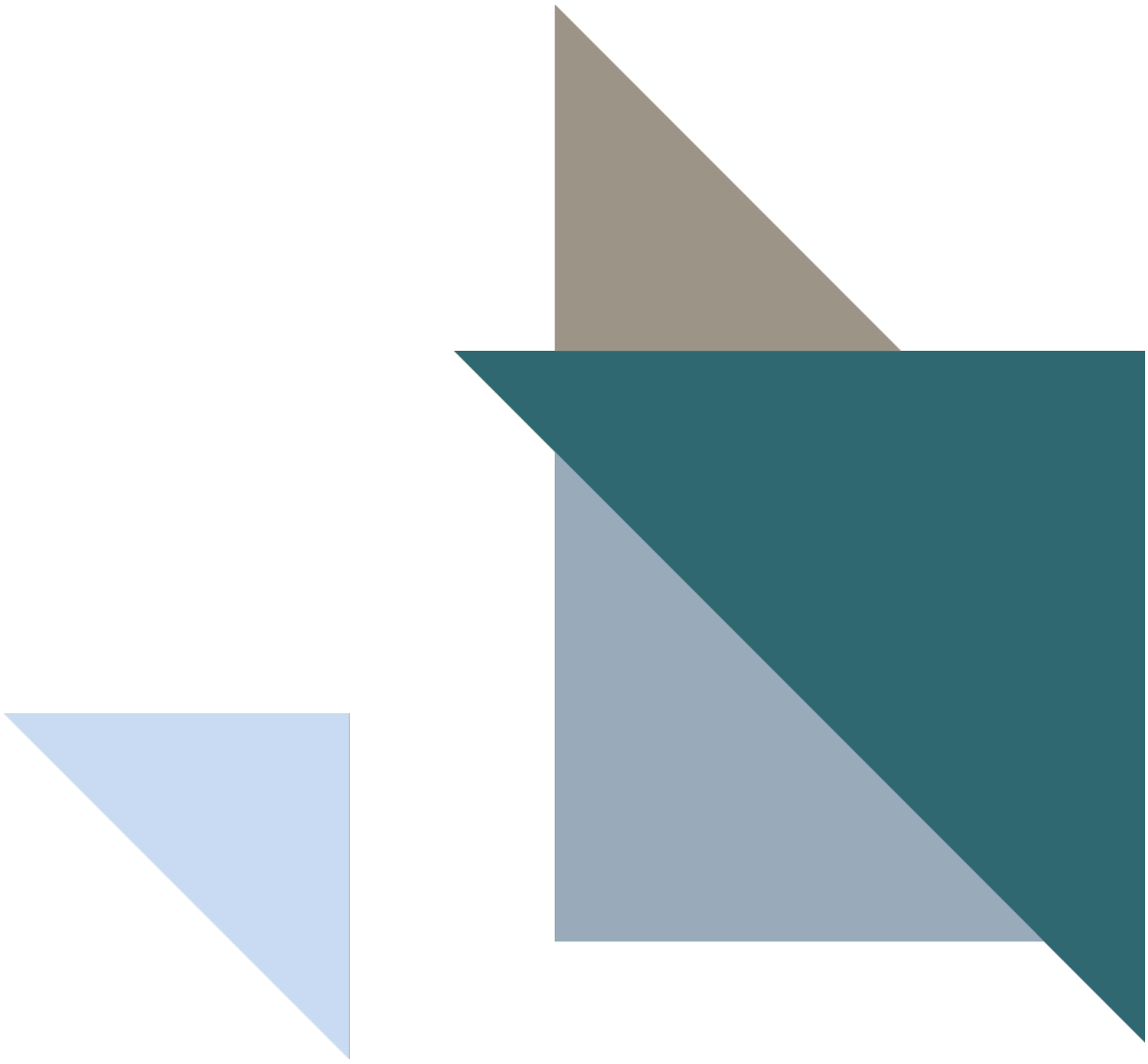
NORDIC INVESTMENT BANK

FINANCING THE FUTURE



Operational Risk Policy

Adopted by the Board of Directors of the Nordic Investment Bank on 29 August 2024 with entry into force as of 3 September 2024

NORDIC INVESTMENT BANK

FINANCING THE FUTURE

Adopted by	Board of Directors
Entry into force	3 September 2024
Adoption date	29 August 2024
Document ownership	Risk & Compliance Department
Implementation responsibility	Operational Risk & Security Control Unit
Control responsibility	Operational Risk & Security Control Unit
Review cycle	At least every three years
Replaced document	Operational Risk Policy of 15 December 2022

NORDIC INVESTMENT BANK | FINANCING THE FUTURE

Table of Contents

OPERATIONAL RISK POLICY

1 SCOPE AND OBJECTIVE

This Operational Risk Policy ("**Policy**") sets out the high-level requirements for managing operational risks and ensuring business continuity during disruptive situations at Nordic Investment Bank ("**NIB**"). The Policy sets the overall requirements for identifying, analysing, reporting on, responding to, controlling and monitoring operational risk exposures. Furthermore, it sets the high-level business continuity management and third-party risk management requirements of NIB. The Policy lays out the roles and responsibilities for the needed activities across first and second lines of defence, in accordance with the three-lines-of-defence model as described in NIB's Risk Management Policy.

2 GOVERNANCE

NIB upholds a sound and effective framework with respect to managing operational risk. This means there are clear lines of responsibility for managing – identification, analysis, reporting, response, control and monitoring – of operational risk. In the NIB operational risk framework, there is a clear separation between the risk-taking units and the control functions. Roles and responsibilities for managing operational risk are described below.

Operational risk management is an inseparable and integral part of NIB's business operations and risk management framework. On an overall level, the Board of Directors, the President and the Executive Committee are accountable for ensuring operational risks at NIB are adequately and effectively managed. The control functions, as stated in Risk Management Policy, are responsible for overseeing NIB's operational risk management and analysing NIB operational risk profile.

3 ROLES AND RESPONSIBILITIES

Operational risk can arise from any of NIB's activities. Therefore, NIB integrates operational risk management into its whole organisation and deems it as a dynamic and iterative process where all departments and personnel play a role.

All employees of NIB are responsible for managing operational risk to ensure NIB stays resilient against internal and external risks and threats. Resilience in this context means NIB is able to stay operational despite an operational risk materialising, uphold a high reputational standing and preserve owner, client and stakeholder trust.

3.1 First line of defence

NIB business units in the first line of defence own the operational risks related to their own activities. This means they are the risk owners of these risks and consequently, they are responsible for managing them. Operationally, Heads of Departments are responsible for ensuring these operational risk management requirements are adhered to in their own Departments. Heads of Departments are also responsible for managing the risks of any services they have outsourced. Finally, they are responsible for business continuity arrangements in their Departments, acting in collaboration with their colleagues across NIB, with the objective of keeping NIB operational during a disruptive event.

Heads of Departments may delegate the responsibility for these activities to process owners or other personnel in their respective organisations. The accountability – i.e. the ultimate responsibility for these activities – cannot be delegated, as is the principle with all management activities at NIB.

3.2 Second line of defence

The Risk & Compliance department is responsible for developing and maintaining a consistent operational risk management framework (including methodologies and related documentation) for managing operational risks and ensuring business continuity.

Operationally, the Operational Risk & Security Control unit ("**OR&SC**"), within the Risk & Compliance department, is responsible for developing the overall requirements for operational risk management at NIB, including third party risk management and business continuity management. OR&SC shall develop and maintain documentation, processes and systems to enable the risk owners to manage their own operational risks in accordance with this Policy. OR&SC provides support and advice to the first line of defence risk owners in risk-related matters and facilitates certain risk management processes as described later in this Policy. OR&SC informs risk owners of risks and provides recommendations for how to mitigate them. To facilitate this, operational units shall provide information to support the identification, management and monitoring of operational risks.

OR&SC informs the senior management of NIB on operational risk exposures and the risk profile of NIB. This is done with relevant and actionable reporting. It is OR&SC responsibility – along with the Risk Management Office and Integrity & Compliance Office for their respective remits – to monitor operational risk across NIB and test the controls designed to mitigate such risks. Finally, OR&SC promotes sound risk culture with awareness training to all staff, or sub-sections of staff, when relevant.

3.3 Third line of defence

Internal Audit provides an independent evaluation of the effectiveness of controls, risk management and governance processes as described in the Risk Management Policy and in accordance with the Internal Audit Charter. Internal Audit evaluations also cover operational risk management.

4 CORE OPERATIONAL RISK MANAGEMENT ACTIVITIES

NIB defines operational risk as the risk of direct or indirect losses arising primarily from products, processes, models, use of technology, misconduct, human error, financial crime or a security breach. Operational risks are defined in NIB Risk Taxonomy.

NIB adopts a risk-based approach to managing operational risk. This means that risks with higher potential impact to NIB business will be scrutinised in higher detail and shall be subject to more control measures than risks with less potential impact. This approach is applied consistently to all operational risks at NIB.

NIB manages operational risk by applying the following core operational risk management activities:

- risk *identification*,
- risk *analysis*,
- risk *reporting*,
- risk *response*,
- risk *control*,
- risk *monitoring*,
- and *business continuity measures*.

The activities and their related risk management methods are not necessarily applied in a sequential manner in practice, but simply presented here in a particular order for illustrative purposes.

5 IDENTIFICATION

5.1 Background

Risk identification is a crucial aspect of NIB's operational risk management. Sources of operational risk that NIB is exposed to need to be identified before they can be managed. Finding risk exposures

requires vigilant employees, constant screening and exploration of systems, applications, processes and the external environment NIB operates in.

5.1.1 Operational risk event reporting

All NIB employees are responsible for informing their immediate manager and OR&SC of operational risk events and/or new risk exposures they have identified. A key element supporting operational risk identification is that all NIB staff are able to report process failures, major vulnerabilities and risk events without this leading to negative personal consequences. NIB management shall ensure a positive risk culture in this regard.

5.1.2 Emerging risk identification

Emerging risk identification is a top-down process for identifying risks, threats and threat themes that may over time develop into more specific risks for NIB business. By identifying and responding to emerging risks, NIB can adapt its strategies, allocate resources in a more efficient manner and protect its operations, reputation and stakeholder interests.

6 ANALYSIS

6.1 Background

At NIB, risk analysis is a key measure in operational risk management. It helps in quantifying the identified risk exposures in terms of their likelihood and harmful impact to the enterprise. Analysis helps in comprehending the nature of risks and their characteristics, which again supports in choosing the appropriate response for each exposure. Analysis helps NIB in taking informed decisions on risk mitigation and ensures the most serious risks are given priority in time and resources are allocated to develop and maintain adequate controls.

6.2 NIB Risk Assessment

NIB's principle way of analysing operational risk exposures is *NIB Risk Assessment*. It is an analysis process that shall be used for identifying and analysing risks in:

- Existing processes and material process changes;
- New products and material product changes;
- New IT systems and applications and their material changes;
- Other material changes in how NIB operates, including significant outsourcing arrangements.

Operational risks, to which NIB is exposed to across the mentioned areas, differ. Therefore NIB Risk Assessment differs based on the prevalent NIB Risk Taxonomy risk types and the asset being assessed. The NIB Risk Assessment types are:

- *Process Risk Assessment*, which aims to gain an understanding of which operational risks NIB is exposed to in its activities and how to best control those risks;
- *Product Risk Assessment*, used to understand the risks and NIB IT system compatibility when launching new products to clients or materially changing existing products; and
- *Change Risk Assessment*, used to capture risks related to new IT systems, applications, significant outsourcing arrangements, process changes and other material changes in how NIB operates.

6.3 Lessons Learned reviews

Operational risk events and other cases with actualised impact or where an impact was close to actualise (a *near miss event*) offer a possibility to analyse and improve processes. NIB promotes an operational risk culture, where the focus is not on who made a mistake, but rather what NIB can learn to prevent similar issues in the future. To this end, Lessons Learned reviews, facilitated by OR&SC, are performed.

6.4 Top Operational Risks method

For getting an overview and proper understanding of NIB's risks on enterprise-wide level as well as the materiality of such operational risks, NIB uses a 'Top Operational Risks' evaluation methodology. The method pools in risk exposures derived from different identification and analysis processes. As a result, the most significant operational risks to NIB are identified and brought to senior management attention for their information and response.

The result of the evaluation helps NIB senior management to compare risks to one another and understand the materiality of operational risks. The method is an enabler for risk scenario analysis, which further refines the impact and severity as well as details the available mitigation strategies for the identified Top Operational Risks.

6.5 Risk scenario analysis

For the most potentially severe operational risks and threats identified, Risk & Compliance facilitates operational risk scenario analysis with quantification means to identify risk impact more accurately. Scenario analysis is conducted to gain an understanding of NIB's ability and preparedness to react to and function effectively in different plausible situations. Scenarios assist NIB in determining exposure to relatively rare, but potentially significant events, including catastrophic or "tail event" type events.

NIB allocates capital to cover unexpected (financial) losses due to, inter alia, operational risk. The capital adequacy assessment is done in line with the procedures and framework as described in the ICAAP Guidelines. Scenario analysis in the context of stress testing is an important method used to support or complement the calculations of operational risk and capital buffer requirements.

7 REPORTING

Reporting operational risk exposures and assessment results to relevant decision-makers and governance bodies of NIB is essential for informed decision-making and oversight of risks. Receiving accurate and relevant information in a timely manner enables NIB management operate in line with risk appetite and take strategic action to mitigate risks.

OR&SC provides an overall report on operational risks at a minimum on semi-annual basis to both senior management and the Board of Directors.

8 RESPONSE

8.1 Background

The purpose of operational risk response is to select and implement the right means for addressing operational risk. Once senior management has been made aware of NIB's operational risk exposures through reporting, it needs to take action and respond to the identified exposures.

As a response to risk, NIB can accept, mitigate or avoid risk. In all cases, the response to risk needs to be informed, meaning senior management is made aware of the risks and the possible consequences of both accepting and mitigating them. Selecting the most appropriate risk response

option involves balancing the potential harm of unmitigated risk with the cost of mitigating it (or avoiding it altogether).

8.2 Response approaches

The risk appetite also for operational risk is set out in the Risk Appetite Statement. In the Risk Appetite Statement, NIB sets the *aggregate level* of all operational risk exposures it is willing to accept in its operations.

In individual instances of risk exposures, the senior management of NIB decides on the response, primarily choosing from the approaches of *acceptance*, *mitigation, transfer* and *avoidance, all* such decisions to be made in accordance with the risk appetite as outlined in the Risk Appetite Statement. A decision that would entail an operational risk exposure beyond the risk appetite, should be avoided. A decision breaching the Risk Appetite Statement is to be reported to the Board of Directors immediately.

9 CONTROL

In the context of operational risk management, a control is an active, risk-mitigating measure put in place by NIB in its processes, products or general operations. Controls help mitigate the likelihood and/or impact of operational risks by preventing and detecting potential impacts. NIB aims to uphold a robust set of *controls* that are actively decided upon by senior management and appropriately mitigate the operational risks identified.

The main types of controls for mitigating operational risks are:

- *Preventive controls*, attempting to prevent risk events from occurring;
- *Detective controls*, aiming to identify risk events; and
- *Corrective controls*, which are processes or other measures activated when harmful events have been detected, to mitigate a risk of harm to future operations.

10 MONITORING

Continuous risk monitoring is an important component of NIB's operational risk management. Monitoring means verifying that the operational risk management framework works as intended. The purpose of risk monitoring is to provide assurance and improve the quality of NIB's operational risk management framework. Risk monitoring may also help in detecting harmful issues early on before they have a significant impact.

Key monitoring approaches include control testing, third-party performance reviews and key-risk indicators.

11 Business Continuity Management

11.1 Background

Business continuity is defined as the capability of the organisation to continue operating and delivering services at acceptable pre-defined levels following a disruptive incident. Business continuity management is a holistic process that identifies potential threats to an organisation's business and support operations, as well as mitigates the potential impact of the threat if realised.

As a main principle, NIB shall maintain business continuity and crisis management capabilities that limit the potential impact of incidents and disruptions with an efficient response and recovery process.

11.2 Key business continuity approaches

11.2.1 Business impact analysis

Business impact analysis is a process for analysing diverse types of impacts over time that the disruption would cause to a defined process or activity, recognise viable alternative delivery methods, define how vulnerable a process is to disruption, determine if a delivery is time-critical for NIB and how long does the owner tolerate the disruption. As a result, a recovery-time objective and recovery-point objective can be defined to ensure adequate recovery and continuity measures and preparedness.

11.2.2 Business continuity planning

Business continuity planning is a process where the outcome from the business impact analysis provides the basis for a planned response to disruption as well as controlled recovery and continuing operations. A business continuity plan is a documented procedure that guides to respond, recover, resume, and restore to a pre-defined level of operation during and after an incident, or a disruption.

11.2.3 IT continuity planning

Information technology working properly is critical for NIB staying operational and being able to operate. NIB maintains a bank-wide IT continuity plan and disaster recovery plan, consisting appropriate recovery process and incident response model of IT infrastructure, services, and IT-systems.

11.2.4 Crisis management planning

A crisis is a situation where NIB's operations widely are under threat due to a critical incident or a prolonged disruption. Crisis management is the NIB-wide strategic level response for addressing a crisis and recovering from it. The Crisis Management Plan is a predefined model and mechanism for responding to and enabling operations during a crisis.

11.2.5 Testing and rehearsing

Individual business continuity scenarios and the crisis management process shall be tested and rehearsed regularly to verify functionality and ensure that the staff is familiar with their roles and responsibilities during an incident or a disruption. The testing shall be focused on the areas where it is recognised to be vulnerabilities or potential for impact to evolve as a wider disruption or crisis.

12 Outsourced activities and supplier management

When considering outsourcing of activities, NIB shall ensure that operational risks related to outsourced services used by NIB are carefully assessed. Special attention shall be given to 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. Monitoring and response means shall correspond to the criticality of the service to NIB and the risk-level the outsourced activity poses.

Critical activities are processes of such importance to NIB that any failure or weakness in carrying them out could have a significant impact on NIB's operational resilience, profitability, or solvency. The decision to outsource critical processes must always be preceded by an overall review of the risks of the outsourcing taking into account the scope and importance of the activity concerned.