Nordea

Group Directive

Document Title **3.1 Policy for Internal Control in the Nordea Group**

25 October 2016 Approval Date

Adopted by The Board of Directors of Nordea Bank AB (publ) ("Group Board") has issued this policy, which was last updated on 25 October 2016.

Information class Internal

Group Directive Responsible Function ("GDRF")	Group Risk Management
Group Directive Content Experts ("GDCE")	Head of Methodology and Risk Assessment, Group Compliance ("GC") and Head of Regulatory Office and Public Affairs Contact: Philip Brackenhoff (GC, Head of Methodology and Risk Assessment), +46 10 1565454 Nicola Oregan (Regulatory Office and Public Affairs), +45 55472171
Applicable	This policy applies to Nordea Bank AB (publ) and, subject to local regulations, to its subsidiaries, including branches and representative offices. Where required for implementation this policy is to be resolved by the board of directors in the subsidiary concerned.
References to external rules	This policy is derived from • Guidelines on the implementation, validation and assessment of Advanced Measurement (AMA) and Internal Ratings Based (IRB) Approaches ("GL10") • Swedish Banking and Financing Business Act (SFS 2004:297) • European Banking Authority (EBA) Guidelines on Internal Governance ("GL 44") • Finansinspektionen's Regulations and General Guidelines regarding governance, risk management and control at credit institutions ("FFFS 2014:1") • Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms ("CRR") • Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms ("CRD IV")
References to internal rules	

The information above related to the GDCE and the references to the external and internal rules is not part of the Group Board's decision and may be amended without involvement of the Group Board. Such amendments may only be made by Group Corporate Law within Group Legal.

1 Purpose and scope

This policy defines the basic principles and the roles and responsibilities for internal control in the Nordea Group ("Nordea" or the "Group").

All employees of Nordea, including non-permanent staff working on behalf of the Group, are subject to this policy.

It is the responsibility of each manager to ensure that this policy is where relevant known and conformed to within his/her respective area of responsibility.

2 Definitions

2.1 Internal control:

Internal control framework

The components of the internal control framework are:

- control environment;
- risk assessment;
- control activities;
- information and communication; and
- monitoring (including reporting of findings and deficiencies).

It creates the necessary preconditions for the whole organisation to contribute to the effectiveness and the high quality of internal control.

It is based on clear definitions, assignments of roles and responsibilities, common tools and procedures and is expressed in a common language.

Control environment

The control environment is the foundation of an effective internal control and includes the following elements:

- values and management culture;
- goal orientation and follow-up;
- a clear and transparent organisational structure;
- segregation of duties;
- the four-eyes principle;
- quality and efficiency of internal communication; and
- an independent evaluation process.

Internal control process

The internal control process is the process carried out by personnel within Nordea, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- prudent conduct of business;
- adequate control of risks;
- effectiveness of operations;
- reliability of financial and non-financial reporting;
- compliance with external and internal regulations;
- adherence to relevant decisions and procedures on all the levels within Nordea; and
- safeguarding of assets, including sufficient management of risks in the operations.

2.2 Lines of defence:

First line of defence: Consist of all Business Areas ("BA") and all Group Functions ("GF") that are neither in the 2nd nor in the 3rd Line of Defence ("LoD").

Second line of defence: Consist of Group Risk Management ("GRM") and Group Compliance ("GC"), which are Nordea´s 2nd LoD independent control functions.

Third line of defence: Consists of Group Internal Audit ("GIA"), which is Nordea´s 3rd LoD independent control function.

2.3 Control functions:

Group Control Functions The 2nd and 3rd LoD are collectively referred to as Group Control Functions.

Independent control function[1] In order for the Group Control Functions to be regarded as independent the following conditions should be met:

a. staff of the function shall not perform any tasks that are included in the operations they are to monitor and control;
b. it shall, in organisational terms, be separate from the functions and areas it is to monitor and control;
c. the person responsible for the control function shall regularly report directly to the board of directors and attend board meetings at which the area of responsibility or reports of the function in question are addressed; and

[1] As defined in FFFS 2014:1, chapter 6, section 6

d. the method for establishing remuneration for the staff of the control function shall not be devised such that it jeopardises or could perceivably jeopardise the objectivity of the staff.

2.4 Model typology[2]:

Business Model These models' primary purpose is to serve a business need (e.g. pricing and hedging models, budget and forecasting models[3], decision models, marketing response models etc.).

They can also have a secondary risk purpose by being feeder models providing inputs to risk models (prepayment models, ALM balance sheet models etc.)

Risk Model These models' primary purpose is to serve a risk management or control need (assessment of risks, limit setting, minimum capital requirements, minimum liquidity requirements etc.)
They include e.g. models for limit setting, capital purposes (stress testing, rating and scoring, loss forecasting, VaR models) etc.
They can also have a secondary business purpose (e.g. capital management, risk budgeting and allocation etc.)

3 Roles and Responsibilities

The Group Board is ultimately responsible for ensuring that an adequate and efficient internal control framework is established and maintained within the Group. Furthermore, they are to ensure that Group Directives, supporting internal rules and necessary limits are adopted for the risks associated with the central areas of the Group's operations.

The President of Nordea Bank AB (publ) and Chief Executive Officer of the Group ("CEO") is responsible for developing and maintaining an effective internal control within the Group and for regular assessments[4] of the effectiveness of the internal control process.

All head of units reporting to a member of Group Executive Management ("GEM") are responsible for ensuring proper internal control in the unit, for reporting on a regular basis (at least annually) on the quality of internal control to the closest

[2] See further Appendix 1.
[3] Including models for stress- and scenario testing as needed.
[4] See section 2 j) in the *"Instructions for the President of Nordea Bank and Chief Executive Officer of the Nordea Group"*.

superior and for annually reporting the status of operational risk within the unit to Group Operational Risk ("GOR").

Each manager is obliged to report to GC on core compliance risks and deficiencies that are prevalent or could arise.

Each employee is responsible for complying with external regulations, Group Directives and the supporting internal rules. Violations are considered as serious breaches and shall be dealt with through a formal disciplinary process. In particular, staff in first line of defence is responsible for risk management, for operating their business and maintaining a high competence within their respective area of responsibility. They shall carry out their preventive, detective and mitigating activities including effective implementation of internal control frameworks.

4 Governance principles, LoD mandates and Group Board oversight

4.1 Governance principles

The primary governance principle is the adherence to the three LoD model ("3LoD") which forms the basis for a clear division of roles and responsibilities in the organisation.

The following additional principles shall be adhered to when designing internal rules or making governance decisions:

1. a proper 3LoD governance is in place ensuring that the segregation of duties is defined and established between risk management and risk control;
2. 1st LoD is the ultimate risk owner and shall ensure that prudent 1st LoD risk management and controls are in place;
3. 2nd LoD is in place, ensuring independent 2nd LoD risk control and model validation functions;
4. 3rd LoD is in place, ensuring an independent review of the first two LoDs;
5. appropriate information barriers i.e. Chinese Walls are defined and put into practice whenever needed;
6. there are clear reporting and escalation procedures within each LoD.

4.2 Mandates of each LoD

In line with the above governance principles, the mandates for each LoD shall be the following.

First line of defence: Is responsible for its own risk management and for operating its business within limits for risk exposure and in accordance with adopted framework for internal control and risk management.

This covers identifying, assessing, performing quality assurance and reporting of issues related to all material financial and non-financial risks. For credit risk, decisions which determine the level of risks taken should be based on both quantitative and qualitative input as well as macroeconomic environment trends and data. Such assessments shall be formally integrated into material risk decisions.

Second line of defence: The Group's 2nd LoD independent control functions are responsible for providing the framework for internal risk control, by designing relevant processes as well as issuing relevant internal rules.

In doing so they shall: verify effective and efficient operations; ensure adequate control of risks; verify prudent conduct of business; verify reliability of financial and non-financial information reported or disclosed (both internally and externally); and ensure compliance with laws, regulations, supervisory requirements and Nordea's internal rules. For credit risk, decisions which determine the level of risks taken should not only be based on quantitative information or model outputs, but should also take into account the practical and conceptual limitations of metrics and models, using a qualitative approach (including expert judgement and critical analysis). Relevant macroeconomic environment trends and data should be explicitly addressed to identify their potential impact on exposures and portfolios. Such assessments shall be formally integrated into material risk decisions.

GRM and GC define the structure and assessment scales for their respective risk areas and issue guidance on reporting.

The respective Group Control Functions´ in the 2nd LoD responsibilities and mandates are described in more detail in the *"Charter for Group Compliance"* and the *"Charter for Group Risk Management"*.

Third line of defence: GIA is an independent and objective assurance activity who supports the Group Board and GEM in protecting the assets, reputation and sustainability of the organisation. GIA does this by assessing whether all significant risks are identified and appropriately reported by management and the risk functions to the Group Board, its committees and GEM, assessing whether all significant risks are adequately controlled, and by challenging GEM to improve the effectiveness of

governance, risk management and internal controls.

The mandate and responsibilities of internal audit are described in more detail in the *"Charter for Group Internal Audit"*.

A more detailed description of the mandates of each LoD is provided in the Appendix.

4.3 Group Board oversight

All risks in Nordea are included in the Group's planning, monitoring and resource allocation processes, and are monitored by the Group Board and CEO. The risk taxonomy identifies sources of risk within the Group. This includes, but is not restricted to, the following risk types:

- Financial risk, including Credit, Counterparty Credit, Market, Liquidity and Leverage risks;
- Non-financial risks, including Operational and Compliance risks;
- Business and strategic risks;
- Life insurance risks; and
- Model risks.

Specific Group Directives approved by the Group Board, and where relevant the subsidiary boards, cover the definition, the management and the control of these risks. They include in particular the:

- *Charter for Group Finance & Business Control*
- *Charter for Group Corporate Centre*
- *Charter for Group Risk Management*
- *Charter for Group Compliance*
- *Charter for Group Internal Audit within the Nordea Group*
- *Risk Policy for the Nordea Group*
- *Nordea Operational Risk Policy*
- *Credit Policy and Strategy for the Nordea Group*
- *Credit Instructions for the Nordea Group*
- *Nordea Counterparty Credit Risk Policy*
- *Nordea Market Risk Policy*
- *Nordea Liquidity Risk Policy*
- *Instructions for Nordea's IRB approach*
- *Nordea Group Capital Policy*

Risk management and controls within the Nordea Group are based on the Group Board Risk Appetite Statement which annually determines the scope of the operations of the Group, including where applicable:

- the composition and size of the Group's assets, liabilities and capital base;
- the exposure to credit risk including the quality and structure of the credit portfolio;
- the scope and direction of investment activities;

- limits in respect of market risk;
- limits in respect of liquidity risk;
- an apprehension of exposure to operational risk; and
- a view on business and strategic risk.

The Group Board ensure the maintenance of high standard of risk management, which includes the application of available techniques and methodology to its own needs in a cost efficient way. Management of risks is proactive, emphasising training and risk awareness. Risk management efforts are consequently proportional to the risks in question, and risk mitigation is designed based on the Group's risk appetite. Risk management is accepted as a natural part and cost of running the business.

Lastly, Group Board decisions are based on preparations executed by inter alia the Board Risk Committee ("BRIC"), the CEO, the Asset and Liability Committee ("ALCO"), the Risk Committee and on GRM's, GC's and GIA's reporting covering (non-exhaustively) the quality of controls, exposure to financial risks, the level and development of operational risks including events and assessments of threat scenarios.

5 The Internal Rules Framework

The Group Board's and CEO's principal policies and instructions defining the authorities and key responsibilities for themselves and other units are outlined as Group Directives. Supporting guidelines, and routines/standard operating procedures ("SOP") may be issued, within the scope and limits set by the Group Directives, by heads of units, committees and fora within their areas of responsibility. The Group Directives together with guidelines and routines/SOPs constitute the Internal Rules Framework[5].

The Internal Rules Framework shall be adapted to the nature, scope and complexity of the operations, and shall set the overall principles for how Nordea operates. The Internal Rules Framework shall cover all relevant parts of Nordea's business, regardless of whether it is delegated to another party or not, and correspond to regulatory requirements. A clear and comprehensive Internal Rules Framework is essential in order to fulfil regulatory requirements, to otherwise manage the business and for the Group Board and CEO in GEM to govern the organisation of Nordea in an efficient way.

The forum that has adopted an internal rule within the Internal Rules Framework shall regularly, at least once a year, evaluate and update the relevant internal rule. Updates during the year must always be done if material changes take place, e.g. changes related to the operations of Nordea or changes to the relevant regulatory requirements.

[5] See 2.11 Policy for the Internal Rules Framework in the Nordea Group.

Appendix 1

Detailed roles and responsibilities of each LoD

This appendix outlines in more details the roles and responsibilities of the Nordea's three LoDs set out in Section 4.

- **1st LoD** is empowered to take and manage risks within the constraints of the internal rules, external regulations, the risk appetite and other risk limits (i.e. first line of defence is the risk owner). Among the key roles and responsibilities are to:
    - provide input and recommendation on the risk appetite framework to the 2nd LoD;
    - provide input and recommendation on the Group risk frameworks and standards as well as firm-wide methodologies to the 2nd LoD;
    - apply Group risk frameworks and standards as well as firm-wide methodologies in consultation with the 2nd LoD. Develop and implement additional internal rules, if relevant (e.g. internal control policies and procedure descriptions);
    - perform allocation of business limits within risk limits (in line with the Group Risk Appetite Framework) and provide recommendation to the 2nd LoD on the risk limits;
    - design, develop, implement and maintain business risk models[6], where required to complement the firm-wide risk models (which are designed and implemented by the 2nd LoD);
    - conduct (often "day-to-day") operational risk control activities (e.g. compliance with risk limits) in order to *manage and mitigate* the risks;
    - conduct stress- and scenario testing as needed;
    - provide relevant BA specific risk reporting (e.g. on a desk risk level) for the (often "day-to-day") *management* of risks, including necessary mitigating actions;

[6] Business and risk models are defined in section 2.4 and the rational for the split of responsibilities between the LoDs for them are set out in ownership of business and risk models in the 3 LoD framework as described later in this Appendix.

- provide BA specific risk training (if relevant); and
- own data and systems while securing the needs of the 2nd LoD.

- **2nd LoD** includes independent risk oversight and control functions in terms of mandate, resources, organization and reporting lines[7]. Among the key roles and responsibilities are to:
  - design, develop/maintain and recommend Group-wide internal rules as well as methodologies for approval by the Group Board (and subsidiaries Boards). This may happen in consultation with the 1st LoD and in line with the business strategy.
  - prepare and recommend risk appetite framework to the Group Board (and subsidiaries Boards) which may include input from the 1st LoD.
  - design, develop and maintain the Group-wide risk models which may include input from the 1st LoD, or specify, approve and validate risk models developed and maintained in the 1st LoD (c.f. subsection below on *Business and risk mode*l).
  - validate the Group-wide risk models (and other business models, as necessary) under separate reporting lines to the CRO (and audit/external assurance).
  - prepare and recommend risk limits (e.g. on a BA, product, segment level) which may include consultation with 1st LoD for approval by the Group Board (and subsidiaries Boards).
  - set risk limits (e.g. on a BA, product, segment level) to supplement the Group Board (and subsidiaries Board's) limits after consultation with 1st LoD.
  - monitor and control (e.g. through access to 1st LoD controls and sample checks) 1st LoD adherence to regulations, group risk frameworks and the Internal Rules Framework, limits, as well as firm-wide methodologies.
  - perform independent risk assessment, measurement, monitoring, control and challenge of risks taken in the 1st LoD, including:
    - evaluation of trends and new or emerging risks arising from changing circumstances and conditions;

[7] In this policy the split of roles between Group Risk Management and Group Compliance is not described but it states the overall roles & responsibilities for the 2nd line of defence.

  - regular reviews of actual risk outcomes against previous estimates (i.e. back-testing);
  - stress-testing, including both the risk control portion of the ICAAP and ILAAP;

- have a "right of veto" as specified, if needed, in the *"Charter for Group Risk Management"*;
- participate in the credit process as described in the credit risk framework;
- participate in and evaluate the impact of exceptional transactions (e.g. M&A, creation or divestiture of subsidiaries or SPVs etc.) on Nordea's overall risk profile;
- provide independent risk opinions by compiling, analysing and reporting on all risks to GEM, the Group Board and other key stakeholders;
- provide risk and compliance advisory support and training to the 1st LoD [8];
- propose risk mitigation actions to senior management, when appropriate; and
- own data and systems when needed for risk management purposes and while securing the needs of the 1st LoD.

- **3rd LoD** provides independent – from 1st LoD and 2nd LoD - objective and relevant assurance to the Group Board. The primary role of the 3rd LoD is to help the Group Board and GEM to protect the assets, reputation and sustainability of the organisation. It does this by:
  - Assessing whether all significant risks are identified and appropriately reported by management and the risk functions to the GEM, BAC, BRIC and Group Board.
  - Assessing whether they are adequately controlled.
  - Challenging GEM to improve the effectiveness of governance, risk management and internal controls.
  - Other key responsibilities are (not exhaustive):

[8] BRIS organizations may also provide training within their BA or GF.

- Provides summary reports to GEM, BAC and Group Board based on the, by the Group Board, approved annual plan.

- Follows up and reports on actions planned to address the audit issues.

In order to secure good cooperation and coordination between the 1st LoD and 2nd LoD, Nordea has established a number of group wide committees (i.e. Risk Committee and its sub-committees).

Ownership of business and risk models in the 3 LoD framework

Nordea defines its models in one of two categories of Business models or Risk models in (see section 2.4 above). As stated above in this appendix business models are developed and maintained in 1st LoD and validated in the 2nd LoD if deemed relevant by the 2nd LoD. Risk models shall be developed, maintained and validated in the 2nd LoD or alternatively specified, approved and validated by the 2nd LoD while they are developed and maintained by the 1st LoD.

The latter option for risk models is meant to cater for models that have both an equivalently legitimate business and risk purpose (for e.g. ALM models for non-maturing deposits, models for loans or deposits behavioural characterisation, etc.) whose ownership needs to rest within the 1st LoD but whose design need to be controlled by the 2nd LoD.