank (CRO of the Group)** is a head of the Risks Block of Sberbank.

**CRO Supervising the Group Member** is CRO of a business block responsible for the supervised Group Member (in accordance with /30/)[50].

**CRO of a Business Block** is an employee who is responsible for interaction between the Risks Block and the business block as part of the risk management system, and serves as 'a single access gateway' of communications for the business block. CRO of the Business Block performs the risk management functions, including, but not limited to the following: is responsible for building the risk management system in the Bank and the Group Members; organizes work on risk management within his/her area of responsibility through interaction with the Bank's business units and the Group Members; monitors the implementation of the risk management targets in the Group Members. CRO of the Business Block is also a member of collegial bodies of the Bank/ the Group Member.**CRO of the Ecosystem** is a head of the International Business and Ecosystem Risks Division of Sberbank, who is responsible for interaction between the Risks Block and ecosystem companies as part of the risk management system.

**Risk Appetite** means the aggregate maximum risk level of the Group/ the Bank/ the Group Member that the Group/ the Bank/ the Group Member is ready to accept in the course of creating shareholder value and achieving established strategic goals.

**Sberbank Group (Group)** means the banking group defined according to /1/, where Sberbank is the parent credit institution.

**Digitalization** means activities on process optimization, which implicate obligatory use of technological components providing a client with the necessary service level.

**Capital Adequacy** means adequacy of disposable (available) capital to cover the overall amount of accepted and potential risks. The capital adequacy ratio shall be calculated as a ratio of available capital to the overall amount of accepted and potential risks.

**Available Capital** means disposable capital to cover the overall amount of accepted and potential risks, which is calculated for both regulatory and internal goals.

**Available Financial Resources** mean the capital at the disposal of the Group/ the Bank/ the Group Member, available to cover accepted and potential risks, that is assessed under the internal models of the Group/ the Bank/ the Group Member, among others, using internal assessments of expected losses.

**Risk identification** means a process of detection and classification of risks.

**Risk appetite cascading** - decomposition and / or transfer of risk appetite to the level of structural divisions, authorized working collegial bodies and to the level of the Group members.

**Collegial Working Bodies of the Bank (CWB)** are those the establishment and termination of which fall within the competence of the Bank's Executive Board pursuant to the Bank Charter.

**Controlled Member of the Group**, for the purposes of this Strategy, means the Group Member in which the Bank is the sole participant, shareholder, incorporator (100% interest, either direct or indirect) or has a dominant participation (>50% interest, either direct or indirect).

**Major Group Member** means the Group Member whose equity (capital) calculated excluding operations (transactions) between the parent credit institution of the banking group and (or) banking group participants is equal to 5 and more percent of the equity (capital) of the banking group, and (or)

[50] For the Group Members falling under /31/, it is CRO of the Sberbank International Block.

financial result, excluding gains (losses) from operations (transactions) between the parent credit institution of the banking group and (or) banking group participants, is equal to 5 and more percent of the financial result of the banking group (calculation is made in absolute values with ignoring a sign of the financial result of the banking group participant or the banking group as a whole), and (or) assets which are weighed taking into account the risk and calculated excluding operations (transactions) between the parent credit institution of the banking group and (or) banking group participants are equal to 5 and more percent of banking group assets weighed taking into account the risk. The definition corresponds to the second paragraph of Subclause 6.7 of Bank of Russia Ordinance No. 4482-У (4482-U) dated 7 August 2017 On Forms and Procedures for Disclosure by Credit Institutions (Parent Credit Institutions of Banking Groups) of Information on Accepted Risks, Risk Assessment Procedures, Risk and Capital Management Procedures.

**Risk Limit** means a preset numeric limitation of the indicator value characterizing the risk level (risk metric). The limit can be set as either an absolute value and/or a relative one.

**Material Risk** means a risk that is not recognized as substantial, in respect of which the requirements are imposed on availability of the management system according to Subclause 6.2.

**Model** means a quantitative method, system or approach in which statistical and mathematical theories are applied to input data to obtain quantitative estimates.

**Necessary (Required) Capital** means the capital value of the Group/ the Bank/ the Group Member, which is necessary to cover any risks taken by the Group/ the Bank/ the Group Member in its operations.

**Non-Relevant Risk** means a risk that does not arise at the Bank/ the Group Member due to the absence of transactions exposed to such risks and of plans on such transactions within the business planning horizon.

**Non-Material Risk** means a risk that has not been recognized as non-relevant, substantial or material.

**Non-Financial Institutions** are legal entities engaged in production of goods and provision of non-financial services or works, that is, the entities that do not belong to financial institutions which are legal entities that carry out banking operations and transactions pursuant to an appropriate license or provide services in the securities market, insurance services, services rendered in accordance with a lease agreement, services for provision of secured loans, or other financial services, namely, those not related to investment companies, management companies, stock exchanges, brokerage organizations, leasing companies, entities that effect financing against assignment of monetary claims (factoring companies), private pension funds, management companies of private pension funds, management companies of mutual investment funds, consumer credit unions, microfinance organizations, pawnshops, self-regulatory organizations of the financial market, insurance agents or brokers being legal entities, and other entities carrying out operations and transactions in the financial services market.

**Financial Markets Transactions** mean purchase or sale of currency in cash or non-cash form, marketable securities, precious metals and other commodities, placement or attraction of loans/deposits in currency or precious metals in the interbank lending market, direct or reverse repurchase transactions, and derivative transactions.

**Risk Assessment** is an assessment of the risk probability and the potential losses and/or other negative effects in case of realization of a particular risk and/or overall risks accepted by the Group/ the Bank/ the Group Members.

**Business Unit Responsible for Risk** means the business unit responsible for building a system to manage the risk recognized as substantial or material.

**Risk Taking** means an action (or omission) resulting in a change in the risk level of the Group. The risk taking by the Group shall take place:

1. when resolutions are adopted to enter into transactions, perform operations, sign a services agreement between the Bank or the Group Member and external/internal counterparties to the Group (for credit and market risks, as well as liquidity risk);

2. when the participants of the risk and capital management system (Subclause 5.3) perform any functions associated with the risks other than those related to adopting resolutions on performance of operations or conclusion of transactions (e.g. compliance risk).

For any risks managed on a consolidated basis (liquidity risk, interest rate and currency risks in the banking book), there are active risk acceptance (at the time of making an operation/transaction) and passive risk acceptance (through consolidation of a position exposed to this risk).

**Regulator** is an authorized body exercising the functions of regulation, control and supervision of the activities of credit institutions, banking groups, non-credit institutions, and also in financial markets (as applied to the Russian Federation in accordance with Chapters X, X.1 /35/).

**Regulatory Standards or Ratios** are standards or ratios calculated by the Group/ Bank/ Group Member within the jurisdiction of the Russian Federation in accordance with the requirements established by the Bank of Russia, and standards or ratios calculated by the Group Member outside the jurisdiction of the Russian Federation in accordance with the requirements established by a local regulator, and also standards or ratios calculated in accordance with the requirements established by other governmental authorities or international institutions that develop regulation for certain business areas.

**Regulatory Capital** means the capital value of the Group/ the Bank/ the Group Member, which is required to cover any risks accepted in the course of activities and the determination methodology of which is prescribed by the regulator[51].

**Risk** means the possibility, inherent to the Group's activities, of occurrence of an event that results in financial losses of the Group and/or negatively affects the Group's reputation and/or liquidity position.

**Internal Audit Service of the Bank** means a complex of the Bank's structural units (the Internal Audit Division of the Bank's Central Head Office and relevant business units of the Internal Audit Service in the Bank branches) carrying out their activities in compliance with the Regulation on the Internal Audit Service of Sberbank.

**Risk Management Department of the Bank** means a set of the Bank's independent structural units which are part of the Risks Block of Sberbank.

**Stress Testing** means an analytical tool for assessment of a potential impact of preset risk factor changes on financial condition, capital adequacy and liquidity of the Group/ the Bank/ the Group Member in improbable, but possible stress scenarios, using approaches based on scenario analysis and sensitivity analysis.

**Sub-holding** means an association of the Group Members that is not a legal entity, where the parent institution (hereinafter the management company of sub-holding) has an opportunity to use its powers directly or indirectly (through third parties) to influence the decisions made by executives, management and collegial bodies[52] of other sub-holding members, and also the amount of their financial result. The

[51] On the level of the Group, the Bank, the Group Members, meaning credit institutions subject to regulation of the Bank of Russia, the capital value is determined in accordance with Bank of Russia Regulation No. 646-P dated 4 July 2018 On the Methodology for Determining the Equity (Capital) of Credit Institutions (Basel III).

[52] The terms 'management body' and 'collegial working body' are defined in /16/.

management company of sub-holding is a controlled subsidiary of Sberbank (in which the direct equity interest of the Bank is more than 50%). The Bank itself may be a management company of sub-holdings.

**Substantial Risks** mean risks, which, if realized, have adverse consequences that impact the consolidated financial result and/or available capital and/or liquidity of the Group/ the Bank/ the Group Member, as well as reputation of the Group/ the Bank/ the Group Member or the capability to comply with the requirements of the regulators in the Russian Federation and in the countries of operation of the Group Members.

**Risk Management** means a complex of measures to identify, assess, and aggregate all substantial/material risks, monitor, constrain, and control the amount of taken risks, plan the risk level, implement the measures to mitigate the risk level in order to keep the amount of taken risks within the set external and internal containments in the course of implementation of the Development Strategy approved by the Supervisory Board of the Bank.

**Group Member** is a legal entity under control or significant influence of Sberbank, a parent credit institution of the banking group as defined in accordance with /1/.

**Economic Capital** means the amount of capital of the Group/ the Bank/ the Group Member required to cover unexpected losses on a given time horizon with an established level of confidence probability, which is determined, inter alia, on the basis of target rating.

**APPENDIX 2.**

## Abbreviations

**CRO** stands for Chief Risk Officer.

**RA** stands for Risk Appetite.

**AS** means an automated system.

**The Bank** means Sberbank.

**Bank of Russia** means the Central Bank of the Russian Federation.

**BCBS** stands for Basel Committee on Banking Supervision, a committee of banking supervisors, which was established by the central bank governors of the G-10 countries in 1974.

**Risks Block** means the Risks Block of Sberbank.

**IRD** stands for Internal Regulatory Document.

**ICAAP** stands for Internal Capital Adequacy Assessment Process.

**FSR** stands for Financial Stability Recovery.

**SB** stands for subsidiary bank.

**IRMD** stands for Integrated Risk Management Department.

**SC** stands for Subsidiary Company.

**AFR** stands for Available Financial Resources.

**KRIs** stand for Key Risk Indicators.

**CWB** stands for Collegial Working Body

**LICS** stands for Loans and Investments Committee of Sberbank.

**KPI** stands for Key Performance Indicators.

**GRC** stands for Group Risk Committee of Sberbank.

**MRC** means Market Risks Committee of Sberbank.

**ALCO** stands for Assets and Liabilities Committee of Sberbank.

**CSRBB** means Market Credit Spread Risk of Securities of the Banking Book.

**IFRS** stand for International Financial Reporting Standards.

**SPB** stands for Supervisory Board.

**OAD** stands for Organizational and Administrative Document.

**INAS** stands for Internal Audit Service of Sberbank.

## APPENDIX 3. List of Reference Documents

1. Federal Law No. 395-1 dated 02/12/1990 On Banks and Banking Activities.
2. Letter of the Bank of Russia No. 06-52/2463 dated 10 April 2014 On the Corporate Governance Code.
3. Letter of the Bank of Russia No. 14-T dated 6 February 2012 On Recommendations of the Basel Committee on Banking Supervision "Principles for Enhancing Corporate Governance".
4. Bank of Russia Ordinance No. 3624-У (3624-U) dated 15/04/2015 On Requirements for the Risk and Capital Management System of Credit Institutions and Banking Groups.
5. Letter of the Bank of Russia No. 96-T dated 27 May 2014 On Recommendations of the Basel Committee on Banking Supervision "Principles of Risk Aggregation and Submission of Risk Reports", the appendix Principles of Risk Aggregation and Submission of Risk Reports.
6. Bank of Russia Regulation No. 242-P dated 16 December 2003 On the Organization of Internal Controls in Credit Institutions and Banking Groups.
7. Bank of Russia Ordinance No. 3883-У (3883-U) dated 07/12/2015 On Procedure for Assessing the Quality of Risk and Capital Management Systems and the Capital Adequacy of Credit Institutions and Banking Groups by the Bank of Russia.
8. Bank of Russia Ordinance No. 4482-У (4482-U) dated 07/08/2017 On Forms and Procedures for Disclosure by Credit Institutions (Parent Credit Institutions of Banking Groups) of Information on Accepted Risks, Risk Assessment Procedures, Risk and Capital Management Procedures.
9. Bank of Russia Regulations No. 729-П (729-P) dated 15/07/2020 On the Methodology for Calculation of Equity (Capital) and Mandatory Ratios, Capital Adequacy Ratio Buffers, Mandatory Ratio Values, and Open Currency Positions (Limits) of Banking Groups.
10. Principles for Perfecting the Corporate Governance, October 2010, BCBS (ISBN 92-9131-844-2).
11. Corporate Governance Principles for Banks, July 2015, BCBS, Consultation Document: Recommendations (ISBN 978-92-9197-130-5 (hard copy), ISBN 978-92-9197-126-8 (online)).
12. Principles of Risk Data Aggregation and Submission of Risk Reports, BCBS, January 2013, (ISBN 92-9197-913-9).
13. Basel III: Completion of post-crisis reforms, December 2017, BCBS.
14. Directive 2013/36/EU of the European Parliament and the EU Council dated 26 June 2013 on Access to the Activity of Credit Institutions and on Prudential Supervision of Credit Institutions and Investment Companies, amending Directive 2002/87/EU and repealing Directives 2006/48/EU, 2006/49/EU (CRD IV).
15. EU Regulation No. 575/2013 of the European Parliament and Council dated 26 June 2013 on Prudential Requirements to Credit Institutions and Investment Companies with amendments to EU Regulation No. 648/2012 (CRR).
16. Charter of Sberbank of Russia as amended.

17. Regulation for Development and Approval of Internal Regulatory Documents of Sberbank No. 360 as amended.

18. Corporate Governance Code of Sberbank as amended.

19. Sberbank's Internal Control Organization Policy No. 5234 as amended.

20. Regulation on the Internal Audit Service of Sberbank No. 3502 as amended.

21. Business Planning Regulation of Sberbank Group No. 3058 as amended.

22. Instruction of the Bank of Russia No. 154-I dated 17 June 2014 On the Procedure for Assessing the Remuneration Systems of Credit Institutions and the Procedure for Submitting to Credit Institutions the Orders to Eliminate Violations Identified in Remuneration Systems.

23. Bank of Russia Ordinance No. 4927-У (4927-U) dated 08/10/2018 On the List, Forms and Procedures for Preparing and Submitting Credit Institution Reporting Forms to the Central Bank of the Russian Federation.

24. Regulation on the Assets and Liabilities Management Committee of Sberbank No. 1850 as amended.

25. Capital Adequacy Management Policy of Sberbank Group No. 3690 as amended.

26. Capital Contingency Plan of Sberbank Group No. 4361 as amended.

27. Bank of Russia Ordinance No. 4662-У (4662-U) dated 25/12/2017 On Qualifying Requirements for the Head of Risk Management Department, Internal Control Service, and Internal Audit Service of Credit Institutions; for the Risk Management Officer and Controller of a Private Pension Fund, and the Auditor of an Insurance Company; on the Procedure for Informing the Bank of Russia about the Appointment to (Termination of) these Positions (Except for the Controller of a Private Pension Fund) and the Position of Special Officers Responsible for the Implementation of Internal Controls Rules Aimed at Countering the Legalization (Laundering) of Proceeds of Crime and the Financing of Terrorism of Credit Institutions, Private Pension Funds, Insurance Companies, Management Companies of Investment Funds, Unit Investment Funds and Private Pension Funds, and Microfinance Companies; of an Internal Control Officer of a Management Company of Investment Funds, Unit Investment Funds and Private Pension Funds; and on the Procedure for the Bank of Russia to Assess the Compliance of These Persons (Except for the Controller of a Private Pension Fund) with Qualifying and Business Reputation Requirements.

28. Bank of Russia Ordinance No. 4983-У (4983-U) dated 27/11/2018 On Forms, Procedures and Terms for Disclosing Performance Information by Credit Institutions.

29. Bank of Russia Regulation No. 483-P dated 6 August 2015 On the Procedure for Credit Risk Calculation from Internal Ratings.

30. Policy for Sberbank Participation in Profit and Non-Profit Organizations (except for foreign banks) No. 2240 as amended.

31. Sberbank of Russia's International Business Management Policy No. 3809 as amended.

32. Sberbank Group's Ecosystem Risk Management Policy No. 5137 as amended.

33. Sberbank Group's Credit Risk Management Policy No. 1303 as amended.

34. Bank of Russia Regulation No. 646-P dated 4 July 2018 On Methods of Determining the Equity (Capital) of Credit Institutions (Basel III).

35. Federal Law No. 86-ФЗ (86-FZ) dated 10/07/2002 On the Central Bank of the Russian Federation (Bank of Russia).

36. Bank of Russia Regulation No. 716-П (716-P) dated 08/04/2020 On Requirements for the Operational Risk Management System in Credit Institutions and Banking Groups.

37. Sberbank Group's Model Risk Management Policy No. 3194 as amended.

## APPENDIX 4.
## Classification of Group Members for ICAAP Purposes

In order to comply with the principle of proportionality, different requirements regarding creating the risk and capital management system shall be specified to Group Members in which substantial/material risks are identified according to results of the Group's risk identification stage (Subclause 6.1.1). Six member classes shall be distinguished in the Group:

| **Group Member (category)** | **Requirements for Risk Management System** | **Requirements for ICAAP** |
|---|---|---|
| Parent credit institution of the Group | – Shall determine risk materiality at the Group level.<br>– Shall form requirements for the substantial/material risk management system on the level of the Group and the Group Members.<br>– Shall control compliance with Group's requirements by Group Members included in the risk management system perimeter.<br>– Shall manage risks on the level of the Bank and the Group. | – Shall develop requirements for ICAAP at the Group level.<br>– Based on the Group ICAAP, shall establish approaches to ICAAP organization in Group Members on an individual basis and ensure the development of and compliance with the Group ICAAP requirements by the Group Members.<br>– Shall develop and implement ICAAP on an individual basis. |
| Major Group Member whose risks are recognized within ICAAP of the Group according to the requirements of /4/ | – The Group Member shall build in full the risk management system on an individual basis in accordance with the Group standards, the Strategy requirements and the requirements of local regulators. | – Requirements for ICAAP shall be obligatory in full according to /4/. |
| Credit institutions which are the Group Members (not major ones) whose risks are recognized within ICAAP of the Group according to the requirements of /4/ | – The Group Member shall build the risk management system on an individual basis in accordance with the requirements of the Bank. | – The Group Member shall develop and comply with, on an individual basis, the requirements of local regulators for ICAAP subject to the Group requirements. |
| Non-credit regulated[53] Group Members whose risks are recognized within ICAAP of the Group according to the requirements of /4/ | – By resolution of the business unit responsible for risk | – No requirements shall be specified to the Group Member;<br>– Capital requirements shall be assessed centrally by the Bank. |
| The Group Members whose risks are recognized within ICAAP of the Group | – By resolution of the business unit responsible for risk | – No requirements shall be specified to the Group Member;<br>– Capital requirements shall be assessed centrally by the Bank. |

[53] The Group Members whose risk management systems shall comply with the regulators' requirements.

| **Group Member (category)** | **Requirements for Risk Management System** | **Requirements for ICAAP** |
|---|---|---|
| according to the requirements of /4/ | | |
| The Group Members whose risks are not recognized within ICAAP of the Group according to the requirements of /4/ | – By resolution of the business unit responsible for risk | – Requirements are not specified. |

According to assess criteria of the Bank of Russia /7/, quality of ICAAP implementation in Group Members included in building the risk and capital management system impacts significantly on efficiency of the Group's risk and capital management system.

## APPENDIX 5.
## Organization of Interaction in the Group for Building the Risk Management System

For building the risk management system, the Group introduced the term 'sub-holding'. Sub-holding means an association of the Group Members that is not a legal entity, where the parent institution (hereinafter the management company of sub-holding) has an opportunity to use its powers directly or indirectly (through third parties) to influence the decisions made by executives, management and collegial bodies[54] of other sub-holding members, and also the amount of their financial result. The management company of sub-holding is a controlled subsidiary of the Bank (in which the direct equity interest of the Bank is more than 50%). The Bank itself may be a management company of sub-holdings.

Sub-holdings include only those companies in which both the direct and indirect equity interests of the management company of sub-holding in the charter capital of the Group Member is more than 50%.

The companies incorporated in a sub-holding and which are not a management company of sub-holding refer to the members of sub-holding. The requirements for the risk management system on the sub-holding level shall apply to all members of sub-holding.

The management company of sub-holding performs the following functions within its sub-holding in the Group:

- spreads the information about requirements for the risk management system;
- organizes identification and assessment of risk materiality;
- provides the consolidated information on sub-holding to assess the overall level of risks;
- takes part in planning risk exposure of the Group;
- participates in management of the Group's overall risk exposure;
- performs other functions during creation of the risk and capital management system for the Group.

The company which is not incorporated in a sub-holding but is controlled by the Bank (the direct equity interest of the Bank is more than 50%) takes part in the creation of the risk and capital management system on an individual basis.

[54] The terms 'management body' and 'collegial working body' are defined in /16/.

## APPENDIX 6.
## Reporting Generated within the Risk and Capital Management System of the Group and the Bank, Procedure and Deadline for Submission

| Sberbank | SPB/ Risk Management Committee of SPB | Executive Board | GRC | CRO of the Bank/ Group / members of the Bank committees for managing substantial/material risks[55] |
|---|---|---|---|---|
| On ICAAP implementation results | Annually | Annually | - | - |
| On stress testing results | Annually | Annually | Annually | - |
| On substantial risks of the Bank and the Major Group Member | Quarterly | At least once per month | Quarterly | Risk amount taken and utilization (violation) of established limits: daily;<br>Aggregated information: at least once per month |
| On compliance with mandatory ratios[56] by the Group, the Bank, and the Major Group Member | Quarterly | At least once per month | Quarterly | At least once per month |
| On the capital amount and the capital adequacy assessment results of the Group, the Bank, and the Major Group Member | Quarterly | At least once per month | Quarterly | - |
| On compliance with the risk appetite of the Group and the Bank | Quarterly | Quarterly | Quarterly | Quarterly |
| On violations of the established risk appetite and mandatory ratios by the Group and the Bank | Upon detection | Upon detection | Upon detection | Upon detection |
| Report of the Internal Audit Service on deficiencies in the operation of internal risk management systems and actions taken to eliminate them | Annually | Annually | | |

The information provided:

- on a quarterly basis, shall be included in the quarterly risk report of Sberbank;

[55] And also the heads of business units responsible for risks.
[56] For those risks, in respect of which the Regulatory Standards or Ratios are established.

- on a monthly basis, shall be included in the monthly ICAAP report of Sberbank;
- on a daily basis, shall be included in the daily ICAAP report of Sberbank.

In addition to the above reporting, by resolution of the risk-responsible business unit, any management bodies or collegial working bodies, including the substantial/material risk management committee, may receiveanother risk reporting in compliance with IRD for this risk management.

## APPENDIX 7.
## Approval Level of IRDs Governing Risk and Capital Management[57]

| Document Type | Approval Level[58] |
|---|---|
| Risk and Capital Management Strategy of the Group | The Supervisory Board of the Bank |
| Risk Materiality Assessment Methodology of the Group | CEO, Chairman of the Executive Board of the Bank |
| Regulation on Integrated Risk Management of the Group | Bank's Executive Board |
| Policies for Management of Substantial/Material Risks | Bank's Executive Board[59] |
| Economic Capital Assessment Methodologies | CEO, Chairman of the Executive Board of the Bank |
| Regulation on the Organization of Stress Testing Procedures | CEO, Chairman of the Executive Board of the Bank |
| Stress Testing Methodologies | CEO, Chairman of the Executive Board of the Bank |
| Regulations for Management of Substantial/Material Risks | Risk Management Committees of the Bank |
| Methodologies for Management of Substantial/Material Risks | CRO / Heads of Blocks in CHO/ CWB |
| Process Charts for Units Interaction | CRO / Heads of Blocks in CHO/ CWB |

[57] Subject to the requirements of the Bank of Russia /4/.
[58] The Major Group Members are advised to rely on the specified IRD approval level when approving similar documents at the local level, unless it contradicts to the established practice and the requirements of local regulators. The Major Group Members are also advised to annually advise the documents developed under ICAAP.
[59] Unless otherwise stated in IRDs of the Bank.

## APPENDIX 8.
## Procedure for Management of Substantial Risks

Identification and materiality assessment of the Group's risks are performed in accordance with the procedure specified in Subclauses 6.1.1.

**Credit Risk Management Procedure**

*Definition*

Credit risk means the risk of losses associated with full or partial loss of asset value or increase in liabilities due to default or deterioration of the credit quality (migration) of a counterparty/issuer/third party under the following instruments (including those received as security):

- a financial instrument in a counterparty transaction;
- an issuer's security;
- a derivative financial instrument linked to a credit event associated with a third party.

For the purposes of separate management of credit risks at the Group, credit risk is divided into:

*For all instruments exposed to credit risk*

- Concentration risk (in terms of credit risk) is a risk related to:
  - providing large loans to a separate borrower or a group of related borrowers;
  - the concentration of indebtedness in separate branches of economy, segments, portfolios, or geographical regions etc.;
  - implementing measures to mitigate credit risk (applying same types of collateral, independent guarantees provided by one counterparty);
  - considerable investing in instruments of the same type and instruments which value depends on changes in common factors

  please see also the section Concentration Risk Management Procedure.

Residual risk is a risk occurring due to the fact that the risk mitigation methods used by the Bank (institution) may not give the expected effect in connection with implementation in relation to the collateral received, e.g. legal risk, liquidity risk.*For a separate group of instruments*

- Counterparty risk in financial markets transactions[60] is a risk related to the counterparty's unwillingness or inability to completely perform their obligations under the transaction in due time. Counterparty risk is a two-side credit risk of forward transactions [61]with values under exposure which may change with time as fundamental market factors or underlying asset prices change.

[60] The approaches to managing the counterparty risk in financial markets transactions are specified in the section Procedure for Managing the Market Risk in the Trading Book and the Counterparty Risk in Financial Markets Transactions.

[61] Thus, counterparty risk of financial markets transactions does not include credit risk per issuers for investments in securities/third parties for credit derivative financial instruments (i.e., it includes part of the credit risk associated with financial markets transactions).

Among transactions that could result in realization of credit risks (credit risk sources) are the following ones:

- granting of loans (including loan facilities and overdrafts);
- provision of bank guarantees/ counter-guarantees/ sureties;
- transactions on purchase of bills of exchange;
- operations under financing transactions against assignment of a money claim (factoring);
- purchase of obligations under transactions of assignment of rights (claims);
- purchase of mortgage obligations in the secondarymarket;
- transactions on payment of letters of credit (in terms of unsecured export and import letters of credit);
- operations under financial lease transactions;
- obligations on which receivables arise (for those Group Members and types of receivables for which the credit risk of receivables has been recognized as substantial under the procedure for identifying and assessing materiality of the Group's risks (Section 6.1.1));
- provision of interbank loans (subject to the specifics /33/);
- transactions on purchase of bonds, and also other invested funds, including claims for receipt (return) of debt securities, stocks and bills of exchange provided under a loan agreement (subject to the specifics /33/);
- effecting transactions on sale (purchase) of financial assets with a deferred payment (delivery of financial assets) (subject to the specifics /33/);
- transactions on acquisition of financial assets with an obligation of reverse disposal (subject to the specifics /33/);
- effecting credit derivative transactions (subject to the specifics /33/);
- other investing transactions of the Group Members;
- other (not explicitly indicated above) transactions in the financial markets.

*Division of Functions and Powers*

Any credit risks of the entire Group and of the Bank are managed by LIC. The credit risks aremanaged, among others, by authorized collegial working bodies as part of transactions subject to the credit risk, in accordance with the powers delegated by the Loans and Investments Committee.

Responsibility to manage the credit risk is assigned by business segment.

The business units responsible for risk are as follows:

- in terms of the Group's credit risks (top-level group requirements) - the Integrated Risk Management Department;
- in terms of credit risks of customers of the Corporate and Investment Block and customers being financial institutions: the Corporate and Investment Risks Division;
- in terms of credit risks of customers of the Retail Block: the Retail Risks Division;

- in terms of credit risks of customers of the Sberbank International Block: the International Business and Ecosystem Risks Division;

- in terms of credit risks of customers of the Wealth Management Block: the Center for Wealth Risks Management.

The 1st and 2nd lines of defense in terms of credit risk management are defined as follows:

1. Performance of the functions related to risk taking by business units as those of the 1st line of defense[62]:

In the Bank:

- in terms of credit risks for customers of the Corporate and Investment Business, Retail, Sberbank International and Wealth Management Blocks: by business units of the respective block;

In the Group Member:

- in terms of credit risks for customers of the Group Member: by respective business units of the Group Member.

2. The functions of the 2nd line of defense are performed by the business units of the Risks Block[63], which assure credit risk management in business segments of their responsibility. The functions of the 2nd line of defense in the Group Members are performed by a respective business unit of the Group Member, which is responsible for risk management.

*Risk Assessment*

To assess credit risks, the Group uses the following assessment instruments (risk metrics):

- economic capital (ECap) is the capital amount required to cover unexpected losses on a given time horizon with an established level of confidence probability, which is determined, inter alia, on the basis of target rating;

- risk segment is an element of classification of credit claims by the degree of uniformity for the purpose of credit risk components assessment;

- probability of default (PD) is the value of probability of default of a borrower/ credit claim over the horizon of 1 year after the assessment (expressed as a percentage);

- exposure at default (EAD) is the amount of credit claims provided by the Bank to a borrower and outstanding as of the time of the borrower's default, commission fees and interest accrued but not received as of the time of the borrower's default, as well as contractual fines and penalties accrued but not received as of the time of the borrower's default; i.e. the amount that the Group/ the Bank/ the Group Member is exposed to as of the time of the borrower's default, if the borrower goes into default within 1 year after the assessment;

- loss given default (LGD) is the level of loss under a credit claim of a borrower in case the borrower goes into default within 1 year after the assessment (expressed as a percentage);

- expected loss (EL) is the indicator of expected loss within 1 year after the assessment;

[62] Corresponds to the basic rule; in some cases related to the specifics of generation of management statements as stated in other OADs/IRDs of the Bank, the correlation of business units and customer categories may differ.
[63] It is defined as a result of the annual procedure aimed at identifying and assessing the materiality of risks for the Group.

- increase of non-performing loans (NPL90+) share shows the ratio of loan liabilities that moved to category NPL90+ within 1 year to the average portfolio volume for a year;
- risk-weighted assets (RWA) are used to calculate the equity (capital) adequacy;
- credit risk coverage rate is residual credit loss provisions to the credit portfolio;
- cost of credit risk (CCR) means expected losses in case of realization of the credit risk and is used in credit pricing;
- risk concentration ratios of the Bank and the Group (RCRBG);
- and also other metrics specified in more detail in /33/.

*Risk Management Approaches*

To limit credit risks, the Group applies the following instruments:

- risk appetite;
- other limits of different levels and structure, including but not limited to:
  - limits for the Bank, other Group Members, and their structural units performing the functions on acceptance of credit risks based on the risk appetite set for the Group;
  - limits on the volume of transactions conducted with one counterparty or group of counterparties connected by certain features, according to the ownership ratio and the volume of transactions able to result in realization of credit risks, or with counterparties from a particular economic sector (portfolio level).
- provisioning of credit operations;
- security for providing credit products;
- stress testing.

The residual risk management system is an integral part of the credit risk management system, based on the general principles of credit risk management and aimed at determining and maintaining an acceptable residual risk.

The credit risk management process is specified in Sberbank Group's Credit Risk Management Policy No. 1303 as amended.

In terms of transactions in financial markets, credit risk management is carried out within the framework of the system for managing market and credit risks for transactions in financial markets (see the section "Procedure for managing market and credit risks for transactions in financial markets").

**Country Risk Management Procedure**

*Definition*

Country risk is a risk of losses related to inability or unwillingness of counterparties:

- that are residents of a foreign country (including sovereigns);
- that have assets in a foreign country;

- that bear the ultimate risk in a foreign country (i.e. if residents of a foreign country are related to formation of the sources of repayment of the counterparty obligations[64])

fulfill its obligations as a result of economic, political, social changes in a foreign country, or as a result of the fact that the currency of a foreign country may not be available to the counterparty due to the specifics of local and/or national legislation (regardless of the financial position of the counterparty itself).

*Division of Functions and Powers*

The country risk management function uses centralized and decentralized approaches at the Group level. The country risk of the Bank and of the entire Group is managed by LIC.

The Corporate and Investment Risks Devisionis a business unit responsible for country risk management in the Group. Responsibility to manage the country risk is assigned by business unit. The business units of the Bank/ the Group Members perform the functions of the 1st line of defense, including:

- identification and initial assessment of the country risk in a transaction (a group of identical transactions with a single counterparty or a counterparty);
- initial control of the compliance of the country risk accepted on a transaction with preset country risk limit.

The functions of the 2nd line of defense are performed by the Corporate and Investment Risks Devisionthat monitors the country risk accepted by the Group on a consolidated basis, assisted by the Center for Expert Review of Credit Risks of Corporate Customers and by similar business units of the Group Members, which verify the country risk detection in any transactions made by business units.

*Risk Assessment*

Economic capital indicator determines the Group capital value[65] needed to cover the potential losses associated with the realization of the country risk over the given time period (one year) and with established confidence level.

*Risk Management Approaches*

The Group's country risk is managed by the Bank. The Group Members, excluding the Bank, perform the operations subject to country risk within the requirements and restrictions established by the Bank, and also the requirements of local regulators in the countries of operation of the Group Members. The primary purpose of country risk management for the Group Members is compliance with the requirements and restrictions imposed by the Bank.

The Group's country risk management system ensures identification of country risks for all transactions of the Bank and of the Group Members influencing the Group's country risk level. The procedures for assessing the level of country risk and deciding on its admissibility by transaction exposed to country risk are included in decision-making processes on whether it is possible to perform such transactions.

[64] Customers, suppliers, investors, and other persons who influence the formation of the counterparty revenue are residents of a foreign country.

[65] For specific members of the Group, the country risk is accounted for in the assessment of economic capital for credit risk.

The key tools of country risk management of the Group are as follows: the system of country risk limits and the country risk reporting system.

The country risk management process is specified in Sberbank Group's Country Risk Management Policy No. 3206 as amended.

**Liquidity Risk Management Procedure**

*Definition*

Liquidity risk is a risk reflecting the inability to finance activities, i.e. to ensure the growth of assets and/or perform obligations as they become due, or the violation of regulators' requirements relating to liquidity risk.

There are risk components, which are identified:

- Physical liquidity risk is the risk of default by the Bank/Group Member on its liabilities to customers or counterparties in any currency or precious metal because of a shortage of cash or noncash funds (inability to make a payment, disburse a loan, etc.).

- Regulatory liquidity risk is the risk of non-compliance with the mandatory liquidity ratios of the Bank of Russia[66], as well as mandatory liquidity ratios established by local regulators in the countries of the Group Members' operation.

- Structural liquidity risk is a risk of a significant deterioration of physical or regulatory liquidity due to an imbalance in the asset and liability structure, including a strong dependence of the Bank's/ the Group Member's liability base on one or several customers or funding sources in a certain currency or with a certain maturity term, or, if necessary, on other parameters (such as, economy sector, geographical zone, type of instrument, etc.); please see also the Concentration Risk Management Procedure section.

*Division of Functions and Powers*

The Treasury is a business unit responsible for the liquidity risk. The liquidity risk of the entire Group is managed by ALCO. The functions of the 1st line of defense are performed by the Treasury, those of the 2nd line are performed by the Integrated Risk Management Department. The Integrated Risk Management Department distributes and controls implementation of the group standards of liquidity risk management as part of the functions of the 2nd line of defense at the level of the Group Members. The liquidity risk is managed on a centralized basis for the entire Group and for the Bank by the Treasury, and for the Group Members it is by a business unit of each Group Member that performs the functions of the 1st line of defense[67].

*Risk Assessment*

The liquidity risk is assessed on an aggregated basis for all operations of the Bank/ the Group Member/ the Group as a whole. For this purpose, liquidity risk for all operations in the banking book[68] is consolidated in an arbitrary unit, which is the Domestic Bank in the framework of the system of

[66] The mandatory liquidity ratios established by the Bank of Russia are the ratios N2, N3, N4, N26, N28 and other liquidity ratios, if those are included as binding upon the Bank/ the Group Member.
[67] For specific members of the Group, the liquidity risk management function may be performed by the Bank's Treasury on the basis of a service level agreement concluded between the Bank and the Group Member.
[68] For the Group Members: if applicable.

internal fund transfer pricing. Business units shall be isolated from liquidity risk exposure, and the cost of liquidity risk management is incorporated into the funding cost.

For specific members of the Group (non-credit or financial institutions), the liquidity risk management function (in terms of the 1st line of defense) may be performed by the Bank's Treasury on the basis of a service level agreement concluded between the Bank and the Group Member. For such organizations, the Bank's Treasury shall coordinate any actions of the Group Member related to liquidity risk management (integrated members of the Group). The decision to integrate the liquidity risk management function in the context of the Group Members in terms of the 1st line of defense shall be made by the Director of the Bank's Treasury. The functions of the 2nd and 3rd lines of defense as concerns the liquidity risk may be left unintegrated.

Liquidity risk is assessed by calculating liquidity risk metrics and determining the degree of their correspondence to the established limits, warning indicators and other restrictions.

*Risk Management Approaches*

The liquidity risk in the Group is managed by establishing the risk management procedures to be applied on an ongoing basis. No capital requirements are imposed for liquidity risk.

The key tool of liquidity risk containment is the system of limits and warning indicators of liquidity risk metrics. To ensure an acceptable liquidity risk level, the Group has a limit hierarchy in place, where the observance of lower-level limits ensures the compliance with upper-level limits.

The liquidity risk management system provides for various management tools depending on business environment: those available in a business-as-usual mode and those available in stress conditions. The liquidity management strategy shall be based both on management of assets (accumulation of liquid assets) and management of liabilities (attraction of funds in the amount sufficient to cover the expected demand for liquidity) with due regard to all established liquidity risk limits and containments. The planning of the balance sheet structure shall be carried out so as to ensure the compliance with regulatory requirements in terms of liquidity risk and established liquidity risk limits and containments. Operational management of liquidity risk is performed using procedures for forecasting liquidity risk metrics.

In terms of financial markets transactions, during the liquidity risk management one shall also apply the provisions of the section Procedure for Management of Credit and Financial Market Risks, which are relevant to the market risk and consistent with this section.

To reduce the risk, measures aimed at raising liquidity may be taken, as well as measures aimed at limitation of active operations, including price and non-price measures (administrative sanctions). The list of measures to reduce liquidity risk, the organization of liquidity risk management process, the functions and powers of the process participants are described in specific regulatory documents of the Bank and the Group Members.

The liquidity risk management process is specified in Sberbank Group's Liquidity Risk Management Policy No. 826 as amended.

**Management Procedure for Market and Credit Risks in Financial Markets Transactions**

*Definition*

The market risk in the trading book is a risk of incurring losses or profit decrease due to unfavorable fluctuation of the market value of financial instruments, prices of goods, exchange rates of foreign currencies and precious metals.

Credit risk - see the section “Credit Risk Management Procedure”. In terms of transactions in financial markets, credit risk in general (and its identified subspecies, including counterparty risk for transactions in financial markets) is managed within the framework of the system for managing market and credit risks of transactions in financial markets.

Within the framework of the system for managing market and credit risks of transactions in financial markets, the principles of formation and structure of portfolios of transactions in the financial markets, both in the trading and banking books, for the Group as a whole and for the Bank are determined.

Among financial markets transactions that could result in realization of market and credit risks are the following ones:

- transactions with bonds;
- transactions with shares;
- derivative transactions and other financial markets transactions subject to presettlement risk;
- transactions on provision of interbank loans, trade finance, and other loan products, as well as transactions subject to settlement risk.

*Division of Functions and Powers*

The Corporate and Investment Risks Divisionis a business unit responsible for these risks. Subdivisions responsible for credit risk (except for customers-financial institutions) are defined in the section “Procedure for managing credit risk”.

The management of the market risk of the trading book, the credit risk of clients-financial institutions, as well as the approval of the architecture and descriptions of portfolios of transactions in the financial markets for the trading and banking books for the Group as a whole and for the Bank is carried out by the MRC. Credit risk management (except for clients-financial institutions) is carried out by LICS.

1. The functions of the 1st line of defense are performed:

In the Bank: by Treasury, and business units;

In the Group Member: by a business unit of the Group Member (structural unit of the Group Member entitled to make decisions on performing operations/transactions with contractors/customers exposed to risks);

2. The functions of the 2nd line of defense are performed:

In the Bank: by the Corporate and Investment RisksDivision;

In the Group Member: by a respective business unit of the Group Member, which is responsible for risk management.

*Risk Assessment*

To assess and reduce the market risk in the trading book and the creditrisk in financial markets transactions, the Group applies the following assessment instruments (risk metrics):

1. For the market risk:
   - Dedicated economic capital
   - Value-at-risk (VaR)
   - Losses due to a sharp negative change of market factors (stress test)
   - Restrictions on deterioration of the financial result (stop-loss);
2. For credit risks:
   - Probability of default (PD) for a counterparty and the counterparty's internal rating
   - Loss given default of a counterparty (LGD)
   - Exposure at default (EAD)
   - Expected losses (EL)
   - Credit Valuation Adjustment (CVA).

*Risk Management Approaches*

The market risk in the trading book and the counterparty risk in financial markets transactions are managed through unified common procedures of market and credit risk management and control.

When establishing and reviewing the limits of the market risk in the trading book of the Group, the following indicators are taken into account:

- risk appetite, including the distributed one (on the level of a business unit performing the financial markets transactions);
- dedicated economic capital;
- risk factors substantial for a portfolio (group of portfolios) subject to limitation;
- transformation of economic capital into risk factor values;
- macroeconomic forecasts;
- previous and planned profitability indicators;
- regulators' requirements.

When the limits of the market risk in the trading book are established, sublimits for portfolios of financial markets transactions may be set which are linked to a specific Group Member; it is connected to increased control of market risk limits and containments at the integration of market risk management systems implemented by the Group Members.

The creditrisk in financial markets transactions is managed within the credit risk limit systems that are uniform for the entire Group and include country risk limits (CRLs), single name limit (SNL), and sublimits on the total of transactions.

The system of the limits of the market risk in the trading book and the creditrisk in financial markets transactions has a hierarchical structure where the hierarchy level of a specific limit defines authorized individuals whose responsibility is to adopt the limit values and who are notified in accordance with formalized escalation procedures provided for the violation of the limit.

All the Group Members have implemented the basic process of controlling the market risk in the trading book and the credit risk in financial markets transactions (depending on the hierarchy level of the total of transactions).

The control process of the market risk in the trading book includes, among others, control of the market risk limits and containments, escalation of violations of the market risk limits and containments, price control at revaluation of financial instruments, control over compliance of transactions with the arm's length principle.

The monitoring process for the credit risk in financial markets transactions, includes, among others, the processes of preliminary, current and subsequent control of credit risk limits, timely notification and escalation of violations of credit risk limits and containments, the process of assignment, monitoring and regular reconsideration of internal credit rating, and also the collateral management process.

The management process of the market risk in the trading book and the credit risk in financial markets transactions is specified in Sberbank Group's Management Policy for Market and Credit Risks in Financial Markets Transactions No. 2625 as amended.

**Procedure for Management of Interest Rate and Currency Risks in the Banking Book (hereinafter IRCRBB)**

*Definition*

The banking book interest rate risk is the risk of losses, decrease in profit, capital or capital adequacy due to an adverse change in interest rates of financial instruments in the banking book and/or market interest rates influencing the value of the banking book financial instruments.

Currency risk in the banking book is a risk of financial losses, decrease in capital or capital adequacy as a result of changes in foreign exchange rates or precious metal prices in the banking book positions.

*Division of Functions and Powers*

The Treasury is a business unit responsible for the interest rate and currency risks in the banking book.

ALCO is a committee that manages IRCRBB. The functions of the 1st line of defense are performed by the Treasury, those of the 2nd line are performed by the Integrated Risk Management Department. The Integrated Risk Management Department distributes and controls implementation of the group standards of IRCRBB management as part of the functions of the 2nd line of defense at the level of the Group Members. The Bank's Treasury is a business unit responsible for the risk on the level of the Group as a whole and of the Bank. The Group Members develop the IRCRBB system individually in compliance with the principles, requirements, approaches and standards defined by the Bank for Group Members and the Group as a whole.

*Risk Assessment*

IRCRBB shall be assessed by calculating the values of IRCRBB metrics and economic capital with respect to IRCRBB. IRCRBB metrics shall be calculated based on accounting data and management accounts of the Bank and Group Members.

*Risk Management Approaches*

A multi-level system of IRCRBB restrictions is used within the Group which includes risk appetite (RA) limits in respect to IRCRBB, limits on IRCRBB aggregated risk metrics not included in the risk appetite and IRCRBB position limits.

Management of IRCRBB level is ensured through management of interest rate and foreign exchange positions of the banking book as part of management of assets and liabilities of the Bank and the Group Members.

Positions of the banking book exposed to IRCRBB shall be consolidated in an arbitrary unit which is the Domestic Bank in the framework of the system of internal fund transfer pricing (FTP systems). Business units that conduct banking operations and conclude deals shall be isolated from IRCRBB exposure by means of paid redistribution of resources, and the cost of IRCRBB management is taken into account in the approaches to defining transfer incomes/expenses of business units.

Management of consolidated interest rate and foreign exchange positions includes: defining target positions, planning of assets and liabilities structure to reach target positions (among others, as part of business planning), regular calculation, monitoring and forecast of IRCRBB metrics values, assessing deviation of actual and forecasted values of IRCRBB metrics from their target values, as well as their compliance with the established limits, development and implementation of corrective measures to reduce IRCRBB and to reach target position values, conducting operations of position adjustment to provide observance of the established limits.

To reduce the level of IRCRBB, both financial markets transactions may be used (e.g. derivative transactions) and balance sheet management measures (e.g. modifying banking product details or using instruments of internal fund transfer pricing system).

In terms of financial markets transactions, during the IRCRBB management one shall also apply the provisions of the section Procedure for Management of Credit and Financial Market Risks, which are relevant to the market risk and consistent with this section.

The list of measures to reduce IRCRBB, the IRCRBB management process, the functions and powers of the process participants are specified in Sberbank Group's Management Policy for Interest Rate and Currency Risks in the Banking Book No. 2991 as amended, and in other regulatory documents of the Bank and Group Members.

**Management Procedure for the Market Credit Spread Risk in the Banking Book (hereinafter CSRBB)**

*Definition*

Market Credit Spread Risk of the Banking Book is a risk of losses or decrease in capital as a result of a decrease in market prices of securities in the banking book as a result of adverse changes in market credit spreads, except for investments being an equivalent of lending. For the purposes of this definition, investments being an equivalent of lending mean those in debt securities bought for holding

to obtain contractual cash flows and involving only repayment of principal debt and interest over the period of funds use[69].

*Division of Functions and Powers*

The Integrated Risk Management Department is a business unit responsible for the market credit spread risk of securities of the banking book.

The Bank shall ensure the division of functions related to CSRBB taking and CSRBB management. CSRBB of the Group as a whole and of the Bank is managed by ALMC.

The functions of the 1st line of defense on CSRBB identification and management within the set containments are performed:

- in the Bank: by Bank's Treasury;
- in the Group Members: by a business unit of the Group Member, which is responsible for management of the banking book portfolios sensitive to CSRBB;
- for the Group as a whole: there is a decentralized approach that implies the CSRBB management within the limits set at the group and local levels.

The functions of the 2nd line of defense on independent assessment and control of CSRBB are performed:

- in the Bank: the Integrated Risk Management Department;
- in the Group Members: by the risks unit of the Group Member;
- for the entire Group: the Integrated Risk Management Department.

*Risk Assessment*

To assess CSRBB of the Group, the metric Value-at-Risk (VaR)[70] is used, which is an estimate of the maximum loss in the fair value of debt securities as a result of changes in market credit spreads over a given period of time with a given probability (confidence level). To assess VaR for RMCSBB, the Monte Carlo method is used.

The corresponding value of VaR is used as economic capital for RMCSBB.

*Risk Management Approaches*

The main procedures for CSRBB management are as follows:

- CSRBB identification and assessment, including assessment of economic capital required to cover CSRBB;
- CSRBB limitation (establishing the system of limits);
- stress testing of CSRBB;
- control of CSRBB and of compliance with the set limits;

[69] Attributed to the 'Hold' business model, where the contractual cash flow characteristics (SPPI) test was passed.
[70] The Group Members may use a simplified approach in consultation with the risk-responsible business unit.

- CSRBB management, including development and implementation of the measures required to comply with the set limits of CSRBB;
- generation of reports on CSRBB;
- validation of models used for quantitative assessment of CSRBB;
- assessment of quality and efficiency (internal audit) of the CSRBB management system.

In terms of financial markets transactions, during the CSRBB management one shall also apply the provisions of the section Procedure for Management of Credit and Financial Market Risks, which are relevant to the market risk and consistent with this section.

The CSRBB management process is specified in Sberbank Group's Management Policy for the Market Credit Spread Risk in the Banking Book No. 4752 as amended.

**Operational Risk Management Procedure**

*Definition*

Operational risk is a risk of incurring direct and indirect losses as a result of inadequate or improper internal processes of credit organization, actions of employees or other individuals, failures or shortcomings of information, technological or other systems, as well as external events.

In order to unify the operational risk management in accordance with /36/, the Bank identifies the following types of operational risk, which management procedures are performed by special business units assisted by a business unit responsible for operational risk management: cybersecurity risk (in the terms of the Bank of Russia, information security risk); technology risk, including risk of failures and (or) malfunction of information systems; legal risk; risk of errors in project management; risk of errors in management processes; regulatory risk and compliance risk (in the terms of the Bank of Russia, risk of errors in the internal control processes); behavior risk (in the terms of the Bank of Russia, risk of lost funds of customers, counterparties, employees, or third parties (not compensated by a credit institution)); model risk; risk of errors in the staff management process; operational risk of the payment system.

The procedures for managing the risk of errors in project management or staff management process, and the operational risk of the payment system, are carried out as part of the overall operational risk management system and do not require any individual management procedures.

Operational risk includes the following types of events:

- Intentional acts by third parties (external fraud);
- Intentional acts by employees (internal fraud);
- Violations of HR policy and occupational safety;
- Violations of customer and counterparty rights;
- Damage to physical assets;
- Systems and equipment failures and malfunctions;
- Failure in organization, execution and management of processes.

*Division of Functions and Powers*

The Integrated Risk Management Department is a business unit responsible for the operational risk.

The operational risk of the Group/ Bank is managed by GRC.

1. The functions of the 1st line of defense are performed by all business units of the Bank/ the Group Member, however, the operational risk is managed by them in inextricable connection with execution of their main functions.

The heads of structural units are responsible for operational risk management within their business units based on supervision of the activities of employees, Identification and primary assessment of the risks arising from performing operations and concluding transactions, including when launching new products and/or entering into new markets, for the organization of investigation of operational risk incident causes and circumstances, for development and implementation of the measures aimed at reducing the operational risk, for timely assignment of risk coordinators for their business units in accordance with the procedure established in the Group Member, as well as for updating the lists of risk coordinators.

All the employees of the Bank/ the Group Member are responsible for timely informing about operational risk incidents, as well as for assistance to the investigation of causes and circumstances of operational risk incidents.

2. The functions of the 2nd line of defense are performed by the Risks Block: development of the operational risk management methodology, establishment of risk containments for the 1st line of defense, assessment of operational risks independent of the 1st line, provision of the expertise within own competences in identification of the risks arising when launching new products and/or entering into new markets, materiality assessment of operational risks, control over compliance with the regulatory requirements for operational risk, development of risk culture, etc.

3. The functions of the 3rd line of defense are performed by the Internal Audit Division in terms of independent assessment of compliance of the risk management system with internal and external requirements.

*Risk Assessment*

To get an adequate assessment and forecast of operational risk levels based on the approved classification of risk events, the Bank/ the Group Member creates an event base of realized operational risks including the detailed information about the date of a risk event realization, its type, sources, causes, the duration of risk factors impact, the amount of direct and/or indirect losses, frequency of repetitions of a specific risk event, etc.

The Bank uses the results of the procedure for identifying operational risk and maintaining the event base to perform the procedures for quantitative and qualitative assessments of the operational risk.

*Risk Management Approaches*

The operational risk management process contains the following procedures:

1. Operational risk identification, including the following methods:

   - analysis of the event base;

- annual self-assessment of the operational risk and controlling forms (methods) for its reduction, made by the Bank's business units and based on formalized questionnaires;

- trend analysis of quantitative indicators aimed at measuring and monitoring the operational risk at a point in time (KRIs);

- interviews with employees to discuss operational risks;

- analysis of inspection certificates, judicial acts, and acts of executive authorities or the Bank of Russia for any facts related to operational risk realization, or other external and internal sources of information.

2. Collection and registration of information on internal events of operational risk and losses from its realization, including:

- automated identification of information from information systems;

- manual identification and collection of information using an expert opinion;

- input of information about events, classification and registration in the event base.

- Determination of losses and compensation for losses from realization of operational risk events, including:

- procedures and methods for determining direct losses;

- procedures and methods for determining indirect losses, including consequentialor quality losses;

- procedures and methods for determining potential losses;

- procedures and methods for determining the cost of compensation.

3. Quantitative assessment of operational risk, including the following methods:

- aggregate assessment of the operational risk for the entire Bank and its business units, and also by operational risk event type or business area, including in terms of their constituent processes;

- assessment of the capital allocated by the Bank within ICAAP to cover losses from realization of operational risk events for the entire Bank or in terms of business areas, including their constituent processes;

- assessment of expected losses from operational risk realization in terms of business areas, including their constituent processes, for which the statistics of operational risk events are observed, in order to cover these losses through the pricing of services and tariffs.

4. Qualitative assessment of operational risk, made for identified operational risks in addition to the quantitative assessment, including the following methods:

- operational risk self-assessment;

- scenario analysis of operational risks;

- professional (expert) assessment made by the Bank employees and (or) external experts assigned for this procedure, subject to the rules for engaging external experts as established by the Bank.

5. Selection and application of the operational risk response method according to the results of the qualitative assessment of operational risk, including the following methods:

- risk avoidance meaning the Bank's refusal to provide the respective type of services and transactions due to high operational risk;

- risk transfer meaning insurance or transfer of risk to another party, such as the counterparty and (or) the customer;

- risk acceptance meaning the Bank's readiness to accept possible losses within the established loss limit, according to the limit compliance monitoring procedure;

- taking the measures aimed at reducing any negative impact of operational risk on the quality of processes, and also the amount of losses from operational risk realization, including development by the Bank of controlling forms (methods), including:

    - updates to processes;
    - establishment of extra forms (methods) of control;
    - training of employees, including process participants;
    - application of automated solutions;
    - other measures aimed at reducing the negative impact of operational risk.

6. Operational risk monitoring, including the following methods:

- generation and monitoring of KRIs;

- statistical analysis of operational risk events, including the reasons for occurrence of operational risk events and losses from their realization;

- implementation control of the measures aimed at improving the quality of the operational risk management system and reducing any negative impact of operational risk, including those aimed at preventing (reducing the probability of) operational risk events, and those aimed at limiting the amount of losses from realization of operational risk events;

- implementation control of the measures aimed at reducing the negative impact of operational risk;

- monitoring of compliance with the selected methods of responding to operational risks;

- monitoring of information flows as part of operational risk realization, coming from the Bank's business units and competency centers, sole and collegial management bodies of the Bank.

To effectively manage operational risks, the Bank/ the Group Member shall:

- maintain its capital adequacy at the level satisfying the regulator requirements in case of operational risk;

- resort to insurance procedures in respect to the risk of possible losses due to extraordinary operational risks which cannot be managed by the Group Member and are out of its immediate control, or due to operational risks able to lead to the amount of losses which would be disastrous or critical for the Bank/ the Group Member.

Key methods of operational risk management:

- division of powers and subordination hierarchy system;

- identification, determining the level of materiality of potential operational risks proper to each business process as a whole and to its specific stages (operations), development of additional control measures and procedures aimed at preventing (minimizing) identified risks at the stage of development and approval of internal regulatory documents;

- collegiality of decision making concerning operations exposed to risk. All the operations (transactions) exposed to risk are based on the resolutions of collegial bodies of the Bank/ the Group Member or executives of the Bank/ the Group Member within the established authority, in compliance with the internal regulatory documents regulating such transactions;

- system of limits and restrictions;

- procedure of development, agreement, legal expert review and approval of internal regulatory documents;

- system of authorizing operations;

- management of IT services based on applying methodology of IT service management;

- implementation of the extra control principle when making accounting operations under the specific card of accounts or entering data into accounting and operating systems;

- availability of an effective system of internal control, etc.

The operational risk management process is specified in Sberbank's Operational Risk Management Policy No. 1302 as amended.

**Concentration Risk Management Procedure**

*Definition*

For the Bank and the Group Members being credit institutions[71], the annual identification procedure provides for the concentration risk to be recognized as substantial, accounted for and managed as part of credit and liquidity risks. It arises from the credit institution's exposure to major credit risks which, if realized, may result in considerable losses that might damage the credit institution's solvency and ability to continue as a going concern.

The concentration risk occurrence is taken into account in the Bank as part of the management procedures of other substantial risks, namely, in terms of credit risk and liquidity risk (structural liquidity risk). As part of other substantial risks (market risk, operational risk), the concentration risk is not emphasized, but it is assessed and controlled as part of these risks.

Concentration risk (in terms of credit risk) is the risk associated with:

- providing large loans to an individual borrower or a group of related borrowers;
- the concentration of debt in individual sectors of the economy, segments, portfolios, or geographic regions, etc .;
- implementation of measures to reduce credit risk (use of identical types of collateral, independent guarantees provided by one counterparty);

[71] For the Group Members that are not credit institutions, the concentration risk materiality is estimated as a result of the annual procedure aimed at identifying and assessing the materiality of risks of the Group.

- a significant amount of investments in instruments of the same type and instruments, the cost of which depends on changes in general factors.

Structural liquidity risk (concentration risk in terms of liquidity risk) is the risk of a significant deterioration in physical or regulatory liquidity due to imbalances in the structure of assets and liabilities, including the high dependence of the Bank's / Group member's liabilities on:

- one / several clients;
- one / several funding sources in a certain currency or for a certain period;
- if necessary, other parameters (for example, the economic sector, geographic area, type of instrument, and others).

Depending on whether the concentration risk is qualified as a substantial one, the Group considers its occurrence, among others, at the following key levels:

- at the level of a particular counterparty (group of related counterparties);
- at the portfolio level:
  - at the level of industry concentration of business;
- at the level of the balance-sheet structure.

*Division of Functions and Powers*

The division of functions and responsibilities among the Bank's business units and the Group Members during the concentration risk management procedures, shall be made according to the 'three lines of defense' principle. The principle implies that the risk management functions shall be performed by three different business units which are independent from each other by organization, i.e. subordinate to different members of the Executive Board of the Bank. The assignment of responsibility for credit and liquidity risks by line of defense is specified in detail in the relevant sections of this Appendix.

Any credit risks of the entire Group and of the Bank are managed by LIC.

The structural liquidity risk as one of the liquidity risk components of the entire Group is managed by ALCO.

The concentration risk management principles are described in more detail in corresponding IRDs within the procedures for managing any substantial risk characterized by the concentration risk.

*Risk Assessment*

For the purposes of identification and measurement of concentration risk, the Bank shall establish a system of indicators enabling identification of concentration risk with respect to substantial risks, certain major counterparties (groups of related counterparties) and related persons, economy sectors and geographical areas.

The concentration risk in terms of credit and liquidity risks is assessed under the substantial risk management procedures by calculating the risk level indicators (risk metrics) established in the policies for managing respective risks, and also determining their compliance with the set limits, warning indicators, and other containments.

When assessing the concentration level for the credit risk, one shall also calculate the mandatory risk concentration ratios of the Bank and the Group (hereinafter RCRBG) (N6/PKC6.1, N7, N25, N21, N22).

*Risk Management Approaches*

In order to manage and monitor the level of concentration of the credit risk in terms of RCRBG, the system of limits and warning indicators has been implemented; in addition, forecasting and monitoring RCRBG and estimation the impact of any changes in the regulatory requirements on changes in the ratios of the Bank and the Group are carried out.2. In order to control the liquidity risk concentration, the Group has implemented the system of liquidity risk limits, which allows to ensure an acceptable liquidity risk level in the Bank and the Group consistent with the established risk appetite and other containments in order to ensure that the Bank and all Group Members are able to promptly and unconditionally fulfill any obligations to their customers and counterparties and that the Bank and the Group operate on a going concern basis.

3. In order to monitor the credit risk concentration in a single economic sector, one shall provide for the risk metrics and the system of limits on them. The concentration risk limits per industry are set under the behavioral scenario of each specific industry, adjusted for the current condition of risk metrics. The established limits and their utilization are recognized in the statements to be submitted to the Bank of Russia on a quarterly basis.

The credit risk management process, including management of concentration risk as part of credit risk, is specified in Sberbank Group's Credit Risk Management Policy No. 1303 as amended. The liquidity risk management process, including management of structural liquidity risk, is specified in Sberbank Group's Liquidity Risk Management Policy No. 826 as amended.

The concentration risk management procedures of the Group Members being credit institutions shall be determined based on the concentration risk management approaches established on the Group's level, and shall be agreed upon with the Bank.

**Model Risk Management Procedure**

*Definition*

Model risk is a risk of adverse effects arising from inaccuracies (errors) in the operation of models and/or incorrect application of models in the processes of the Bank/ the Group Member.

The main sources of model risk are errors or features of the input data used in model development and application, uncertain estimates and methodological errors in model development, and also incorrect usage of the model in the processes.

*Division of Functions and Powers*

The Validation Division is a business unit responsible for the model risk assessment.

The model risk management function is centralized on the Group's level. The model risk of the entire Group and of the Bank is managed by GRC.

Responsibility to manage the model risk is assigned by functional unit. The functions of the 1st line of defense are performed by model developers during the model development process, as well as model owners and users during model application. The functions of the 2nd line of defense are

performed by the Validation Division that validates the models and assesses the model risk, but does not take part in model development.

According to the model risk management, the Validation Division shall submit the regular reports on the model risk to the GRC meeting. GRC regularly reviews and analyzes the reports and up-to-date information on the model risk as provided by the Validation Division. If necessary, GRC gives instructions regarding any appropriate measures to adjust the model risk level.

*Risk Assessment*

The model risk is assessed both at the level of a single model and at the level of groups of models aggregated by various criteria. The model risk is assessed under any and all models of High or Medium Significance falling under Sberbank Group's Model Risk Management Policy No. 3194 as amended.

The following approaches to the model risk assessment are applied (for all models):

Qualitative assessment. The qualitative assessment of the model risk is based on verification of the model in accordance with approved validation methodologies, the result of which is assignment of qualitative assessments for models based on the traffic light principle.

Aggregate assessment. The total model risk is indicated as the share of red/yellow/green traffic lights in the model groups generated, among others, by assigning to any business blocks, SBs, SCs.

At the moment, there is no separate model for determining the capital needs of the Group to cover the model risk. In the future, the need for capital to cover the model risk will be estimated using quantitative methods and the model risk will be derived from the capital for coverage of other risks.

*Risk Management Approaches*

The aim of managing model risk is to limit a negative impact of the model risk on the Group Member's operations. In practice, this means developing and maintaining a set of measures aimed at reducing the probability of model risk and mitigating the possible consequences in the event of its realization.

Due to the fact that the model is an imperfect representation of real economic and social processes, if the management system is constructed correctly, the model risk can be reduced, but it cannot be completely eliminated.

To manage the level of model risk, the following main approaches are mostly used:

- improvement of the quality and completeness of documentation for models;
- improvement of data quality, availability and completeness;
- revision of models;
- revision of processes;
- revision of IT systems.

The model risk management process is specified in Sberbank Group's Model Risk Management Policy No. 3194 as amended.

**Technology Risk Management Procedure**

*Definition*

Technology risk means a risk of direct or indirect losses as a result of unavailability of IT systems, data quality and integrity violations, violations in the work of contractors and partners, and errors in the development and updating of IT systems.

There are four subcategories of the technology risk:

1. Risk of unavailability: any demonstration of AS unavailability, including the risk of reducing the AS operation efficiency;

2. Data integrity and timeliness risk: any demonstrated violation in completeness, accuracy, or timeliness of data both stored or in transit and processed in AS;

3. Risk of incorrect changes in AS: any functional shortcomings caused by errors in selection/development and implementation of AS changes, including incorrect architectural solutions and changes in the respective IT infrastructure;

4. Risk of lost service quality of an IT partner: any lost quality of service from the Group's IT partners, including intra-group outsourcing, and also due to economic sanctions.

*Division of Functions and Powers*

The Integrated Risk Management Department is a business unit responsible for the technology risk.

The technology risk of the Bank/Group is managed by GRC.

1. The functions of the 1st line of defense are performed by all business units of the Bank/ the Group Member, along with the supervising business units of the Technology Block. They are the technology risk owners in terms of ASs they are responsible for, and jointly and severally liable in case of technology risk realization in terms of ASs owned.

2. The functions of the 2nd line of defense are performed by the Risks Block along with the Technological Reliability Department of the Technology Block: development of the technology risk management methodology, establishment of risk containments for the business units performing the functions of the 1st line of defense, risk assessment independent of those business units, risk identification and materiality assessment, control over compliance with the regulatory requirements for the technology risk, development of risk culture, etc.

3. The functions of the 3rd line of defense are performed by the Internal Audit Division in terms of independent assessment of compliance of the risk management system with internal and external requirements.

*Risk Assessment*

The technology risk is subject to quantitative assessment, and its methodology depends on the technology risk subcategory. The risk assessment takes into account any potential damage to the Group in case of risk realization, including direct/indirect damage, impact on the profitability of the Bank customers, legal effects, and potential reputational damage. The probability is assessed for each subcategory of the risk.

Among the risk assessment tools are retrospective incidents for risk subcategories already realized, artificial intelligence (AI) models, and expert judgement.

*Risk Management Approaches*

The Group performs proactive identification of the technology risk. To this effect, the lists of standard negative scenarios have been developed to specify any potential impact of the technology risk on AS. The risk identification targets have been set, ensuring that over 90% of the Bank incidents is due to known and assessed risks.

For the technology risk, the acceptable risk ratios and limiting criteria have been determined when developing the business plans for business units to evolve ASs assigned.

The Group monthly monitors the technology risk. The Bank's Executive Board is notified of the current risk levels and violations of limits.

Any technology risk incidents in the Bank/ Group are registered, and in case of significant damage from the incident, it is communicated to the Bank's Executive Board. Root causes are identified for the incident and included in the risk assessment.

**Cybersecurity Risk Management Procedure**

*Definition*

Cybersecurity risk is a risk of information security threats, which are caused by shortcomings in information security processes, including technological and other activities, weaknesses in the application software, ASs and apps, as well as the inconsistency of these processes with the activities of an organization.

*Risk Management Approaches*

The cybersecurity risk management is aimed at determining and ensuring the cybersecurity risk level that is necessary for sustainable development of the Bank and the Group Members, and also at complying with requirements of regulators.

The cybersecurity risk is managed on an ongoing basis in the course of ordinary operations, development and introduction of new products or processes, and also strategic initiatives of the Bank in order to timely identify potential negative events due to implementation of the cybersecurity risk scenarios. The process includes identification, assessment, processing, monitoring and control of the cybersecurity risk, and also timely provision of complete and reliable information to the Sberbank Executives as may be required for making management decisions.

The losses from cybersecurity risk materializing is included when assessing the overall operational risk.

The cybersecurity risk management process is specified in Sberbank Group's Cybersecurity Risk Management Policy No. 4641 as amended.

*Division of Functions and Powers*

1. The functions of the 1st line of defense are performed by all business units of the Bank: identification of risks in the course of ordinary operations, initial risk assessment, etc.

2. The functions of the 2nd line of defense are performed:

    a. by the Cybersecurity Department: development of the methodology for managing and assessing cybersecurity risk, independent assessment of the risk level, monitoring of the current state of the cybersecurity risk management system, etc.;

    b. by the Risks Block: interaction with the Cybersecurity Department as part of the

integrated cybersecurity risk management processes, consideration of cybersecurity risk information when assessing the consolidated risk for internal and external reporting purposes, etc.

3. The functions of the 3rd line of defense are performed by the Internal Audit Division in terms of performance assessment of the cybersecurity risk management system, control over elimination of identified deficiencies, etc.

Any decisions on the cybersecurity risk are made as part of unified Decision-Making Procedure for Certain Risks as approved by the Bank.

The Group Members (except for the Bank) organize the cybersecurity risk management in accordance with the Group's requirements, and also provide the Cybersecurity Department with any necessary information to manage the aggregate cybersecurity risk of the Group.

*Risk Assessment*

To assess the cybersecurity risk, one shall estimate the risk factors identified (risk factors of damage, actual threats and breakers, existing vulnerabilities, and protection measures), subject to which the risk rating and the qualitative indicator are calculated.

The cybersecurity risk assessment is used while making organizational and technical decisions with regard to data protection methods, tools and mechanisms in the cybersecurity provision system, as well as while conducting risk management activities.

**Participation and Forced Support Risk Management Procedure**

*Definition*

Participation and Forced Support Risk is a risk of damages/losses due to adverse changes in their financial position/ market value of investments in equity securities that allow for controlling or significantly influencing the issuer/ charter capital of an organization[72], or due to forced financial support provided by a parent institution to organizations that are not taken into account when calculating the Group's capital adequacy ratio.

The main source of the participation risk is the transactions on investing in the Group Members.

*Division of Functions and Powers*

The functions of the 1st line of defense related to investing in the Group Members are performed by the Bank's business units supervising the Group Members in accordance with the executive document in effect in the Bank.

The functions of the 2nd line of defense: The Integrated Risk Management Department is a risk-responsible business unit in terms of any companies included in the regulatory consolidation perimeter, but not related to the ecosystem perimeter. It determines the general approaches to risk management and ensures the aggregation of results for considering the common issues at the relevant collegial bodies of the Bank. The International Business and Ecosystem Risks Division is a risk-responsible business unit in terms of any companies included in the ecosystem perimeter of the Group, but excluded from the regulatory consolidation perimeter.

[72] These investments are made according to the resolution of the Bank's management body/ Group Member's collegial body.

GRC is a collegial body to manage the risk.

*Risk Assessment*

The risk is assessed by calculating the use of established buffers to cover anticipated losses, and considered revaluation of investments within the regulatory consolidation perimeter in the Bank capital in accordance with /**Ошибка! Источник ссылки не найден.**/.

*Risk Management Approaches*

Risk management includes:

- identification and assessment of risk;
- risk limitation (formation of a system of limits);
- stress testing of the Bank's and the Group's exposure to risk;
- control of the risk level of compliance with the established limits;
- formation of risk reporting;
- validation of models used for stress testing and quantitative risk assessment;
- assessment of the quality and efficiency (internal audit) of the risk management system.

The risk management approaches are determined depending on the company type and entry into the consolidation perimeter according to the diagram below.

| | **Credit institutions** | **Financial companies** | | **Non-financial institutions** | |
|---|---|---|---|---|---|
| | *N20 Perimeter* | *N20 Perimeter* | *Other companies* | *N20 Perimeter* | *Other companies* |
| **Participation risk** | Deduction from the Bank’s capital | Deduction from the Bank’s capital | ICAAP buffer | Consideration of other risks through EC | ICAAP buffer |
| **Forced support risk** | Solvency buffer | Solvency buffer | ICAAP buffer | Solvency buffer | ICAAP buffer |

The Bank has developed the system of buffers that are created to cover losses from realization of risks of the Group Members.

The Solvency buffer is created as part of the business planning procedures for the Group Members included in the ICAAP perimeter, if the capital adequacy forecast turns out to be under the target according to the established risk appetite (yellow zone of the capital adequacy ratio), for the missing difference.

The ICAAP buffer is created to cover losses on the risks of investment depreciation and forced support of companies outside the ICAAP perimeter.

The investment depreciation amount is limited by the subsidiary equity adjusted for the depreciation probability (depending on the business area of the Group Member).

**Behavior Risk Management Procedure**

*Definition*

Behavior risk is a risk of the Bank/ the Group Member and their employees using unfair business practices that violate the business ethics principles and have a negative impact on the customers, including their financial interests or expectations formed by the Bank/ the Group Member, or on the market stability[73].

The main sources of Behavior risk are:

- Asymmetry of information. The Bank and the members of the Group have more information about the products / services provided than clients. Incomplete availability, insufficient disclosure of information about the features of products / services can lead to the formation of incorrect expectations among customers.

- Biases and heuristics. Biases and heuristics limit the client's ability to fully assess their own needs, long-term interests and adequately understand the offered products / services, therefore they have a significant impact on the financial decisions of clients.
- Low financial literacy of clients. Purchasing a product / service is a complex and not always clear process for the client. This also applies to the paperwork process, and misinterpretation of the terms of contracts, and misunderstanding of the process of providing financial services.
- Business priorities. The Bank's business models and development strategy can distinguish certain customer groups and thus potentially discriminate against others.
- Business culture and incentives. The incentive system can provoke the spread of unfair practices in the Bank or Group members, encouraging risky short-term business development plans or putting pressure on the sales process in order to promote specific products / services, regardless of the needs and requests of customers.

*Division of Functions and Powers*

The Integrated Risk Management Department of the Risks Block is a business unit responsible for the behavior risk in the Group.

The behavior risk events of the Group/ Bank are managed by GRC.

For the purposes of efficient behavior risk management and taking into account the need to prevent the conflict of interest between behavior risk acceptance, limitation and control, and also audit of the behavior risk management system, the organizational structure of the Bank/ the Group Member shall be formed with due regard to the necessity for allocation of roles and responsibilities among business units of the Bank/ the Group Member in accordance with the '3 lines of defense' principle:

1. 1st line of defense: identifying the behavior risk and implementing the measures to mitigate risks, selecting the risk response strategy and ensuring compliance with the containments and approaches established by the 2nd line of defense;

The functions of the 1st line of defense in behavior risk management under the '3 lines of defense' principle are performed by the Bank's/ Group Member's business units that affect the customers

[73] The risk does not involve management of such risks as cybersecurity risk, reputational risk, compliance risk, risk of changes to legislation, legal risk, tax risk, operational risk.

(including in design of customer paths, development of products/services, and also the processes of promotion, sale, after-sales service, and termination) or the markets where the Group operates.

2. 2nd line of defense: development of the operation methodology for the behavior risk management system, development of the behavior risk management measures, independent risk assessment, and control of compliance with established approaches and containments;

The functions of the 2nd line of defense are performed by the Risks Block.

3. 3rd line of defense: independent assessment of compliance of the behavior risk management system with internal and external requirements.

The functions of the 3rd line of defense are performed by the Internal Audit Service[74].

*Risk Assessment*

The Bank uses the results of the behavior risk Identification procedure to perform the procedures for quantitative and qualitative assessments of the operational risk.

The behavior risk estimate is formed cumulatively according to the following ratios:

- number and quality of complaints/ information about the Group frauds, as received from customers;
- direct losses/ losses of the Group from decreased customer confidence due to any frauds of the Bank/ the Group Members;
- measures of regulatory response to any frauds of the Bank/ the Group Members.

*Risk Management Approaches*

The behavior risk management is aimed at:

- determining and ensuring the target behavior risk required for sustainable development of the Bank/ the Group Member, including through reducing the behavior risk probability and mitigating potential effects in case of risk realization;
- adhering to the best international banking practices in behavior risk management, business ethics standards, and consumer protection standards.

The behavior risk management process in the Group consists of the following main stages:

- Behavior risk identification is determination of the reasons and prerequisites that have or may have a negative impact on the customers, including their financial interests or expectations formed by the Bank/ the Group Member, or on the market stability, and also consideration of all transactions subject to this risk;
- Behavior risk assessment is the analysis of information received at the risk identification stage, and determining the probability of events that may lead to losses, and also the amount of potential or incurred damage;

[74] For all Group Members that have the behavior risk recognized as material or substantial, the functions of the 3rd line of defense are performed by the Internal Audit Service, failing which a business unit is selected that can ensure the principle of independent performance of functions or an external audit is engaged.

- Decision-making on corrective measures for the risk means making a management decision with respect to the identified behavior risk and monitoring the progress of the approved measures for behavior risk mitigation and elimination of problem zones in processes;

- Monitoring and oversight of the behavior risk and losses means identification of events that contribute to changes in the degree of exposure of the Bank/ the Group Member to the behavior risk and its changes, and also monitoring of the dynamics of indicators characterizing the behavior risk in order to determine its trends.

The behavior risk management process is specified in Sberbank's Behavior Risk Management Policy No. 5507 as amended.