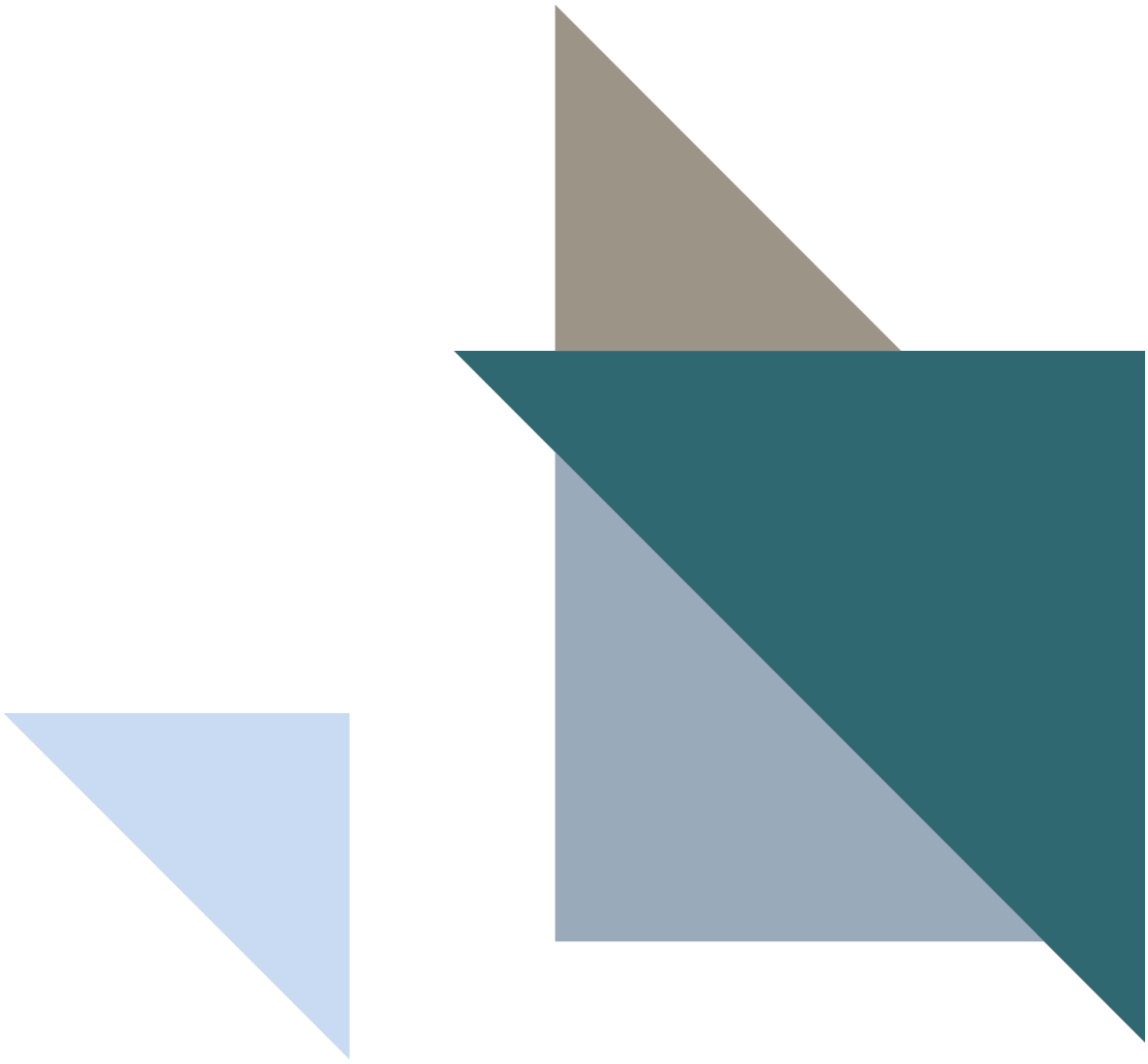
NORDIC INVESTMENT BANK

FINANCING THE FUTURE



Operational Risk Policy

Adopted by the Board of Directors of the Nordic Investment Bank
on 8 December 2022 with entry into force as of 15 December 2022

NORDIC INVESTMENT BANK | FINANCING THE FUTURE

Table of Contents

Responsible Unit(s)/Department(s)

Operational Risk & Security Control Unit / Risk & Compliance Department

Document version history and review dates

Document name	*Adopted by*	*Adopted on*	*Entry into force as of*
Operational Risk Policy	Board of Directors	8 December 2022	15 December 2022

Replaced documents

Document name	*Adopted by*	*Adopted on*	*Entry into force as of*
Operational Risk Policy	Board of Directors	11 February 2021	16 February 2021
Operational Risk Management Policy	Board of Directors	23 April 2015	24 April 2015
Operational Risk Management Policy	Board of Directors	11 December 2008	11 December 2008

OPERATIONAL RISK POLICY

1 SCOPE AND OBJECTIVE

This Operational Risk Policy ("**Policy**") sets out NIB's operational risk management principles and governance structure. The management of operational risk is an integral part of NIB's overall risk management activities and covers all functions of NIB. Operational risk cannot be confined to specific organisational units but is present in all activity. Responsibility for operational risk remains largely with all staff and particularly the unit and department heads or defined process owners.

This Policy sets out the principles for the identification, assessment, monitoring and reporting of all operational risks relating to NIB's activities. The principles of the operational risk management framework are further outlined in the Operational Risk Guideline.

This Policy is under the umbrella of Risk Management Policies ("**RMP**") that provides an overall framework for risk management at NIB as well as high-level principles for risk identification, mitigation and reporting. More specifically, the RMP defines NIB's general risk management principles in the context of mission and strategy, risk-bearing capacity and risk appetite.

2 DEFINITION OF OPERATIONAL RISK AND GENERAL APPROACH

Operational risk can broadly be defined as the risk of direct or indirect losses or damaged reputation due to risk events attributable to technology, people, processes, procedures or physical arrangements and or external events.

The main objective of NIB's operational risk management is to ensure operational resilience, identification and mitigation of operational risks, and accuracy of information used internally and reported externally, a competent and well-informed staff, and its adherence to established rules and procedures as well as on security arrangements to protect the physical and IT infrastructure of the Bank. The Operational Risk Management function also promotes risk awareness in NIB's culture by advising business and support units upon changes in relevant risk policies or providing input for internal training programmes on risk management issues.

3 ROLES AND RESPONSIBILITIES

NIB follows the three-lines-of-defence model, where the first line of defence consists of risk-taking business functions. The business functions are responsible for day-to-day risk management within their business units and are required to comply with the relevant internal policies, regulations and procedures. The second line (Risk & Compliance department) and the third line (Internal Audit) provide oversight, monitoring and audit activities and provide independent evaluations and reporting to the senior management on the adequacy of the Bank's internal control environment.

3.1 Role of the Chairmanship of the Control Committee

The Control Committee is responsible for monitoring that the operations of the Bank are conducted in accordance with the Statutes. Its Chairmanship monitors especially the Bank's financial position, risk levels and capital and liquidity position. Thus, they both oversee that the operational risk management in NIB is well organised and functions properly. For this purpose, the Operational risk management function shall report minimum annually to the Chairmanship of the Control Committee.

3.2 Role of the Board of Directors

The Board of Directors has overall responsibility for the Bank's risk management and oversees the implementation of the Bank's risk management framework, including the operational risk

management framework. Roles and responsibilities are further outlined in the Risk Management Policies.

3.3 Role of the President and the Executive Committee

The President, assisted by the Executive Committee and the Asset, Liability and Risk Committee, is responsible for the management of the risk profile of the Bank in accordance with sound banking principles, the statutory requirements, and the risk appetite as set out in the Risk Appetite Statement (RAS). Consequently, the President is responsible for implementing the operational risk management activities and systems across the Bank and for ensuring that the operational risk management framework as a whole is reviewed and updated when necessary.

NIB's activities and operations are defined as a set of core (and sub-) processes. The President and Executive Committee shall determine NIB's core processes in accordance with section 4.3 and appoint the process owners.

3.4 Role of the Chief Risk Officer

The Chief Risk Officer (CRO) heads the Risk & Compliance department and reports to the President. The CRO is a member of the Executive Committee and the Asset, Liability and Risk Committee, with the role and purpose to ensure that risk considerations are properly taken into account, to influence decision-making and, when necessary, challenge decisions that give rise to material risk.

3.5 Role of the Process Owners

The process owners are responsible for managing operational risk in accordance with this Policy and the Operational Risk Guideline.

Each process (core and/or sub-process), is assigned an owner, who is responsible for monitoring, assessing and reporting risks on a regular basis at the process level, unless more urgent action is called for, and for ensuring that any material changes to and/or observations of the operational risk profile are recorded and fed into the business planning process, as necessary.

All core processes shall be documented and reviewed on regular basis. The documentation shall be on a sufficient level to support the risk identification process and control design. The process documentation is a fundamental tool of internal control and is utilised in the regular risk assessment of the processes as set out in the Bank's risk management framework.

3.6 Role of the Operational Risk Management function[1]

The Operational Risk Management function is responsible for coordinating, monitoring, and reporting on operational risks and for developing operational risk management procedures and methodologies. The Operational Risk Management function shall influence and promote measures to ensure NIB's operational resilience, information security and the accuracy of information used internally and reported externally.

The Operational Risk Management function shall work in close cooperation with other internal control functions, and exchange information as needed. The Operational Risk Management function is headed by the Head of Operational Risk and Security Control. The Head of Operational Risk and Security Control reports to the Chief Risk Officer.

3.7 Role of the Integrity & Compliance function

The Integrity & Compliance function is responsible for overseeing, coordinating and reporting on matters relating to compliance and integrity risks, including any related risk to reputation. Its

[1] The Board of Directors approved amendments to this section in their meeting 17.2.2022

responsibilities cover conduct issues (conflict of interest, misuse of insider information, confidentiality), investigating fraud and corruption as well as coordingating the liaison with relevant external bodies with respect to anti-money laundering and prevention of terrorist financing. The Chief Compliance Officer reports to the Chief Risk Officer, with a dotted reporting line to the President and has unrestricted access to the chairpersons of the Board of Directors and the Control Committee.

3.8 Role of Business Continuity and Security function

The Business Continuity and Security function is responsible for designing, implementing, and monitoring the business continuity, security and crisis management frameworks for the whole organisation. Business continuity shall be managed in accordance with the Business Continuity Guideline. The Business Continuity and Security function reports to the Head of Operational Risk and Security Control.

3.9 Role of the Information Security function

The Information Security function is responsible for policies and security program as well as for overall planning in the area of information security to ensure protection of IT and other information assets. The Information Security function provides guidelines to develop, maintain and monitor processes across the Bank to mitigate information security risks. The Information Security function also performs monitoring activities, provides guidance and is responsible for overall information security awareness. Information security shall be managed in accordance with the Information Security Policy. The Information Security function reports to the Head of Operational Risk and Security Control.

3.10 Role of Internal Audit

Internal Audit is an independent, objective assurance function with reporting lines to the Board of Directors and the Control Committee. Internal Audit provides an independent evaluation of the controls, risk management and governance processes as set out in the Internal Audit Charter. The Internal Audit function shall, without jeopardizing its independence, co-operate with the Bank's Risk & Compliance department in order to have a better understanding of current and evolving key risks. The Internal Audit function shall also independently analyse the work of the Risk & Compliance department.

4 PRINCIPLES FOR OPERATIONAL RISK MANAGEMENT

4.1 General principles

The Bank shall have policies and guidelines that set the operational risk framework of the Bank. These define the roles and responsibilities and set the requirements in the management of operational risk, and provide practical guidance on operations.

NIB shall aim for a risk-based approach to management of operational risk. This means that risks with higher impact will be scrutinised in higher detail than risks with less impact. This approach applies consistently to all operational risks at NIB. NIB shall identify and assess the operational risk inherent in all its activities, processes, products and systems.

NIB applies the three-lines-of-defence model[2] for managing risk. The main principle for organising workflows is to segregate the business-generating functions (1st line) from the recording and monitoring functions (2nd line). Furthermore, NIB shall mitigate operational risk by following rules for the assignment of duties and responsibilities among and within the functions in both the first and second line along with a system of internal control and supervision.

[2] Three-lines-of-defence model as described in NIB Risk Management Policies.

Management of operational risk is to a large extent process-based and NIB mitigates operational risks by defining, documenting and regularly assessing the appropriateness of relevant processes.

The continuous development and upgrading of strategic information and communication systems as set out in the IT Vision and Governance Statement and the Information Security Policy is also an important factor in operational risk mitigation.

4.2 Categorisation of operational risk

NIB shall categorise operational risk according to a risk taxonomy. The risk taxonomy brings a common language and helps to classify different types of risk and operational risk events. The taxonomy is maintained by the Operational Risk Management function.

4.3 Structure to identify and manage operational risks

The Bank's activities and operations shall be defined as a set of core and sub-processes, in which the operational risks shall be identified, reported, followed up and managed. The Operational Risk Guideline provides more specific information regarding the operational risk management framework. To reflect changes in the NIB's operations and/or organisational structure, the defined core and sub-processes might from time to time be amended.

4.4 Risk control guidelines

In addition to this Policy, NIB maintains an Operational Risk Guideline, congruent with relevant international banking standards. The guideline document provides more detailed operational and practical direction and guidelines on operational risk. The Operational Risk Guideline also supports consistent and comprehensive capture of methods to measure and verify the operational risk exposure, as well as to implement appropriate reporting systems and mitigation approaches.

5 NEW PRODUCTS APPROVAL PROCEDURE

Before new products, activities, processes or systems are introduced or undertaken, the operational risks associated must be identified and assessed in accordance with the Rules for New Products and Process Approval.

6 OUTSOURCED ACTIVITIES AND SUPPLIER MANAGEMENT

When considering outsourcing of activities, NIB shall ensure that operational risks related to outsourced services used by NIB are subject to adequate assessment in line with the Rules for New Products and Process Approval. Special attention shall be given to the risks and controls related to the reliability, service quality, continuity and information security of the supplier.

Supplier risk of both outsourced activities and other services provided to NIB shall be subject to regular monitoring and the risk response shall be adjusted accordingly.

Basically, there should be no distinction between the operational risk management responsibilities of in-house managed activities and activities performed by external parties.

7 BUSINESS CONTINUITY MANAGEMENT[3]

NIB shall take adequate measures to recognise and minimise the impact of possible incidents and disruptions. NIB maintains business continuity and crisis management capability as further defined in the Business Continuity Guideline. The business continuity framework shall ensure appropriate crisis management, protection and safety of NIB's staff, physical and intangible assets, and provide

[3] In their meeting 17.2.2022 The Boars of Directors approved this section to be added.

the planning for NIB to be able to maintain critical business function during a disruption, as well as return to normal operations in the shortest reasonable time following a disruption. The business continuity framework shall be reviewed regularly. The guideline shall cover continuity and resilience of all NIB's: i) business, support and control functions and processes; ii) premises and infrastructure; iii) physical and intangible assets; and iv) staff.

8 REPORTING

When reporting to Senior Management, the Chairmanship of the Control Committee and the Board of Directors on operational risk issues, the structures set out in this Policy shall be followed as regards identifying, measuring, categorising, managing and reporting. The operational risks will be reported on a regular basis to relevant governing bodies.

9 IMPLEMENTATION, MONITORING AND REVIEW

The primary responsibility for the correct implementation and monitoring of this Policy shall remain with the Operational Risk & Security Control Unit.

This Policy shall be reviewed at least every three (3) years.