RESOLUTION OF THE BOARD
OF THE NATIONAL BANK
OF THE REPUBLIC OF BELARUS

29 October, 2012, No.550

On Approval of the Instruction on Arrangement of the Risk Management System

Including the amendments made by the Resolutions of the Board of the National Bank:
dated 01.10.2013, No. 567;
dated 13.08.2015, No. 482;
dated 10.06.2016, No. 311;
dated 29.06.2016, No. 361;
dated 22.01.2018, No. 25;
dated 27.04.2018, No. 196;
dated 26.06.2020, No. 214)

By virtue of the third paragraph in the fourth part of Article 34, the first part of Article 39 of the Banking Code of the Republic of Belarus, the Board of the National Bank of the Republic of Belarus hereby DECIDES:

1. To approve the enclosed Instruction on Arrangement of the Risk Management System (is attached).

2. This Resolution shall come into effect since 22 January, 2013.

The Chairperson of the Board N.A.Yermakova

APPROVED

Resolution of the Board
of the National Bank
of the Republic of Belarus

29.10.2012 No. 550

THE INSTRUCTION

on Arrangement of the Risk Management System
(including the amendments and additions made by the Resolution of the Board of the National Bank dated 26.06.2020, No.214)

CHAPTER 1
GENERAL PROVISIONS

1. This Instruction sets the requirements for the arrangement of the risk management system in banks, Development Bank of the Republic of Belarus JSC, non-bank financial institutions (hereinafter referred to as banks), banking groups and banking holding companies.

2. For the purposes of this Instruction, the following terms shall have the following meaning:

risk – under the conditions inherent to the banking activity, really existing possibility (likelihood) of sustaining losses by a bank, of bank's failure to obtain planned incomes and (or) liquidity worsening and (or) ensuing of other unfavorable consequences for a bank as a result of occurrence of various events related to the internal and (or) external factors in bank's activity;

risk management system – a combination of bank's organizational structure, powers and responsibilities of officials, local regulatory legal acts, defining the strategy, policy, techniques and procedures of risk management as well as the risk management process, with the purpose of reaching the bank's financial reliability;

inherent risk – a risk initially existing in the bank's activity due to the objective causes;

residual risk – an inherent risk after taking the measures to control and restrict (reduce) it;

risk profile – a combination of risk indices and other data describing the bank proneness to various types of risks, taking into consideration the bank's strategy and priorities with regard to the risks accepted;

risk tolerance – a level (an amount) of risk defined by a bank for itself as permissible (safe) for its financial reliability and long-term operation, in view of the strategy, nature, scopes and complexity of types of activity as well as the financial position;

propensity to risk (risk appetite) – a level (an amount) of risk such that a bank (bank's subdivisions) is (are) ready to accept in implementation of their activity for the purposes of profit-making or to achieve other goals;

management reporting – formalized and structured information (reporting) about the bank's activity submitted regularly, in accordance with the established procedure, to the bank's shareholders and (or) to its executive bodies or officials for making the necessary management decisions;

key risk indicators – the set of indices (parameters) used to monitor the major risk factors and to control the level of risks;

stress test (stress testing) – the assessment of possible effects for the bank's financial position resulting from a series of specified shocks (shocking situations), i.e. variations in risk factors corresponding to extraordinary but probable events.

3. The principal organization of a banking group or the principal organization of a banking holding company where this principal organization is a bank (except for Development Bank of the Republic of Belarus JSC) must arrange the risk management system in a banking group and (or) a banking holding company on the consolidated basis in such a way that it makes possible to receive the comparable information about the level of risks faced by the participants of a banking group and (or) a banking holding company; for this purpose, unified principles of risk management must be used, in view of the requirements established by this Instruction.

4. The assessment of the risk management system in a bank shall be carried out by the National Bank within the scope of implementation of the banking supervision, in view of a reasoned opinion. In accordance with the results of this assessment, the following decisions may be made by the National Bank:

the state registration of a bank established as a result of the reorganization and simultaneous issuance of a special permit (license) for carrying out banking activity to this bank;

the state registration of amendments and (or) additions made in the bank's Articles of Association (within the scope of the bank reorganization);

the issuance of (or the refusal to issue) the special permit (license) for banking activity implementation to the bank, making (or refusal to make) amendments and (or) additions to the schedule of banking transactions listed in the special permit (license) for banking activity implementation issued to the bank;

application of supervisory response measures.

CHAPTER 2
MAJOR TYPES OF BANKING RISKS AND CONDITIONS (SOURCES) FOR THEIR ORIGINATION

5. A bank must identify the major risks originating during its activity implementation, as well as their origination sources, and manage the risks inherent to it, taking their significance into consideration. The major types of

banking risks and their origination conditions (sources) are defined in Clauses 6-14 of this Instruction. A bank may, in its local regulatory legal acts, stipulate other definitions for major banking risks (however, these definitions must not contradict this Instruction in their essence), define more sources of their origination and define more risks inherent to its activity.

6. The credit risk is the risk of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of debtor's non-fulfillment, fulfillment not in due time or incomplete fulfillment of financial and other property obligations towards the bank in accordance with the provisions of a contract or with the legislation.

Credit risk becomes higher in transactions with debtors being the bank's insiders or interrelated persons.

Natural person's or legal entity's relation with a bank may result in non-observance or insufficiently full observance of the legislation or rules and procedures established by a bank for handling the applications for provision of credits and other assets, or those established for debtor's solvency assessment and for making the decisions with regard to the provision of assets; this, in turn, can result in credit risk growth.

Credit risk also arises in case of counteragent's failure to fulfill its obligations with regard to the transactions with the financial instruments that involve exchange of payments under financial instruments or delivery of a financial instrument against a payment and (or) a transaction for the purpose of risk hedging (the counteragent's credit risk).

7. The country risk is the risk of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of non-fulfillment by foreign counteragents (natural persons or legal entities) of their obligations due to economic, political or social changes or because the monetary obligation currency can be unavailable for a counteragent due to the specific factors of the legislation (irrespective of the counteragent's financial position).

Country risk shall be assessed in terms of the country of location of a debtor or its major counteragents and the risk of non-transfer of funds (the transfer risk) including such cases resulting from the activities of the government of debtor's country or the country of debtor's major counteragents (the chain reaction). Changes in political and economic situation in a country, application of sanctions from international organizations and separate countries can significantly affect the debtor's capability to fulfill its obligations towards the bank. The country risk is also associated with a foreign government's incapability or unwillingness to discharge its obligations.

8. The market risk is the risk of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of change of the value of balance items and off-balance items being the elements of the trading portfolio as well as the items denominated in foreign currency and the goods due to

variations of market prices for financial instruments and goods caused by variations of foreign currency exchange rates, market interest rates and other factors.

The market risk includes the trading portfolio interest risk, the stock market risk, the exchange risk and the commodity risk.

The trading portfolio interest risk is the possibility of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of change of the value of balance items and off-balance items being the elements of the trading portfolio, when this change is caused by variations of interest rates. Depending on the sources of origination, the following are the major types of the trading portfolio interest risk:

the risk of change of the value of items in the trading portfolio resulting from differences between the repayment (return) periods for balance assets, passives and off-balance claims and obligations with the fixed interest rates or from setting new rates for financial instruments with the floating interest rate;

the yield curve risk associated with possible variation of the slope and shape of a curve depicting the income acquisition uniformity (the yield curve) as a result of non-coincidence of repayment times for financial instruments in case of changes of their interest rates;

the basis risk resulting from insufficient correlation between interest rates for raised and placed financial instruments with similar repayment periods and interest rate revision characteristics;

the option risk resulting from possible refusal to fulfill obligations by one party in a transaction with standalone options or financial instruments with embedded options.

The stock market risk is the possibility of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of change of the value of equity instruments in the bank's trading portfolio.

The exchange risk is the possibility of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of change of the value of bank's balance items and off-balance items denominated in foreign currency due to variations of foreign currency exchange rates. Bank's items in precious metals, such as bank bullion bars, weighted bullion bars and coins reevaluated in accordance with the established accounting policy of a bank as far as accounting prices vary, are also prone to the exchange risk.

The commodity risk is the possibility of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of changes of values of goods.

9. The bank portfolio interest risk is the possibility of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of change of the value of bank's balance items and off-balance items not being the elements of the trading portfolio, when this change results from variations of

interest rates. The major types of the bank portfolio interest risk are the risk of change of the value of items in the bank portfolio, the yield curve risk, the basis risk and the option risk.

10. The liquidity risk is the possibility of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of incapability to provide fulfillment of bank's obligations in due time and in full. The liquidity risk arises as a result of imbalance between the bank's financial assets and financial obligations (including the imbalance resulting from one or several bank's counteragents failure to fulfill their financial obligations in due time) and (or) arising of unforeseen necessity for the bank to fulfill its financial obligations immediately and at the same time.

The liquidity risk includes the liquidity funding risk and the market liquidity risk.

The liquidity funding risk is the possibility of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of incapability to provide effective satisfaction of its own current or future needs (expected or unforeseen) for money and (or) property for mortgaging.

The market liquidity risk is the possibility of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of impossibility to sell or purchase easily the assets (or obligations) at their market value due to insufficient market depth preventing the scope of transactions from expansion without significant change of related prices or without the destabilization of the market itself.

11. The operational risk is the risk of sustaining damages (losses) by a bank and (or) bank's additional expenses or bank's failure to obtain planned incomes as a result of noncompliance of methods and procedures established by the bank for implementation of banking operations and other transactions with the legislation or violation of these methods and procedures by the bank's employees, the bank's employees incompetence or mistakes, inadequacy or failure of systems used by the bank including information systems, or as a result of external factors.

The major types of the operational risk and its origination sources are listed in accordance with the Annex to this Instruction. The legal risk and cyber-risk are also among the major types of the operational risk that may arise, inter alia, in combination with other types of the operational risk.

The legal risk is the risk of sustaining damages (losses) by a bank and (or) bank's additional expenses resulting from legal mistakes made during the activity implementation, from legislation inconsistency, imperfection and variability, and as a result of trials and other legal procedures negatively affecting the bank activity.

The legal risk arises as a result of nonobservance of the legislation by a bank, incompliance of bank's local regulatory legal acts with the legislation, ineffective arrangement of legal activities leading to legal mistakes, bank's or its clients' (counteragents') failure to fulfill or inappropriate fulfillment of contractual provisions, incorrect legal consultations, inadequate preparation of documents including those prepared within the scope of disputes submitted into judicial bodies of various states, bringing of lawsuits by the bank's employees and (or) other persons.

The sources of origination of the legal risk are any sources of origination of the operational risk according to the Annex.

The cyber-risk is the risk of sustaining damages (losses) by a bank and (or) bank's additional expenses or bank's failure to obtain planned incomes resulting from wrongful acts of a person or entity or a group of persons or entities committed by way of information technologies for the purpose of an unauthorized access to the bank's information infrastructure facilities and intended to violate confidentiality, integrity, availability, validity and safety of sensitive information.

The sources of origination of the cyber-risk are the following sources of origination of the operational risk according to the Annex:

internal fraud;

external fraud;

clients, products and business practices;

operation discontinuity and malfunctions (failures) of systems;

activity implementation and process management.

12. The strategic risk is the risk of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of mistakes (shortcomings) introduced in making the decisions defining the strategy of bank activity and development (the strategic management) and appearing as disregarding or insufficient regarding of possible hazards that can affect the bank's activity, incorrect or insufficiently reasonable identification of promising areas of activities where the bank can achieve an advantage over the competitors, lack or incomplete provision of resources (financial, technical, human) and organizational measures necessary to assure attainment of goals of bank's activity.

13. The risk of bank's business reputation loss (the reputational risk) is the risk of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of clientele reduction, reduction of other indices of development as a result of formation of negative attitude in the society with regard to the bank's financial reliability, quality of services provided by the bank or its activity nature as a whole. The bank's reputational risk can arise due to shortcomings in arrangement of activity, failures in operation of bank's electronic systems, nonobservance of the legislation or bank's local regulatory legal acts, derogation from business partnership customs, violation of norms of public morals and ethical principles of banking, suspected participation of a bank or its

employees in illegal financial transactions, in legalization of proceeds obtained by criminal means, in financing of terrorist activities, in financing of proliferation of weapons of mass destruction and in other unlawful activities.

14. The concentration risk is the risk of sustaining damages (losses) by a bank or bank's failure to obtain planned incomes as a result of concentration of specific types of risks.

Risk concentration means concentration of claims (obligations) or items in financial instruments with regard to the specific client or group of interrelated clients as well as clients associated with specific branches of economy or geographical regions or countries or with regard to the financial instrument, currency or other characteristics of items under risk, where such concentration can result in quite large losses (as compared with the amount of bank's normative or economic capital, the amount of assets, passives or the general risk level) and endanger the bank's financial position or its capability to implement its major activity.

The credit risk concentration appears as giving credits or other assets to a specific client or a group of interrelated clients or as a result of association of bank's debtors with specific branches of economy or geographic regions or focusing of activities on specific types of active operations making the bank vulnerable to the same economic factors.

The liquidity risk concentration appears as bank's focusing on specific sources of funding.

The market risk concentration appears as investments in similar financial instruments of one counteragent or trading portfolio or in specific currencies or goods with their market prices varying due to the impacts of the same economic factors.

The operational risk concentration appears as concentration of operational incidents by specific subdivisions and (or) areas of bank's activity (business lines) including such concentration resulting from growth of the number and (or) amounts of operations carried out, from systemic violations in implementation of risk management or internal control, from implementation of asset surge strategy, during provision of new banking products and services and in cases when a bank depends on one provider of services or on a small number of such providers.

CHAPTER 3
REQUIREMENTS FOR THE RISK MANAGEMENT BODIES IN THE BANK AND FOR THE ORGANIZATIONAL STRUCTURE OF THE RISK MANAGEMENT SYSTEM

15. Bank's management bodies must provide effective risk management and bank capital management meeting the bank's risk profile, nature and scopes

of banking operations and other activities carried out and assuring the bank's financial reliability.

The bank must provide regular participation of management bodies in arrangement and operation of the risk management system as well as clear distribution of powers and responsibilities in risk management between the board of directors (the supervisory board), the risk committee, the executive body, other collegial bodies and bank's officials, risk management subdivisions, risk-generating subdivisions, and provide cooperation between all aforementioned participants in the risk management process.

16. The bank's board of directors (the supervisory board) must provide arrangement of the risk management system on the consolidated basis, including such a system for risks in the banking group and (or) the banking holding where the bank is the principal organization, prevention of conflicts of interests and conditions for onset of these conflicts within the scope of risk management in the bank, the banking group and (or) the banking holding company where the bank is the principal organization, approve local regulatory legal acts defining the bank's risk management strategy, and define the bank-inherent risks tolerance.

17. The bank's board of directors (the supervisory board) must establish the risk committee headed by an independent director.

The risk committee shall:

carry out the internal monitoring of implementation of strategy and decisions made by the board of directors (the supervisory board) with regard to the risk profile and bank-inherent risks tolerance;

carry out the assessment of effectiveness of the risk management system on the consolidated basis, including such assessment in a bank, a banking group and (or) a banking holding company where the bank is the principal organization;

make decisions with regard to the risks within the scope of powers defined by the board of directors (the supervisory board);

submit to the board of directors (the supervisory board), for consideration, the committee's recommendations in matters of risk management;

regularly provide the board of directors (the supervisory board) with the reports covering the risk management system condition and the bank's level of risks.

The scope and intervals of information submission to the board of directors (the supervisory board) shall be appropriate to ensure the information sufficiency and its submission in due time for making the managerial decisions.

18. The bank's executive body must arrange the risk management system and ensure that the bank achieves the goals and fulfills the tasks set by the board of directors (the supervisory board) in this area.

The bank's executive body shall be responsible for limitation of propensity to risk (risk appetite) demonstrated by the risk-generating subdivisions, for compliance with the established bank-inherent risks tolerance and for maintaining the bank's risk profile adequate to the nature and scopes of activities carried out.

19. The executive body must approve the bank's local regulatory legal acts drafted in pursuance with the risk management strategy and regulating the risk management policy, techniques and procedures (unless the bank's Articles of Association defines that the approval of such local regulatory legal acts is within the scope of competence of the board of directors (the supervisory board)), as well as the procedures of decision-making, cooperation between the subdivisions, distribution and delegation of powers during implementation of risk management, and ensure their effective practical application.

20. The bank must appoint an official responsible for the risk management in the bank; this official must be subordinated directly to the head of the bank and accountable to the board of directors (the supervisory board), must be the bank's employee and the member of the risk committee. This official may be the head of the risk management subdivision.

The status, functions, powers and responsibilities of the aforementioned official must be specified in bank's local regulatory legal acts.

To avoid conflict of interests:

the officials (subdivisions) discharging the risk management for specific types of risks and (or) for risks in specific areas of activities (business lines) must be subordinated to the official responsible for risk management in the bank and (or) to the head of the bank's risk management subdivision (if any);

functions of an official responsible for the risk management in a bank must not cover the management of activities of subdivisions (business lines, business processes) generating risks (except for operational, strategic and reputational risks); also, these functions must not cover the management of accounting and preparation of accounting (financial) reporting as well as the responsibility for the internal control in a bank or participation in arrangement or implementation of such control.

The organizational structure of the risk management must be in line with the organizational and functional structure of a bank, nature and scopes of banking operations as well as other activities carried out by the bank.

21. A bank shall, at its own discretion, set the qualification requirements and business reputation requirements for an official responsible for risk management in the bank, and assess the compliance with these requirements; the intervals between assessments must be suitable to ensure that the aforementioned person's qualification and business reputation is maintained at an appropriate level.

22. The risk management system must be staffed with skilled specialists and provided with appropriate information systems, software and hardware suitable for gathering, processing and analysis of information used for the risk

management, stress tests, calculation of needs for capital and preparation of the management reporting.

A bank shall regularly analyze the existing information systems to ensure that they are capable to provide the risk management system operation in accordance with the requirements set by this Instruction, and promptly modify (update) these systems or introduce new ones when necessary.

23. The organizational structure of the risk management system, information flows generated by this system, allocation of areas of responsibility and powers of officials, procedures for implementation of these powers, procedures of cooperation between the bank's subdivisions and employees, subordination and accountability of subdivisions implementing the risk management, procedures for provision of information for subdivisions responsible for the risks to be accepted and for the risk management matters, and decision-making procedures must be arranged in such a way that is appropriate to prevent conflicts of interests, including those between subdivisions (officials) implementing the risk management and risk-generating subdivisions as well as subdivisions (officials) implementing the internal control in a bank.

CHAPTER 4
REQUIREMENTS FOR THE RISK MANAGEMENT STRATEGY, POLICY, TECHNIQUES AND PROCEDURES

24. Local regulatory legal acts must be prepared and approved in a bank to describe the risk management strategy, policy, techniques and procedures; these acts must be consistent, be detailed to a degree adequate for the level and significance of risks accepted and for the scope and complexity of bank's activities, and be applied uniformly in all bank's subdivisions.

These local regulatory legal acts must be assessed for adequacy at least once a year, including considerations of changes, significant for the bank, in bank's activity and condition, and consideration of changes in the financial market; appropriate amendments must be made in accordance with the assessment results.

25. The risk management strategy must reflect the strategic goals, major principles of operation of the risk management system and its development areas for the planning period in terms of the bank's risk profile, and bank-inherent risks tolerance, as defined by the board of directors (the supervisory board). The risk management strategy must take into account the cyclical aspects of the economy and their expected effects with regard to the level of the capital and major risks, composition and quality of the credit portfolio, investment portfolio and trading portfolio, sources for funding of assets and liquidity condition. The strategic goals (targets) of risk management must be realistic in terms of methods necessary to reach them.

The strategy must ensure the systematic approach for decision-making in terms of the risks level and medium-term and long-term risk management. To reach longer-term goals stage by stage, the bank's management bodies must set short-term goals (targets) in quantitative terms (indices and their target development pattern): the normative capital sufficiency level, the market share, target areas (clients, products, geographical regions), percentage of credits in assets, quality of assets, portfolio diversification and other indices.

26. The risk management policy must define the goals and tasks for the risk management, major principles and methods used to reach these goals and to solve these tasks; also, it must contain the list of bank-inherent risks and their definitions, identify the risks most significant for the bank, establish the requirements for the risk management as a whole including the organizational structure, powers and functional duties of bank's executives and employees, risk management process arrangement, approaches for assessment of efficiency of the risk management system and for its improvement.

The risk management techniques must contain the detailed description of procedures by components of the risk management process, the specific features of the risk management for various types of risks, the bank stability analysis in terms of risks, the procedure for application of results obtained within the scope of the risk management and bank stability analysis, other necessary procedures, descriptions and regulations.

27. The risk management process includes the risk detection (identification), measurement (assessment), internal monitoring, controlling, and risk level limitation (reduction).

28. Risk detection (identification) involves detection of major risk sources (risk factors) that have resulted or may result in losses and (or) additional expenses.

The bank must carry out the classification of risks (their types, categories) and must prepare the technique for identification of risk types significant (or insignificant) for the bank; this technique must be suitable, inter alia, to take into consideration the mutual impacts of risks, their concentration, and to identify new risks arising in bank's activity including those resulting from launching the new types of operations (introduction of new products) by the bank or from penetrating the new markets.

29. Risk measurement (assessment) is the determination of the risk level (amount) by quantitative and (or) qualitative (expert) assessment methods, with quantitative and qualitative assessment factors used for formation of reasonable opinion about the risk level.

Measurement (assessment) methods and procedures for calculation of amounts of all bank-inherent risks, being in use, must be described in bank's local regulatory legal acts. For risks not included into calculation of normative capital sufficiency norms but recognized by the bank as significant, the risk amount measurement (assessment) methods shall be chosen by the bank at its own discretion.

The bank must conduct internal assessment of capital adequacy for covering not only expected but also contingent losses, if any abnormal (crisis) situations occur. Within the framework of this process the bank must assess the extra need for the capital and ensure availability of the necessary capital amount taking the aforementioned need into consideration within the scope of its day-to-day activity and in cases when, in accordance with the strategy and (or) the policy, development of new types (areas) of activities (products) or new markets or sharp increase of amounts of operations are planned, involving higher levels of risks.

To assess the aggregate amount of the extra need for the capital, a bank must prepare the procedure for calculation of this amount including both calculation of the need for the capital, with quantitative measurement (assessment) tools used for this purpose, and allocation of an amount from the capital to cover the risks, in accordance with the expert assessment.

Methods chosen for the assessment (measurement) must be adequate to the significance of the risk type and to the scope and complexity of activity carried out by the bank; it means that the input data for the assessment must be detailed sufficiently, the assumptions and assessment factors being in use must be reasonable, and generally accepted terms and concepts must be used.

The procedures used for the risk amounts calculation must be revised from time to time and updated to make them more effective and to ensure their compliance with the legislation and the variations of market conditions.

30. The internal monitoring of risks is the system of gathering (accumulation), processing and analysis of the information used as the background for assessment and controlling of risks and for preparation of prudential reporting and management reporting

The internal monitoring of risks must be carried out by the bank by regular maintenance and analysis of databases containing the data about clients, debtors, counteragents, correspondent banks, security issuers, mortgage assets, market values of assets, exchange rates, operational incidents and other data received from internal and external information sources and necessary for assessment of risks at the levels of a single operation (transaction), portfolio and bank's risk profile as a whole.

The bank must also arrange the system of key indices for each bank-inherent risk; these indices must be associated with the risk level and must demonstrate the potential risk sources, and the system of indices must make it possible to analyze these sources regularly, to set the threshold value (the limit) for each index and to provide for taking appropriate response methods if the index is beyond the limit, and to study the internal and external factors affecting the risk level.

31. The risk limitation (reduction) means that the set of measures must be implemented by the bank to reduce the probabilities of events that can result in losses (damages) including the refusal to accept the risk or the risk transfer to the third party or reduction of the amount of losses (damages) if they take place.

The bank's local regulatory legal acts must describe the methods (tools) being in use for limitation (reduction) of risks, the system of limits and (or) limitations (the limit policy) designed for specific clients, groups of clients, transactions, operations and their types, areas of activity, the procedure for controlling the application and observance of the limit policy and for taking appropriate measures by the management.

32. The procedure for the internal control of risks must be prepared in the bank and described in local regulatory legal acts including the measures to be taken in case of violation of this procedure; the procedure must include, inter alia, the implementation of:

the preliminary control: by selection of skilled personnel; preparation of clear, detailed and unequivocal job descriptions preventing the onset of conflicts of interest, and preparation of the procedures for implementation of operations; preliminary analysis of riskiness and effectiveness of operations to be carried out; bank provision with necessary hardware, equipment, information technologies;

the routine control: by verification of compliance with the requirements of the legislation, bank's local regulatory legal acts in risk management, established decision-making procedures, limits and other limitations, endorsement procedures, payment procedures, validity of records describing the banking operations in the accounting;

the post-control: by verification of reasonability and correctness of operations, compliance of documents with the preset forms, compliance of employees' functions with their job descriptions;

comparison of the incurred versus planned (forecasted, modelled) losses, comparison of planned versus real indices of activity, of the amounts of inherent versus residual risks;

implementation of the assessment of bank's risks by the bank's risk management subdivision (or an authorized employee), and assessment of bank's risk management system effectiveness by the internal audit service.

33. The bank must implement the activities for compensation of possible losses in case of realization of risks including formation of special reserves for coverage of possible damages in assets and operations not recorded in the balance sheet, in accordance with the legislation; in addition to these reserves, a bank may create other reserves (general-purpose and special reserves) in cases and in accordance with the procedures specified in local regulatory legal acts, and may use other methods for compensation of losses.

34. The bank must regularly analyze its stability in terms of bank-inherent risks including modeling, analysis of potential impacts of possible shocking

situations (stress testing) for bank's financial position in accordance with the approved local regulatory legal acts where the schedule of stress tests is described.

The aforementioned local regulatory legal acts must describe the goals and tasks of stress testing; major stages and their purposes; allocation of powers and procedures for implementation of powers; technical resources, information and human resources adequate for formation and development of the infrastructure for the stress testing and for relevant data handling; appropriate intervals between stress tests; procedures for consideration of stress testing results and for submission of these results to the bank's management bodies.

35. The procedure for using the results obtained within the scope of risk management and bank stability analysis shall be prepared in a bank; this procedure must provide for regular informing of bank's management bodies about these results and making the decisions by these bodies including the decisions for exceptions with regard to the established procedures, methodologies and limits (limitations).

To inform the bank's management bodies and officials, the management reporting must be used; this reporting must be prepared to describe the characteristics as for the dates set by the bank for identification of negative trends. This reporting must contain information as follows:

bank's risk profile including the level of major risks, their brief description and key problems in risk management with regard to these risks;

failures to meet the risk limitation norms and other safe operation norms;

normative capital structure and amount; need for extra capital;

major risks; structure of portfolios (credit, investment and trading portfolio) and quality of assets;

liquidity condition;

significant breaches of limits, major operational incidents;

stress test scenarios and results;

other information, conclusions and proposals appropriate for making necessary managerial decisions by the bank owners and (or) management bodies.

Bank's local regulatory legal acts must specify the procedure, scope, levels and intervals for submission of the management reporting to the bank's management bodies and officials, appropriate to ensure sufficiency of information and timeliness of its submission to the bank's management bodies for making the managerial decisions.

The bank must also take the aforementioned results into consideration within the scope of strategic planning, improvement of risk management strategy, policy and procedures, preparation (or regular revision) of plans (activities) for unfavorable (crisis) conditions including the crisis financing plans.

36. The bank must prepare the plan of activities for emergency situations in order to ensure continuity of operation of the bank in case of unfavorable

(crisis) situations; in this plan, the procedures and organizational aspects of bank's activities in emergency situations must be described.

The bank must also prepare the plan of financing in crisis situations. In this plan, the arrangement of activities must be described for overcoming serious breaches of bank's capability to provide funding for several or all kinds of its activity, in due time and with affordable expenses; crisis financing sources must be specifically listed, and forecasted amount of resources that can be obtained from these sources must be specified; the procedures, scopes of competence and decision-making hierarchy in case of liquidity problems must be specified; time frames for these decisions must be set for various assumptions and stresses. These plans, as far as necessary, must be brought in line with plans of activities for emergency situations.

The controlling of implementation of plans must be carried out in a bank; the plans must be revised and corrected with intervals defined by the bank's risk management policy and with due consideration of variations of market conditions.

37. From time to time (at least once a year), a bank must carry out the risk management system effectiveness assessment (verification) to keep the system adequate to the varying conditions.

The risk management system and (or) its elements must be regularly inspected by the bank's internal audit service or an auditing organization (or an auditor carrying out an activity as an individual entrepreneur), or by other entity having appropriate qualification.

The results of these inspections (assessments) must be taken into consideration within the scope of the processes of development and improvement of the risk management strategy, policy and procedures.

38. The bank must specify, in its local regulatory legal acts, the procedure for disclosure of information about the risk management system arrangement, and define the procedure implementation method and the scope of information to be disclosed.

Annex
to the Instruction on Arrangement of the Risk Management System
(including the amendments and additions made by the Resolution of the Board of the National Bank dated 26.06.2020, No. 214)

MAJOR OPERATIONAL RISK TYPES AND ITS ORIGINATION SOURCES

Operational risk source	Definition	Operational incidents	Operational risk type
Internal fraud	Bank employees' activities for deliberate deception, bank property stealing, deliberate violation of established rules, legislation and (or) bank's policy (except for the cases of discrimination in employment)	Stealing; extortion; appropriation of property or embezzlement; computer thievery; document forgery; fraud in accounting and reporting; intentional failure to record and intentional failure to reevaluate the trading portfolio items; illegal operations with securities based on in-house information about the security issuer's activity, other usage of confidential information for acquisitive purposes; unauthorized operations, other abuses in implementation of banking operations on bank's behalf and at bank's expenses; intentional destruction of property; bribery; tax evasion	Internal fraud risk
External fraud risk	Third persons' activities against the bank for deliberate deception, bank property stealing and (or) activities involving breach of legislation	Stealing, robbery, fraud, extortion; information theft; crime against information security; payment document forging	External fraud risk
Staffing policy, occupational health and safety	Bank's failure to observe labor legislation, occupational health and safety legislation,	Payments of claims for compensation of harm inflicted to citizen's life and health as a result of violation of occupational health and safety rules;	Personnel risk

	application of ineffective procedures for personnel recruiting, training, work assessment and motivation	payments in cases of accidents that took place during the discharge of their job duties by the employees, resulting in their incapacity for work; payments of claims for elimination of discrimination in employment; payments resulting from inappropriate termination of labour contract; payments and (or) other losses resulting from activities of trade unions and associations of employees; personnel inadequacy to the nature and scopes of bank's activities; undesirable turnover of personnel; employees' non-association with a bank; ethical inadequacy of banks' employees; employees' absence from work without good reasons; hiring of insufficiently skilled employees; personnel overwork; insufficient number of skilled personnel at a specific working area	
Clients, products and business practices	Inappropriate practice of client service and (or) shortcomings of banking services (products)	Inappropriate preparation of new banking services (products); client's problems with access to their accounts; lack of information delivered to a client and received from a client; unavailability and (or) inappropriate preparation of necessary client's documentation; unfair implementation of established rules, procedures and regulations; incorrectly specified limits, breach of limits; application of inadequate mathematical or statistical models; unintentional disclosure of confidential information including insider information; client manipulation and market manipulation; breach of antitrust legislation; legalization of proceeds obtained by criminal means	Operational activity risk Risk associated with legalization of proceeds obtained by criminal means, financing of terrorist activities, financing of mass destruction weapons proliferation

Tangible assets damage	Bank property damaging (destruction), loss of lives as a result of natural disasters, industrial disasters and impacts of other similar factors	Damage resulting from floods, earthquakes, hostilities, terrorism, vandalism, hooliganism; damage resulting from unintentional destruction or damaging of tangible assets	Property risk and force majeure risk
Operation discontinuity, system malfunctions (faults)	Damages or malfunctions in operation of mechanisms, technical facilities and systems supporting the bank functioning	Damages and malfunctions of software and hardware; damages or malfunctions of telecommunications; interruptions in electrical energy supply and other utilities; significant errors, data loss and corruption, operations carried out not in due time in cases when the bank applies information technologies, systems and equipment inadequate to the nature and scopes of activities to be carried out, or unreliable, or poorly adjusted, or outdated or unlicensed software, and there is no backup system	Technical risk, risk associated with information technologies (or IT risk)
Activity implementation and process management	Inappropriate handling of operations (transactions), bank processes management, contacts with suppliers	Errors in data input (loading, maintenance), in preparation of primary accounting documents, in implementation of accounting and conducting of operations	Operation risk
		Inappropriate planning, outdated management procedures, inadequate management reporting, formal and ineffective internal control and risk management procedures	Risk of management and incorrect managerial decisions
		An organizational structure inadequate to the nature and scopes of bank’s activities, mistakes in the function distribution system resulting in duplication of functions or loss of some functions in managerial processes being in use (running control and preliminary control functions), redundant structures, excessive	Risk of inappropriate arrangement of the bank structure, the scope of responsibility and distribution of powers between the bank officials and subdivisions

		levels of management, diffusion of responsibility, onset of conflicts of interests	
		Oversights in various information summarization within the scope of bank’s activity, failures arising in business processes, internal control systems and risk management systems as a result of physical separation between the managing personnel and personnel implementing the operations	Risk associated with geographical diversification of bank’s activity
		Transaction (operation) accounting recording inconsistent with the accounting policy accepted by the bank	Accounting risk
		A methodology inappropriately accepted for implementation of processes, techniques, regulations, calculation methods	Methodological risk
		Breach of contractual periods or obligations, compensation of suppliers’ damages or losses resulting from bank employees’ neglect of duty; conflicts with suppliers, their incorrect and unlawful activities, including wrongful use of confidential information about the bank’s activity	Third-party service usage risk or outsourcing-related risk