

Regulation of the National Bank of Georgia on the Management of Operational Risks at Commercial Banks

Approved by Decree N. 47/04 of June 13, 2014

of the President of the National Bank of Georgia

Effective September 1, 2014

Article 1. General Provisions

1. All commercial banks, both resident and branches of non-resident foreign banks operating in Georgia must have an Operational Risk Framework (hereinafter Framework) in place.
2. The Framework must be appropriate and commensurate with the bank's size and complexity and the nature of its business.
3. The Framework must be fully integrated into the bank's overall risk management process.
4. The bank is permitted to use and develop its own definitions and methodology in line with the Framework, as long as the definitions and methodology are based on Basel Committee for Banking Supervision's (hereinafter Basel) standards or other internationally recognized methodology for operational risk management.

Article 2. Operational Risk Framework

1. The Framework shall consist of policies that incorporate and clearly define and address the following elements:
 - a. operational risk objectives and risk appetite;
 - b. definition of operational risk and differentiation from other types of risk;
 - c. definition of operational loss
 - d. Other terms and definitions associated with operational risk that are based on Basel methodology or other internationally recognized standard;
 - e. classification of operational risks per business line and event type and the relevant risk exposure;
 - f. risk assessment tools and methods to track relevant data , such as material losses; This includes but is not limited to the following instruments;
 - i. An operational loss database;
 - ii. Business process identification and mapping
 - iii. Key Risk Indicators (KRIs)
 - g. risk management lifecycle which must include:
 - i. the establishment of a clear risk identification and control mechanisms;
 - ii. Risk monitoring and reporting;
 - iii. Risk mitigation and the assessment of residual risk.
 - h. Clear, understandable, effective and healthy management structure with well-defined, transparent and consistent lines of responsibility that will be approved by the supervisory board of the commercial bank;

- i. Trainings and courses, the aim of which is to increase the level of operational risk awareness within the organization;
 - j. The dependence of the bank on other sector/s;
 - j.¹ Risk of Outsourcing;
 - k. Management of information systems;
 - l. Business continuity (contingency) management, which also includes provisions for disaster recovery;
 - m. Accuracy risk management, which includes assurance regarding the accuracy of various data associated with a commercial bank and the existence of a well-managed and organized reporting process.
- 2. A commercial bank shall regularly evaluate, assess and update its policies and procedures for operational risk management in accordance with its operational risk exposure and risk profile and make any necessary changes, if needed.
- 3. All policies included within the Framework shall be fully documented in writing.
- 4. When reporting operational risks, commercial banks are required to follow the "Guidance for Accounting for Operational Risk Losses" issued by the National Bank of Georgia.

Order №194/04 of the President of the National Bank of Georgia dated August 1, 2023, published on the website on 02.08.2023

Article 3. Supervisory Board

- 1. The supervisory board is responsible for establishing, approving as well as periodically reviewing all policies within the Framework. This includes, but is not limited to reviews of whether the commercial bank is meeting its operational risk objectives, thresholds, and limits which are set out in the bank's risk appetite;
- 2. The supervisory board of the bank must support a strong risk management culture within the organization that fully takes into consideration and incorporates operational risk.
- 3. The supervisory board must have adequate knowledge and awareness of operational risk.
- 4. The supervisory board must regularly receive internal operational risk reports. The internal reports must be analytical in nature and must be detailed enough to determine whether the risk profile of the commercial bank is in compliance (in line with) the risk appetite as approved by the supervisory board.

Article 4. Board of Directors

- 1. It is the responsibility of the board of directors to raise the level of awareness within their respective organizations on operational risk, so that all employees of the organization are well informed about what operational risks consist of.
- 2. The board of directors must ensure that the commercial bank hires and employees competent and knowledgeable people throughout all business lines, and shall consistently work towards developing and improving competency and ethics standards within the organization. The board of directors is required establish a strong organizational culture that supports professionalism and a high level of responsibility throughout the organization.
- 3. The board of directors is responsible for consistently implementing operational risk policies, processes and systems throughout the organization, which in turn includes all products, services and operations of a commercial bank and which is in line with the commercial bank's risk appetite.
- 4. The board of directors is responsible for defining what constitutes a materially significant operational risk event, which must be approved by the National Bank of Georgia.

5. The board of directors shall establish a mechanism for the notification of materially significant operational loss events to the National Bank of Georgia.
6. A commercial bank must immediately notify the National Bank of Georgia in the event of a high likelihood or expectation that a materially significant operational loss event is about to occur.
7. The board of directors shall ensure that there is an effective mechanism of information exchange about operational risk events.
8. In order to effectively manage operational risks, managers responsible for overseeing the operational risk function should be of equal stature in relation to the managers of other risk functions.
9. Staff responsible for monitoring and enforcing compliance with the institution's risk policy should have authority independent from the units they oversee.
10. The board of directors shall carry out the identification and assessment of operational risk inherent in all material products, activities, processes and systems to ensure the inherent risks and incentives are well understood.

Article 5. New Product Approval

A commercial bank shall have policies and procedures that address the process for review and approval of new products, activities, processes and systems. The review and approval process must consider:

- a. Advance notification of the National Bank of Georgia prior to the introduction of new products, operations, processes and systems;
- a¹⁾ The Information on whether or not those arrangements are outsourcing arrangements;
- b. The inherent risks associated with new products, services and operations;
- c. resulting changes to the commercial bank's operational risk profile and appetite and tolerance, including the risk of existing products or activities;
- d. the necessary controls, risk management processes, and risk mitigation strategies;
- e. the residual risk;
- f. the procedures and metrics to measure, monitor, and manage the risk of the new product or activity; and
- g. changes to relevant risk limits.

Article 6. Requirements for Information Systems

1. All commercial banks must have policies and procedures that address the adequacy and security of their respective information systems and technology.
2. Information systems policies and procedures must be based on recognized international standards and methodology (i.e. NIST, ISACA, and others).
3. Commercial banks shall implement and possess information systems and technologies that are appropriate to the nature and volume of transactions.
4. Commercial banks must regularly assess and review the adequacy of their information systems based on their respective size and complexity.

5. Commercial banks shall regularly conduct independent information systems audits. Independent information systems audits may either be carried out by a commercial bank's internal audit function (independent internal audit), or by other external, widely recognized/accredited auditing companies that are hired by the commercial bank to perform the aforementioned audits. In addition, in order for the commercial banks to maintain well-functioning and effective business processes, they must pay special attention to, and assess the complexity of their information systems. The aforementioned topic includes the necessity for the existence of proper planning and effective management mechanisms in relation to information systems.
6. Banks are required to develop an information security policy that takes into consideration the organization's information security objectives and strategy.

Article 7. Requirements for Business Continuity Management

1. Commercial banks must have a clear and well-documented business continuity plan in order to achieve a high level of business continuity which will allow the organization to recover in a timely manner in case of an unexpected event or disaster.
2. The business continuity plan must include written policies and procedures which help to ensure the continuity and also detail the commercial bank's response mechanisms to unexpected situations/events and/or major disruptions in the bank's operations.
3. The business continuity plan must include the following components:
 - a. Business impact analysis (oriented towards critical business processes);
 - b. Risk assessment;
 - c. Risk management;
 - d. Risk monitoring;
 - e. Regular testing.
4. Commercial banks shall carry out full and comprehensive business continuity tests at least twice per year.
5. At the end of each year, commercial banks are required to create and submit for approval to the National Bank of Georgia a schedule of planned business continuity tests for the following (upcoming) year.
6. The business continuity plan needs to be reviewed and updated regularly, especially when the organization has undergone significant changes and/or when introduction of new products is planned.
7. The internal audit function (independent audit) must be actively involved in the review and assessment of business continuity and testing processes. The recommendations of the internal audit function that are related to business continuity management must be reviewed and considered and all relevant changes must be incorporated into the business continuity plan in a timely manner.
8. A commercial bank is required to document in detail the results of business continuity tests in both written/material and electronic form.

Article 8. Requirements for Outsourcing Arrangements

1. A commercial bank must notify the National bank of Georgia prior to outsourcing arrangement in a timely manner (at least 14 days prior to initiation of any such arrangement) that is directly related to outsourcing of critical or/and important functions of commercial bank. A commercial bank is required to notify the National Bank of Georgia in a timely manner, at least 14 days in advance, if any outsourced functions are expected to become critical or important in the future.
- 1.¹ Outsourcing means an arrangement of any form between a commercial bank and a service provider by which that service provider performs a critical or/and important process, a service or an activity related to financial services that would otherwise be undertaken by the commercial bank itself. Outsourcing, among other processes, includes cloud services. When using cloud outsourcing services, commercial banks must adhere to the „Guidelines for the Use of Cloud Outsourcing Services by Financial Institutions,” as approved by the order of the President of the National Bank."
- 1.² . Commercial banks should always consider a process, service, or activity or their Third-party information systems and technological infrastructure as critical or important in the situations where a defect or failure in its performance would materially impair:
 - a) Their continuing compliance with the licensing requirements and other obligations defined by the current legislation of Georgia;
 - b) short- and long-term financial resilience and viability, including, if applicable, its assets, capital, costs, funding, liquidity, profits and losses;
 - c) Business continuity and operational resilience of their banking and payment services;
 - d) The protection of data and the breach of confidentiality.
2. Any outsourcing agreement should be conducted in a manner so as not to hinder the ability of Georgian supervisors/regulators to reconstruct the activities of the organization in a timely manner, if necessary.
3. The outsourcing contract must include provision/s that the National Bank of Georgia, as the regulator of the commercial bank, has the right to receive any information associated with or pertaining to the commercial bank, in a timely manner.
4. A commercial bank's use of a foreign-based third-party service provider and the location of critical data and processes outside Georgia must not compromise the National Bank of Georgia's ability to examine the bank's operations. Accordingly, the NBG expects the commercial bank to establish such a relationship in a way that does not diminish the NBG's access to data or information needed to supervise the bank. Outsourcing to jurisdictions where full and complete access to information may be impeded by legal or administrative restrictions on information flows will not be acceptable.
5. Commercial banks are required to carry out an adequate risk assessment regarding the planned outsourcing arrangement, which includes a comprehensive analysis of any, and all available information about the service provider (company) which is accessible to the bank. The risk assessment must, at a minimum, include a thorough review of the latest (most recent) independent financial/information systems audit report, if such document/s exists. If the outsourcing arrangement is conducted with a company that is located outside of Georgia, the commercial bank is required to keep the service provider's audit report on the territory of Georgia. If required, and based on the request from the National Bank of Georgia, a commercial bank must submit the risk assessment, along with the service provider's audit report to the National Bank of Georgia.
6. The bank's business continuity plan must include provisions to ensure timely access to critical information and service resumption in the event of unexpected national or geographic restrictions or disruptions affecting a foreign service provider's ability to provide services.

7. In case if the third party that is responsible for the provision of outsourcing services is not able to satisfy the requirements as set forth in this regulation, the commercial bank will be held liable for non-compliance with the requirements of this regulation, in accordance with Article 30 of the Law of Georgia on the Activities of Commercial Banks.

Article 9. (Omitted)

Article 10. Information Disclosure

A commercial bank shall disclose its operational risk management framework in a manner that will allow investors and counterparties to determine whether the bank identifies, assesses, monitors and controls/mitigates operational risk effectively.