Nordea

Group Directive

Document Title **3.2 Nordea Operational Risk Policy**

Adopted by The Board of Directors of Nordea Bank AB (publ) ("Group Board") has approved this policy, which was last updated on 15 June 2016.

15 June 2016 Approval Date

Information class Internal

Group Directive Responsible Function ("GDRF")	Group Risk Management ("GRM") is the Group Directive Responsible Function for this Group Directive.
Group Directive Content Experts ("GDCE")	Group Operational Risk ("GOR") is Group Directive Content Expert for this Group Directive Contact: Chief Operational Risk Officer Søren Thorius Andresen, +45 55473469
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. Amendment as to separate jurisdictions are enclosed as Appendix 1(Amendment Appendix)
References to external rules	This policy is derived from • 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) • Finansinspektionen's Regulations and General Guidelines regarding the management of operational risks (FFFS 2014:4)
References to internal rules	This policy is derived from • 2.6 Charter for the Group Risk Management • 3.1 Policy for Internal Control and Risk Management in the Nordea Group

The information above related to the Contact, the Group Directive Content Expert, 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.

1 Purpose and scope

This policy sets out the general principles for operational risk management within Nordea ("Nordea" or the "Group"), as well as the responsibilities of the 1st Line of Defence ("LoD") for the management of operational risk and the responsibilities of the 2nd LoD function Group Operational Risk ("GOR") for the independent risk oversight and control of operational risk. The policy forms part of the risk management and internal control framework, and is the overarching policy for all other policies, guidelines and instructions that define the Group's Operational Risk Management framework.

The below sections of the Operational Risk Policy are structured as follows:

- Definitions: Description of how operational risk is defined within the Group.
- Roles and responsibilities: Definition of main roles across the three LoDs and within GOR and the respective responsibilities that ensure an adequate and comprehensive management of operational risk in the Nordea Group.
- Nordea Operational Risk Management framework: Description of Nordea's framework to effectively and efficiently manage operational risk; including definition of the main operational risk management processes.

2 Definition of operational risk

Operational risk in Nordea is defined as follows: "The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events, and includes legal risk."[1]

The risk of loss includes direct or indirect financial loss, and impacts from regulatory sanctions, legal exposure, reputational damage and critical business process disruption.

Nordea acknowledges that the bank cannot operate without accepting a reasonable exposure to operational risk; however, this acceptance of operational risk has to always remain within the boundaries of Nordea's risk appetite. Therefore, Nordea regards risk strategy and appetite as a key component of the risk management framework and ensures that it is embedded into decision-making and business processes, see further section 4.1 below.

[1] Article 4.1 (52) of Regulation (EU) No 575/2013 of the European Parliament and Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012,1

Operational risk is inherent in all activities within the organisation, in outsourced activities, and in all interactions with external parties. Nordea uses a Risk Type Taxonomy to further specify the possible operational risk events.

Only regarding capital requirements, operational risk also covers compliance risk.

3 Roles and responsibilities

3.1.1 The Group Board

The Group Board regularly reviews and decides on the internal rules for operational risk management for Nordea, and is responsible for issuing and regularly updating this policy.

The Group Board also decides and regularly reviews the operational risk strategy and appetite, as well as regularly evaluates whether Nordea effectively and appropriately controls and manages its operational risks.

3.1.2 Three Lines of Defence

Nordea has defined its overall operating model for the three lines of defence in a set of core principles. In terms of operational risk management these principles are in particular:

- *First Line of Defence*, which is composed of the Business Areas and Group Functions, is accountable for all operational risks related to its activities across all countries and legal entities. As risk owners, the 1st LoD is responsible to manage those operational risks, i.e. proactively identifying, assessing, mitigating, monitoring and reporting the risks, according to the Operational Risk Management framework defined by the 2nd LoD.

  In order to ensure an adequate setup in the 1st LoD, each Business Area and Group Function must contain a "Business Risk Implementation Support" ("BRIS") unit to support the implementation and application of the Operational Risk Management framework.
- *Second Line of Defence* is an independent risk oversight and control function. It is responsible for developing and maintaining the Operational Risk Management framework and for supporting, challenging and controlling the implementation of the framework by the 1st LoD and to independently assess, monitor, and report on 1st LoD risks and controls.
- *Third Line of Defence,* the internal audit function, is an independent and objective assurance activity who supports the Group Board and Group Executive Management (GEM) in protecting the assets, reputation and sustainability of the organisation. Group Internal Audit 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.

3.1.3 Operational Risk monitoring and control in the 2nd LoD

GOR, which is a division within Group Risk Management ("GRM"), represents the 2nd LoD for operational risk management. The Chief Operational Risk Officer ("CORO") is the Head of GOR.

GOR is responsible for developing and maintaining the Operational Risk Management framework, i.e. the policies and procedures for managing operational risks, and for supporting, challenging and controlling the implementation of the framework by the 1st LoD. GOR also advises and provides an independent view of the operational risks, and independently monitors, challenges, controls, and reports the operational risks and operational risk management activities of the 1st LoD.

3.1.4 Main roles

Two main roles exist within GOR, each of them with a different set of objectives and responsibilities as follows:

Operational Risk Officers

The Operational Risk Officers ("OROs") advise the 1st LoD business on all aspects of operational risk management, provide their documented independent view on main operational risks, and independently monitor, challenge, control, and report on the operational risks and operational risk management activities of the 1st LoD. With the exception of specific Legal Entities, the ORO role is a function located within the 2nd LoD. The term ORO should in general not be used to describe risk management functions outside of the 2nd LoD.

The role of the ORO is adapted to the activities of the relevant business unit, its size and resources. The OROs are organised in GOR and staffed in a sufficient and appropriate way to ensure that they can adequately perform their duties. Because effective control of an entity is only possible based on understanding and knowledge of that entity, the ORO shall have a very good and up-to-date understanding of and familiarity with the 1st LoD divisions the ORO is responsible for.

The role and responsibilities of the OROs are detailed further in the "Guidelines for the Operational Risk Officer (ORO) work" issued and maintained by the Chief Operational Risk Officer.

Risk management framework as well as methodology development and maintenance

GOR is responsible for defining the operational risk strategy and appetite as well as administering the periodic review of the operational risk strategy and risk appetite proposed by the CORO to the Group Board and relevant subsidiary Board of Directors for decision.

GOR is also responsible for developing, maintaining and deciding the Operational Risk Management framework consistent with regulatory requirements which specifically include the elements of the Operational Risk Management framework common to both 1st LoD and 2nd LoD for example, defining standards for identifying, assessing, mitigating, monitoring and reporting operational risks.

GOR establishes the 2nd LoD operational risk reports for all Business Areas and Group Functions, and distributing to all relevant internal and external stakeholders, including regulatory authorities.

GOR also supports and advise on the implementation of the Operational Risk Management framework in the 1st LoD, which includes providing the enterprise wide systems and tools for operational risk management.

3.1.5 Status and Independence

GOR and, in particular, the OROs are to be independent. They must consequently:

1. Not be responsible for performing services or activities they monitor and control or at all be placed in a position where there is a possible conflict of interest between their risk control responsibilities and any other responsibilities they may have;
2. In organisational terms be, in general, separate from the functions and areas they monitor and control;
3. Regularly report to the Group Board directly or via the Chief Risk Officer;
4. Not receive remuneration devised such that it jeopardises or could perceivably jeopardise their objectivity.

The staff of GOR, and in particular the OROs, shall be authorised to communicate with any staff member and obtain all information required to perform their duties and shall have the right to conduct investigations of possible breaches of policies. They are to operate free from interference in performing their work and in communicating its results and as such must:

- Have the status, authority and integrity to challenge actions or persons;
- Follow up on concerns and achieve a satisfactory solution;
- Have access to all information within their respective areas of responsibility including staff, records, paperwork and meetings of the units;
- Have direct and unfettered access to the appropriate senior level of management in the units within their respective areas of responsibility; and
- Have the authority to freely express and make known findings and opinions by using available reporting routines.

Staff in GOR shall have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their specific duties and a sound understanding of relevant laws, rules and standards and their practical impact on the Group's operations.

Head of GOR shall ensure that no OROs have a salary with variable elements, such as VSP or bonus.

3.1.6 Delineation of responsibilities between GOR and GC

Group Compliance and GOR, as the two 2nd LoD functions within the Nordea Group managing compliance and operational risks, work together in a collaborative manner to ensure that there are no gaps and minimal overlap.

Responsibilities across Group Compliance and GOR shall be allocated through an activity-level delineation approach based on a risk type taxonomy, to delineate areas with subject matter expertise between Group Compliance and GOR, thereby establishing a 2nd LoD primary and secondary control responsibility. This implies that for each of these areas, the primary responsible is in charge of covering a specific set of responsibilities, whereas the secondary responsible (not precluding any regulatory obligations) covers other responsibilities so that all regulatory requirements are covered. Additionally, there are activities for which either Group Compliance or GOR are responsible across the risk type taxonomy. Delineation guidelines are established and maintained jointly by Group Compliance and GOR, and decisions related to the delineation are made in the Non-Financial Risk Committee.

4 Nordea Operational Risk Management Framework

As outlined in section 3, the 1st LoD is responsible to manage the operational risks according to the Operational Risk Management framework defined by the 2nd LoD and approved by the Group Board.

4.1 Risk strategy and appetite

The operational risk strategy and appetite for the Group is defined and prepared by GOR as part of the overall Group Risk Appetite Statement for approval by the Group Board and relevant subsidiary Board of Directors. The operational risk strategy is established to reflect the business model, geographical areas, competitive situation and risk culture of Nordea. Nordea's operational risk strategy aims at protecting profit, maintaining a solid balance sheet and capital position, and maintaining the trust of Nordea's key stakeholders (e.g., clients, shareholders, employees and the broader society).

The Group Risk Appetite Statement ("RAS") determines the level of operational risk Nordea is willing to tolerate when conducting its activities. The RAS determines that Nordea does not tolerate (i) a too high overall risk level, (ii) an unfavorable development of top risks, (iii) a breach of the financial appetite for operational risk losses, and (iv) material breaches of risk indicators.

Nordea defines its Risk Appetite Framework ("RAF"), which provides the necessary theoretical and practical elements to articulate the RAS. The RAF is based on qualitative and quantitative measures to establish respective limits, and defines consequence management procedures to ensure that management takes action in case of breaches, and provides the mechanisms to ensure timely and accurate reporting to top management.

Nordea regularly reviews and, if necessary, updates the RAF, including the selected use of risk indicators, in order to reflect the nature, scope and complexity of the operations.

The operational risk RAS and RAF are detailed further in the "Guidelines for the Operational Risk Appetite Strategy & Framework" issued and maintained by the Chief Operational Risk Officer.

4.2 Governance and organization

4.2.1 Committees

Nordea has established a committee structure for non-financial risk management. The relevant committees include:

- The Risk Committee, which ensures a comprehensive view of both financial and non-financial risks. The committee is chaired by the CRO and CORO participates in this committee, providing the operational risk perspective, see "Charter for the overall Committees and Forum in the Nordea Group".

- The Non-financial Risk Committee is established as a subcommittee of the Risk Committee in order to ensure the maintenance and further development of an effective risk management framework, a comprehensive overview of all non-financial risks, to resolve potential differences between the 1st and 2nd LoD, and to ensure close coordination between GOR and Group Compliance The committee is composed of the heads of GOR and Group Compliance (co-chairmen) as well as the BRIS coordinator, see "Charter for the Non-financial Risk Committee ".

- 1st LoD Non-Financial Risk Committees, organized per Business Area and Group Function, chaired by 1st LoD senior management and with participation from both GOR and Group Compliance to advise and challenge the 1st LoD and to provide an independent view. See the "Charter for the BA/GF Business Risk Forum".

4.3 Management and control of operational risks

As part of the Operational Risk Management framework, GOR defines several key operational risk management and control processes that are described in the following sections. For these processes, GOR is responsible for issuing and maintaining more detailed instructions or guidelines, while the 1st LoD is responsible for implementing

the processes in order to adequately and consistently manage and control operational risks.

4.3.1 Risk and Control Self-Assessment

The Nordea Risk and Control Self-Assessment ("RCSA") process aims to develop a comprehensive and standardized overview of all the operational and compliance risks and controls across the Nordea Group to improve risk awareness, and to enable effective assessment, control, and mitigation of the identified risks. Through well-prepared and structured RCSA workshops, the Group's material risks are identified, the existing controls evaluated, the remaining residual risks assessed and for each risk a decision is made on mitigations, acceptance, transfer and change of strategy.

The 1st LoD, as risk owner, is responsible for preparing and running the RCSA workshops, identifying and assessing risk and controls, defining and documenting mitigating actions for key risks and aggregating reports on a divisional and Business Area and Group Functions level. The 1st LoD should also ensure the accuracy and completeness of the RCSA, sign off results and initiate and follow up mitigating actions as required.

The 2nd LoD is responsible for participating in the RCSA workshops to advise and challenge the 1st LoD, validating the 1st LoD risk and control inventory and assessment, and providing an independent view on the assessment carried out by the 1st LoD.

The RCSA process is detailed further in the "Instructions on the Operational Risk Assessment process" issued and maintained by the Chief Operational Risk Officer.

4.3.2 Scenario Analysis

Scenario Analysis is a tool used by Nordea to facilitate a deeper understanding of identified tail risks and gaps in the existing control infrastructure. Scenario Analysis ensures a better understanding of the operational risk environment and additionally allows participants to develop a view on and familiarize themselves with extreme impact risks observed in peer institutions that have so far not materialized in the Group.

The 1st LoD is responsible for organizing and running Scenario Analysis workshops, ensuring all the required resources are in place (participants, content, pre-read material, etc.) and documenting and signing off workshop outcomes.

The 2nd LoD is responsible for challenging and providing advice to the 1st LoD regarding all aspects of the scenario analysis and for ensuring the adequate implementation of the defined standards while coordinating the process and providing an independent assessment of the workshop outcome.

The Scenario Analysis is detailed further in the "Guidelines for Scenario Analysis" issued and maintained by the Chief Operational Risk Officer.

4.3.3 Incident Reporting

Incident Reporting is the process defined to analyse and follow-up on incidents in the Group. All incidents shall be reported in line with the standards defined by GOR regarding incident reporting. Incidents are dealt with immediately to minimise the damage and are reported to the immediate superior, to the relevant ORO and to other relevant staff and support functions upon detection. GOR in co-operation with GL and GC ensure that relevant authorities are informed in accordance with applicable regulations on reporting of events of material significance. Crime or suspected crime against the Group is reported to the police. The 1st LoD is responsible for the proper handling, documentation and reporting of incidents and for ensuring quality of the captured data.

The Incident Reporting process is detailed further in the "Instructions on Incident Reporting in Nordea" issued and maintained by the Chief Operational Risk Officer.

4.3.4 Change Approval Governance (including product approval)

Change Approval Governance defines the process and documentation requirements for the approval of new or materially altered products, services, markets, processes or IT systems or major changes to the operations or the organisation. These requirements are put in place to ensure sufficient financial and operational risk management when planning and implementing changes. Product approval is a particularly important process, which is included in the Change Approval Governance. If the change involves engagement with a third party, appropriate risk management actions should be undertaken in accordance with the defined standards for third party risk management. Change approval uses the mandatory Quality and Risk Analysis ("QRA") tool to adequately document major changes (see next section).

The 1st LoD, as change owner, is responsible for driving the process, including the materiality assessment. The 1st LoD is also responsible for maintaining up to date documentation of the material change and ensuring that all required resources are in place (sufficient employees, support tools, controls, etc.). The OROs are included as mandatory stakeholder during approval processes for material changes to advise and challenge the 1st LoD and provide an independent view.

The change approval process is detailed further in the "Instructions for approval and documentation of new or materially altered products, services, markets, processes, IT systems and major changes to the operations and organisation in the Nordea Group" issued and maintained by the Group Board.

4.3.5 Quality and Risk Analysis

The QRA is used in Nordea to limit new risks and to ensure disciplined change management. It aims at documented decision-making regarding risk and quality aspects connected to changes, explicit responsibility for decisions and actions taken, and a systematic follow up. QRA is a widely used tool to document all changes within the Group, but it is particularly important to highlight the QRA as a key mandatory component of above outline Change Approval Governance.

The 1st LoD, as QRA owner, is responsible for ensuring that all required changes go through the QRA process and that the process is executed, documented and followed-up as required.

The QRA process is detailed further in the "Guidelines on Quality and Risk Analysis (QRA)" issued and maintained by the Chief Operational Risk Officer.

4.3.6 Business Continuity and Crisis Management

Business Continuity and Crisis Management ("BC & CM") are processes defined to ensure that the Group builds and maintains the appropriate levels of resiliency and readiness for a wide range of expected and unexpected operational and financial risk events. Business Continuity requires pre-considered measures and actionable steps to be taken in preparation for unexpected and disruptive events. Crisis Management provides the capability to execute our plans and to respond to an unforeseen event or disruption in a controlled and coordinated manner.

It is the responsibility of the 1st LoD to ensure the execution of the BC &CM processes in accordance with the framework requirements.

The BC & CM framework is detailed further in the "Business Continuity and Crisis Management Policy for the Nordea Group" issued and maintained by the Group Board.

4.3.7 Information Security

Information security is defined as the protection of information in respect of confidentiality, integrity and availability. Information refers to all information processed, stored, used or transmitted in any medium or form, including electronic, physical and verbal. Information Security processes are designed to

- Protect information against accidental or malicious disclosure, modification, or destruction;
- Meet regulatory, legislative and contractual requirements concerning information security; and
- Maintain availability of information.

The Information Security processes are detailed further in the "Information Security Policy for the Nordea Group" issued and maintained by the Chief Operational Risk Officer.

4.3.8 Legal risks

Nordea's definition of operational risk includes legal risks connected to operational risk events, as potential legal actions connected to operational risks can cause financial losses or other damages to Nordea. Therefore, all elements of the Operational Risk Management framework also support the management of those legal risks. Nordea manages legal risks through the following key activities and processes:

- New Product Approval to ensure decisions regarding new products take into consideration the risks of disputes and legal action, see further section 4.3.4 above;
- Third Party Risk Management to ensure appropriate risk management of Nordea's outsourcing activities, see further section 4.3.4 above;
- Divisional management is responsible to ensure that its operational comply with laws, statutes and other regulations and for seeking legal advice when needed. Group Compliance is responsible for providing an independent view on compliance to rules and regulations applicable to the Group, and by contributing to an effective and efficient compliance risk management[2];
- Divisional management is responsible to ensure and follow-up the accuracy and validity of contracts entered into or other legal documents concluded and for seeking legal advice when needed;
- Archiving to ensure all legal documentation is handled and stored in an adequate manner, see further section 4.6 below;
- Dispute handling to ensure an effective and efficient process to manage and follow up legal processes[3].

Legal advice is provided by Group Legal[4] or in-house lawyers in specific legal entities. In addition, in specific legal areas/jurisdictions legal services are provided by external lawyers.

4.3.9 Raising Your Concern

Raising your concern sets out the required procedures to encourage all Nordea employees to transmit their concerns regarding the conduct of operations in accordance with internal rules and instructions as well as with applicable laws and regulations. An employee having a concern that this is not done by staff or managers

---

[2] "Nordea defines compliance risk as the risk to fail to comply with laws, regulations, rules and prescribed practises and ethical standards, governing Nordea's activities in any jurisdiction, which could result in material financial or reputational loss to the Group, regulatory remarks or sanctions" (2.9 Charter for Group Compliance)

[3] See *"Instructions on handling of disputes in the Nordea Group"*.

[4] Group Legal ("GL") is a centralised division within the Chief of Staff Office providing Nordic legal services in order to support the business and support BAs and GFs to identify and handle legal risks. GL provides legal advice applying Nordic rules and regulations in core legal areas. GL does not provide legal services in relation to external customers and does not apply e.g. HR law (except from Nordea Bank Norge), tax law, accounting and reporting regulations. Further capital and liquidity regulations are areas where the main responsibility stays with other GFs. GL thus serves mainly the Nordic operations. As regards specific legal entities and non-Nordic operations, legal services are not provided by GL but by local in-house lawyers employed within the relevant unit and/or by external lawyers.
GL and local legal units in specific legal entities and the non-Nordic operations are to be organised and staffed in a sufficient and appropriate way, and when needed external legal advice should be retained, in order to support the Group's business operations and in order to support that legal risk within the Group is effectively managed.

or others that are acting on behalf of the Nordea Group is encouraged to come forth and voice his/her concerns in accordance to the defined processes.

It is the responsibility of OROs to receive raised concerns within their respective area of responsibility in accordance with defined standards and to proactively support managers and employees in activities and questions related to Raising Your Concern.

The Raising Your Concern process is detailed further in the "Raising your concern instructions" issued and maintained by the president of Nordea Bank AB (publ) and Chief Executive Officer of the Nordea Group ("CEO") in Group Executive Management ("GEM").

4.4 Risk Culture

Risk culture drives behaviours that determine collective risk taking and the ability to understand, and act on the organization's current and future risks. In order to manage operational risk, a common set of standards and a sound risk culture is essential as is to follow best practice regarding market conduct and ethical standards in all business activities.

The board of directors of the Nordea Group as well as the senior management should take the lead in establishing a strong risk culture that supports and provides appropriate standards and incentives for professional and responsible behaviour.

In order to ensure a sound risk culture, all employees are expected to support a culture of:

- Risk transparency: a culture in which communication is effective regarding current and emerging risks across the organisation and in which leadership has communicated a clear risk appetite, leading to an organisation which understands the risk it is running;
- Acknowledgement of risks: a culture in which individuals challenge each other, management and employees feel empowered and open to passing on bad news and learning from mistakes, and feel confident about the superior risk position that a strong risk culture enables
- Responsiveness: a culture in which the organisation identifies external changes and reacts rapidly to them and a culture which instils a responsibility to react to situations and care about the outcome
- Respect: a culture of cooperation among individuals and organizational units and a culture where people's risk appetites are aligned

Both 1st and 2nd LoD are responsible for promoting operational risk culture as an effective ambassador and carrier of the defined culture. Both LoDs should actively work to maintain and further develop a strong operational risk culture where business activities are performed in line with the Nordea values and the risk culture. In a proactive manner, both LoDs should support managers and employees in activities to ensure a strong risk culture.

4.5 Reporting

It is the responsibility of the 1st LoD to adequately report on all material risks, controls, and mitigating actions and to provide access to the 2nd LoD to all the relevant 1st LoD reporting in order to ensure all reports are reviewed and challenged.

GOR shall regularly and independently report on material control deficiencies and risks. The reports shall follow up on previously reported deficiencies and risks, and describe each newly identified material deficiency and risk. The reports shall also include a consequence analysis and a recommendation for measures. The relevant stakeholders shall, as soon as possible, take appropriate measures as response to the GOR reports. Reporting is done to the Group Executive Management ("GEM") and the Group Board or relevant Group Board committee.

The operational risk reporting is detailed further in the "Guidelines for the Operational Risk Reporting" issued and maintained by the Chief Operational Risk Officer.

4.6 Archiving

Each head of unit within the Group is responsible for ensuring that all legal and contractual agreements and relevant supporting material are archived in accordance with laws, regulations and internal rules.

The archiving processes and requirements are detailed further in the "Instructions for Archiving" issued and maintained by the Chief Operational Risk Officer.

4.7 Capital Estimation Model

Nordea follows the framework outlined by the Basel Committee on Banking Supervision for calculating operational risk capital charges. Currently, Nordea applies and follows the criteria defined for the Standardised Approach. This approach entails dividing the banks main activities into relevant business lines as stipulated in the framework. Within each business line, gross income is a broad indicator that serves as a proxy for the scale of business operations and thus the likely scale of operational risk exposure within each of these business lines. The capital charge for each business line is calculated by multiplying gross income by a factor assigned to that business line.

Nordea continuously investigates the appropriate steps towards developing more sophisticated operational risk measurement systems and practices in order to move along the spectrum of available approaches in accordance with the operational risk capital charge frameworks.

4.8 Policies and procedures

The Operational Risk Policy is part of the risk management and internal control framework of Nordea. The policy is the overarching policy for all relevant Operational Risk policies, instructions, and guidelines that are defining Nordea's Operational Risk Management framework.

4.9 Systems and tools

Systems and tools are put in place to support and enable operational risk management. Systems and tools shall not only be user friendly to enable an efficient and effective usage, but also aim towards a consolidated landscape that allows building an aggregate view on risk and sharing of information. Nordea aims to have a common system across the three lines of defence in order to support the Operational Risk Management framework as well as to facilitate and support the daily operational risk management.

Appendix 1

Group Directive	3.2 Nordea Operational Risk Policy (the **Policy**)
References to external rules	• Solvency II • CSSF Circular 12/552 on internal governance central administration and risk control, as amended (the **CSSF Circular 12/552**). • The Luxembourg act of 5 April 1993 on financial sector, as amended (the **Banking Act 1993**) • Q&A on CSSF Circular 12/552 (the **Q&A**)

Description on how the Group Directive shall be adjusted to reflect local regulations applicable to subsidiaries, branches etc. within Nordea Group.	**NORDEA LIFE AND PENSIONS COMPANIES.** ***3.1.2 Three lines of defence*** Insert the following clarification: In NLP the 1st Line of Defence carry out the responsibility of BRIS guided by the CROs and Cos. ***3.1.3 Operational Risk monitoring and control in the 2nd LoD*** Insert the following clarification: The ORO responsibility is overall the responsibility of the CROs in NLP's legal entities as per the Solvency II legislation. **4.7 Capital Estimation Model** In NLP the Solvency II framework shall be applied. ***NORDEA BANK S.A.*** ***As a global change, please replace reference to Nordea Bank AB (publ) or Group by Nordea Bank S.A.*** ***A reference to Nordea in the Policy shall mean Nordea Bank S.A.*** **3.1.2 Three lines of defence** **Last bullet point** Pursuant to point 9 of Circular CSSF12/552 the third line consists of the internal audit function which, pursuant to Sub-chapter 6.2 and Section 6.2.7, provides an independent, objective and critical review of the first two lines of defence After the term assurance, please insert: *and critical review of the 1st LoD and 2nd LoD*

	3.1.6 Delineation of responsibilities between GOR and GC Pursuant to point 104 of CSSF Circular 12/552, please include at the end of the first paragraph the following: *and ensure the independence, objectivity and permanence of internal control functions*. **4.2.1 Committees** Pursuant to sub-section 4.1.4.2 of CSSF Circular 12/552, please amend the first sentence as followed : *Nordea has established a committee structure for the risks incurred and Nordea's ability to manage these risks and the internal and regulatory and own funds and liquidity reserves. The relevant committees include :* **4.3.4 Change Approval Governance (including product approval)** Pursuant to sub-chapter 7.3 of CSSF Circular 12/552, please insert as a preliminary paragraph the following: *The Change Approval Governance shall comply with the provisions laid down in point 177 to 180 of CSSF Circular 12/552.* **4.4 Risk Culture** Pursuant to point 21 of CSSF Circular 12/552, please replace in the second paragraph the term "should take the lead in establishing" by this term: *is in charge of promoting.* **4.6 Archiving** Pursuant to point 204 of CSSF Circular 12/552 and for the avoidance of doubt, please insert the following after 1st paragraph: *Nordea Bank S.A. shall ensure that the archiving mechanisms guarantee confidentiality of data.*