National Bank of the Republic of Macedonia

Operational Risk Management Policy of the National Bank of the Republic of Macedonia (Unofficial Consolidated Text)

January 2015

Pursuant to Article 47, paragraph 1, items 9 and 22 of the Law on the National Bank of the Republic of Macedonia (Official Gazette of the Republic of Macedonia No. 158/10, 123/12 and 43/14), the National Bank of the Republic of Macedonia Council adopted the following

Operational Risk Management Policy of the National Bank of the Republic of North Macedonia (consolidated text)[1]

I. GENERAL PROVISIONS

1. The Operational Risk Management Policy of the National Bank of the Republic of North Macedonia (hereinafter: Operational Risk Policy) establishes a system of coordinated, comprehensive and systematic operational risk management in order to identify events that may affect the functioning of the National Bank, to ensure maintenance of the exposure to risks within acceptable limits and to ensure effective accomplishment of the objectives of the National Bank of the Republic of Macedonia (hereinafter: the National Bank).

2. The terms used in this Policy shall denote the following:

– **Operational risk** shall denote the probability of occurrence of material or non-material damage, i.e. occurrence of negative effects on the work, health and lives of employees, financial result and reputation, and thus the achievement of the strategic objectives of the National Bank, under the influence of a number of specific risk events arising from the people management, working processes, infrastructure, information systems, communication, regulations and changes in the environment.

– **Operational risk management** shall denote a process of continuously and systematically identifying, assessing, responding to, reporting on and monitoring operational risks.

– **Probability** shall denote the frequency of the risk event, determined on the basis of historical data or on the basis of examination of the possibility of its occurrence in the future.

– **Effect, impact of operational risk** shall denote the ultimate negative effect, the consequence of the occurrence of the risk event.

– **Level of operational risk** shall denote the size of the operational risk determined on the basis of the effect, the impact and the likelihood of occurrence of the risk event.

– **Risk event** is an event that may cause negative consequences for: a) working processes, which includes the achievement of the goals, health and life of the employees; b) the financial result; and c) the reputation of the National Bank.

– **Working process** shall denote a series of functionally related and structured steps and actions (procedures), which are accomplished sequentially and are aimed at achieving the objectives of the National Bank. The working process is documented by a narrative description of activities.

– The **project** shall include several related activities that need to reach a certain goal, has a limited duration, predetermined budget and resources needed for its execution.

[1] Operational Risk Management Policy of the National Bank of the Republic of Macedonia P. No. 02-15 / I-1/2015 from January 29, 2015, P. no. 02-15 / II-1/2018 from February 1, 2018, P no. 02-15 / XIV-1/2020 from October 13, 2020, P no. 02-15/X-1/2022 from June 30, 2022 and D no. 02-15/X-9/2022 from June 30, 2022.

– **Inherent risk** shall denote the risk that it is characteristic to the nature of the working process or project, without implementing measures and control mechanisms toward its mitigation.

– **Residual risk** shall denote the risk that is determined after the implementation of measures and control mechanisms.

– **Incident** shall denote an individual or a series of unwanted or unexpected events that had or could have a negative impact on the business goals, life and health of the employees, the financial result and the reputation of the National Bank

– **Operational risk tolerance** shall denote the readiness of the National Bank to accept residual risks identified in order to achieve the strategic goals.

– **Maximum acceptable interruption** shall denote the period after the interruption of the working process, where after negative impact on the achievement of the objectives of the operations, financial position and reputation are expected.

II. BASIC PRINCIPLES

3. For the purposes of accomplishing the objectives from paragraph 1, the Operational Risk Policy shall be based on the following basic principles:

– **Efficiency** - measures taken and resources used in response to the identified risks should be proportional to the size of the damage that may occur during the realization of the risk event. The principle of efficiency shall be achieved through constant cost benefit analysis, taking into account the operational risk tolerance, as determined by the National Bank;

– **Effectiveness** - selection of activities and measures that will enable strengthening of the flexibility and the resilience to changes imposed by the environment and achieving the objectives of the National Bank through a systemic and structured approach to the of operational risk management;

– **Transparency and confidentiality** - exchange of information on incidents that occurred, for the purpose of timely, transparent and cooperative monitoring of the potential sources of operational risk and preventing potential risk events. Recipients of information shall be obliged to treat the information properly depending on the degree of confidentiality set by their owner, provider of information.

– **Responsibility and accountability** - allocation of responsibilities and reporting in managing and dealing with operational risks.

– **Increasing the awareness and knowledge of operational risks** - awareness of employees at all levels in the National Bank about their responsibilities and tasks in managing operational risks and promoting integrity and ethical behavior.

III. METHODOLOGICAL FRAMEWORK

4. The methodological framework shall consist of a series of related components that enable establishing a systematic operational risk management and contains the classification of risks, operational risk tolerance of the National Bank and the procedure for operational risk management.

Classification of Risks

5. Classification of risks shall provide for clear and commonly accepted terminology, consistency and accuracy in the identification, analysis and reporting on operational risks, when determining the strategies and implementing the measures and control mechanisms for dealing with risks.

Classification of risks shall include: the main sources of operational risk, potential risk events and consequences of the occurrence of the risk event.

6. The sources of operational risks shall be divided into the following main categories: internal factors (human factors, management and working processes, systems) and external factors.

Identified operational risks and sources of operational risk that are inherent in the execution of working processes and projects shall fall within different categories in the classification of risks and shall be subject to a regular annual review.

7. Potential risk events shall be divided into the following categories: errors and omissions, delay, fraud, unauthorized disclosure of confidential information, non-compliance with the regulations, inaccessibility of the communication infrastructure and systems, injury, disruption of the health, the life (death) of the employee and other events that may cause disruption of the integrity, availability or confidentiality of information and information assets.

8. Deleted.

Operational Risk Tolerance

9. Operational risk tolerance is the readiness of the National Bank to accept the identified residual risks, in order to achieve the strategic goals.

Operational risk tolerance shall be determined relative to the possible effects, impacts and likelihood of occurrence of risk and includes the implemented measures and control mechanisms for its mitigation.

10. The operational risk tolerance defines the limits of the acceptable exposure to operational risk and determines the risk levels that require mitigation measures.

In exceptional cases, as a result of the influence of certain short-term factors or for the purpose of time alignment and undertaking measures, the Council may allow deviation relative to the fixed level of operational risk tolerance in a period of one year.

11. The following operational risks are determined as unacceptable by the National Bank:

- risk that could jeopardize the accomplishment of the objectives and tasks envisaged by the Law on the National Bank;
- risk that could cause significant damage to the interests of the National Bank, the country and the citizens;
- risk of violation of the regulations;
- risk of incurring significant financial loss;
- risk to the reputation, which may adversely affect the credibility of the National Bank;
- risk that could jeopardize the health and lives of the employees.

12. Operational risk tolerance is graphically presented by the Risk Matrix (Figure 1), which contains five levels for assessing the effects and the probability of occurrence of the risk event and four risk zones.

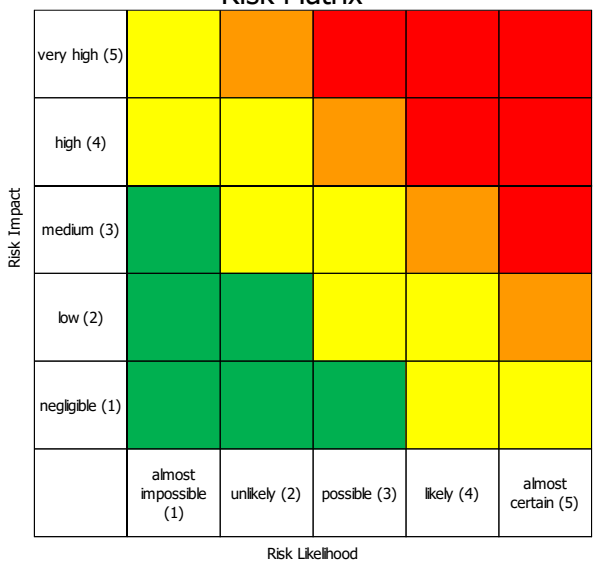
The higher level of operational risk suggests a greater probability and higher negative effects of the occurrence of the risk event.

Operational risks are divided into risk areas based on the probability of occurrence and potential negative effects of the risk event:

– **Risks in the "green zone"** are small and acceptable, so they do not impose a need for taking preventive action, but there is room for implementing specific solutions or improvements without or with minimal financial costs.

Figure 1

Risk Matrix



– **Risks in the "yellow zone"** are moderate, indicating the need of taking certain mitigation measures, but by carefully defining and limiting the costs. The measures for dealing with these risks are adopted by the heads of the organizational units in accordance with the relevant strategic managers.

– **Risks in the "orange zone"** are medium and suggest the need to take mitigation measures in the next short term period (from one to three years). The strategies and measures for dealing with these risks, upon proposal by the managers of the organizational units, approved by the strategic manager, are adopted by the Risk Management Committee.

– **Risks in the "red zone"** are high and suggest undertaking mitigation measures within a year. The Risk Management Committee sets the strategies, the measures and the action plans for taking the measures for dealing with these risks. In case of risks classified in the red zone with new processes or projects, their execution should be postponed until the level of operational risk is lowered.

Operational Risk Management Procedure

13. Operational risk management is carried out through the following steps: registration of the working processes and determining their degree of criticality, identification, recording and assessment of operational risks, determining a strategy and action plan with mitigation measures, reporting and monitoring.

14. **Working processes** are selected according to their importance in achieving the strategic objectives of the National Bank, taking into account internal and external factors.

15. Critical working processes are those processes in which the materialization of a few extreme scenarios may lead to the suspension of their execution, which could have

negative consequences (levels 4 and 5) for the functioning, financial result, reputation of the National Bank, and thus the achievement of the objectives of the National Bank.

The degree of criticality is based on the following scenarios:

– Jeopardizing the integrity of the National Bank due to intentional or unintentional use of incorrect information due to which incorrect results are obtained.

– Jeopardizing the confidentiality of information amid intentional or unintentional publishing of confidential information.

– Disruption of the accessibility of the National Bank due to interruption of working processes and inability to perform them again.

16. **Identification of Operational Risks.** The main objective of the identification of operational risks is to determine the potential sources of operational risk and risk events that could have negative impact on the functioning, financial result and reputation of the National Bank.

Operational risks are identified by applying more methods and techniques, including: analysis of historical data series, systematic monitoring of the working processes performed by the employees, using the findings and recommendations of the internal and external audits, structured interviews, questionnaires, group discussions, analysis of past incidents and other auxiliary methods and techniques including the method of brainstorming.

17. **Recording of operational risks** ensures proper understanding, prioritization and coping with risks.

Risks are recorded in a clear and unambiguous manner, using the established terminology from the classification of the sources of risks and potential risk events.

18. **Assessment of operational risk** involves assessment of the identified risks according to certain qualitative and/or quantitative criteria.

Qualitative criteria are most commonly used in assessing the risks and derive from the experience, knowledge and evaluation of employees.

Quantitative criteria are determined on the basis of statistical analysis, for example analysis of historical data series about past events.

The assessment shall be based on the specifics of the working process, i.e. it takes into account the risks that are typical in its execution (inherent risks) and includes the measures and control mechanisms that have been taken up to that point in time to deal with the identified operational risks.

19. After determining the level of operational risk, **the strategy for dealing with operational risks** is determined.

The National Bank may implement the following operational risk management strategies:

– Avoidance - undertaking measures and activities that do not involve risk, or modifying the processes in order to avoid the risk.

– Transfer - transferring or mitigating operational risk by including another entity that partially or fully accepts the risk.

– Mitigation - undertaking measures and activities that reduce the impact and likelihood of occurrence of the risk event by introducing additional procedures and appropriate controls.

– Acceptance - acceptance of the existing level of operational risk, which includes preparing plans for dealing with the consequences in the event of the occurrence of the

risk. This strategy shall be applied in the following events: a) when the costs for risk mitigation are larger than the losses from the occurrence of the risk event, b) with risks whose consequences can be devastating, but the ability to take action is limited, or c) with risks whose occurrence and magnitude of impact can not be predicted.

20. **The Action Plan** shall provide coordination and effectiveness of the measures for dealing with operational risks, determine the priorities and control mechanisms.

21. **Reporting and monitoring of risks** aims to provide consistent evidence that the process of risk management is being effectively implemented, that the risks are maintained within the operational risk tolerance and that the measures for dealing with the identified risks are implemented in accordance with the action plans.

22. Based on the reports from the organizational units, the Chief Risk Officer prepares a consolidated annual report on the operational risk management and following the approval by the Operational Risk Management Committee, it is submitted to the National Bank Council.

23. Operational risks shall be constantly monitored by:

- examining the possible deviations regarding the operational risk tolerance;
- monitoring the action plans in terms of achieving the envisaged measures and deadlines;
- examining the novelties in the business environment and finding the best solutions for discovering new operational risks, determining control measures and active monitoring and reporting the occurrence of incidents.

IV. ORGANIZATION OF THE OPERATIONAL RISK MANAGEMENT - TASKS AND RESPONSIBILITIES

24. Operational risk management shall be implemented by several organizational levels in the National Bank, and the tasks and responsibilities shall be allocated to: The National Bank Council, the Operational Risk Management Committee, the Strategy and Prevention Office - Strategy and Operational Risk Function, the heads of organizational units[2], the operational risk management officers in the organizational units, the Internal Audit Department and all of the employees in the National Bank.

The National Bank Council

25. The National Bank Council shall be responsible for establishing the framework for the operational risk management by:

- adopting the Operational Risk Policy and monitoring its implementation;
- monitoring, evaluation and, if necessary, reviewing the appropriateness of the adopted Operational Risk Policy depending on the changes in the internal or external environment.
- adopting and performing an annual review of the operational risk tolerance;
- monitoring the exposure of the National Bank to operational risks;
- monitoring the strategies and action plans with measures for operational risk management;

[2] Department managers, Head of the Governor's Office, Chief Internal Auditor and officers authorized by the Governor to be in charge of the organizational units or working processes.

– other activities aimed at the development and improvement of the operational risk management.

Operational Risk Management Committee

26. The Operational Risk Management Committee shall be responsible for providing conditions for the development and consistent application of the risk management framework and for monitoring the implementation of the measures for dealing with operational risks.

27. The Operational Risk Management Committee shall be composed of: the Governor, as a President, and the Vice Governors of the National Bank, the Secretary General, the General Director and the advisor to the Governor in charge for Financial Stability and Macroprudential Policy Department and Banking Regulations and Resolution Department, as members with a voting right.

The sessions of the Operational Risk Management Committee are attended by representatives of the Strategy and Prevention Office (Chief and Assistant Chief for Strategy and Operational Risks, Chief and Assistant Chief for Information System Security, Personal Data Protection and Classified information, representatives of the Compliance function) and the Chief Internal Auditor, without a voting right.

28. The Operational Risk Management Committee shall have the following responsibilities:

– establishing and monitoring the implementation of the Operational Risk Policy, and preparing proposals for its improvement;

– monitoring and analysing the operational risk management process, and the effectiveness and efficiency of the measures and controls with respect to changes in the environment;

– monitoring and analysing the reports on the identification and assessment of the risks by the organizational units regarding the operational risk tolerance;

– approving and monitoring the strategies and action plans in response to the identified operational risks;

– regular semi-annual and annual reporting to the National Bank Council on the exposure to operational risks, and if necessary submits more frequent notifications for significant exposure to operational risks.

29. The Operational Risk Management Committee may adopt additional guidelines for dealing with particular operational risks and for establishing coordination with horizontally related processes.

30. The work of the Operational Risk Management Committee, as a body responsible for implementing the Operational Risk Policy shall be regulated by Rules of Procedure adopted by the Governor.

Strategy and Operational Risk Function

31. The Strategy and Operational Risk Function shall be responsible for ensuring immediate implementation of the methodological framework and coordinated operational risk management in the National Bank.

The Strategy and Operational Risk Function shall have full autonomy and independence in its work and shall be accountable to the Governor of the National Bank.

32. The Strategy and Operational Risk Function shall have the following responsibilities:

- implementation of the Operational Risk Policy;
- regular monitoring of the National Bank's exposure to operational risks relative to the determined level of operational risk tolerance through collection of data and reports on risk management prepared by the organizational units;
- reviewing and monitoring the results of the assessment of the degree of criticality of working processes;
- encouraging the cooperation and exchange of information between organizational units by organizing meetings, presentations or group workshops for identification and assessment of the operational risks (especially in horizontal processes);
- monitoring of reported incidents and checking the status of actions taken;
- preparing a consolidated annual report on risk management in the National Bank, which through the Operational Risk Management Committee shall be submitted to the National Bank Council;
- advisory and methodological support of the Operational Risk Management Committee;
- preparing and submitting proposals for improvement of the Operational Risk Policy;
- development and maintenance of a register of processes of the National Bank;
- regular annual update of the classification of operational risks based on the proposals of the organizational units;
- providing appropriate training and practical experience for the operational risk management.

Heads of organizational units

33. Heads of organizational units shall organize the operational risk management in the organizational units during the implementation of the working processes and projects of the organizational unit they manage.

34. Heads of organizational units shall be responsible for:

- regular monitoring of the register of processes, as well as determining their degree of criticality;
- identification and assessment of the operational risks related to the execution of working processes;
- regular monitoring and reviewing of the records of incidents that occurred;
- determining strategies and developing action plans with draft-measures for addressing the identified operational risks;
- monitoring the exercise and effectiveness of the measures and control mechanisms of action plans in terms of the changes in the environment and the best practices;
- approving the regular reports on operational risks.

35. In the case an operational risk in the orange or red zone of risk occurs, heads of organizational units shall deliver emergency notifications to the Strategy and Operational Risk Function.

The Strategy and Operational Risk Function shall immediately report to the Operational Risk Management Committee.

Operational risk management officers in the organizational units

36. The operational risk management officers are selected from among the employees who are fully familiar with the working processes and risks in current operations in the organizational unit, whose performance has been highly evaluated and who showed positive results in their operations.

37. The operational risk management officers shall be responsible for the following:

- regular updating of the register of processes that are the responsibility of the organizational unit;
- identifying operational risks in the implementation of working processes and projects;
- assessing the likelihood and effects of the materialization of the risk event;
- timely reporting on operational risks, on a regular semi-annual and annual basis, as well as on a monthly basis for determined significant exposure to operational risks;
- timely reporting of operational risks;
- cooperating and regularly exchanging information with the Chief Strategy and Operational Risk Officer.

Internal Audit Department

38. The Internal Audit Department shall review and assess the implementation of the operational risk management framework by monitoring the application of the operational risk management methodology, as well as the performance of the defined measures and control mechanisms for dealing with operational risks.

The Internal Audit Department may give suggestions for improving and increasing the effectiveness of the measures and control mechanisms in the operational risk management process.

Employees

39. The employees of the National Bank shall at all times identify, assess and monitor operational risks that could jeopardize the attainment of the objectives, shall propose measures in response to the identified risks and report on incidents occurring in the performance of regular duties.

V. TRANSITIONAL AND CLOSING PROVISIONS

40. The Governor shall adopt Guidelines for the implementation of the Operational Risk Management Policy of the National Bank.

41. With the entry into force of this Operational Risk Management Policy, the Operational Risk Management Policy of the National Bank, P.no. 02-15/IX-3/2011 of 15.9.2011, shall cease to be effective.

42. The Operational Risk Management Policy shall enter into force on the date of adoption, while items 19, 20, 21, 202, 213 and 224 will apply after one year of enactment.

P. no. 02-15/I-1/2015
29 January 2015
Skopje

Governor
and Chairman
of the National Bank of the Republic of Macedonia Council
Dimitar Bogov