IT Risk Management Policy

1. Objective

The objective of the IT Risk Management Policy (the “Policy”) is to set out the principles for the management of Information Technology (IT) and Security risks in the NordBank (the “Group”)
The Group is exposed to risk relating to the usage of technology. Systematic and co-ordinated management of IT Risk is essential for protecting the interests of the Group’s customers and stakeholders, and for meeting applicable regulatory requirements. The EU and Danish regulatory requirements in-scope of this policy are documented in the Appendix A.
The failure to comply with the IT Risk Management Policy is a serious violation and may lead to action being taken in accordance with the applicable employment regulation, including but not limited to warning, redundancy, suspension or dismissal.

2. Scope

In scope of this Policy are all IT risk management activities within the Group Entity relating to level 1 risk category, Information Technology (IT) and Security risk, and associated level 2 and level 3 risk categories, in the Enterprise Risk Management framework .
This policy supplements the Non-Financial Risk Policy by detailing specific requirements for the management of IT Risks and to comply with internal objectives, applicable regulations and legislations.
Principles of the IT Risk Management Policy should be applied in a third party risk management context, as outlined in the Non-Financial Risk Policy and its instructions
This Policy does not cover control requirements that mitigate Security Risks, which are detailed in the Security Policy. The IT Risk management policy and related governing information along with implemented supporting processes, people and technology, comprise the IT risk management framework of the Group.

2.1. Target Group

This Policy is relevant for all employees across the Group but is mainly relevant for employees who are responsible for implementing the requirements stated in this Policy.
The Management Body of the subsidiary may approve this Policy with deviations in case this Policy conflicts with local regulatory requirements. The policy administrator in the subsidiary should justify the rationale behind the deviation and ensure that the administrator of the Group Policy is consulted and endorses any deviation.
The administrator of this policy must document and report any deviations from the policy to the Executive Leadership Team of NordBank. The Executive Leadership Team shall report all deviations from Group Policies to the Board of Directors of NordBank.

3. Policy Content

Principle 1 A sound governance must be in place to manage and oversee IT Risks

Processes must be developed to enable IT risks to be identified, assessed and mitigated in a consistent manner and in compliance with regulatory requirements.
A tolerance for each IT risk must be defined and set by the Board of Directors supported by appropriate indicators and metrics. In the case of breaches against the set tolerance, these must be escalated in line with Risk Tolerance Guidelines.
All employees must be made aware of and have sufficient knowledge of their responsibilities in the management of IT Risk.

Roles & Responsibilities

➢ *The Executive Leadership Team (ELT) is accountable for implementation of policy and regulatory requirements related to IT Risk, including ensuring sufficient resources.*

➢ *The IT and Security Functions is responsible for establishing and implementing a framework to consistently demonstrate and report compliance with the policy and relevant regulatory requirements related to IT risk*

➢ *Non-Financial Risk (NFR) is responsible for setting policy and control requirements for IT risk*

➢ *NFR is responsible for providing oversight and monitoring to ensure that IT risk management is in line with policy, strategic objectives and regulatory requirements*

➢ *NFR and Group Compliance (GC) are responsible for identifying in-scope regulations, providing guidance on how compliance with those regulations should be met through implementation activity, and relevant risk based monitoring and control of compliance reporting*

➢ *Group Internal Audit (GIA) is responsible for providing assurance. evaluating the effectiveness of the processes used for risk management, controls, and governance*

Principle 2 Applications and Services must be mapped to Business Processes they support

A mapping of Applications and Services to Business Processes must be documented, maintained and recorded in a repository accessible to all impacted stakeholders. The mapping must be of sufficient detail to identify, establish and maintain a mapping of IT assets that support business functions and processes, and therefore identify the IT risk related to business functions.

Roles & Responsibilities

➢ *Process Owners are responsible for identifying Applications and Services which support Business Processes*

➢ *System and Service Owners are responsible for supporting Process Owners in identifying Applications and Services that they are reliant on*

➢ *The IT and Security Functions is responsible for monitoring and controlling mappings to ensure adherence with established frameworks for IT risk*

➢ *NFR is responsible for relevant risk based monitoring and control of the mappings of Applications and Services that support Business Process*

Principle 3 Applications and Services must be classified based on criticality

Applications and Services must be classified based on, at a minimum, confidentiality, integrity, availability and authenticity requirements taking into account the importance of the application to the business process.
This classification must be categorised against financial, customer, regulatory, reputational and market impact aligned to the Non-Financial Risk assessment matrix, with the rationale for the outcome clearly justified.

Roles & Responsibilities

Process Owners are responsible for assigning criticality for their Processes

➢ *System and Service Owners are responsible for classifying criticality for their Applications and Services*

➢ *The IT and Security Functions is responsible for monitoring and controlling criticality assessments to ensure adherence with established frameworks for IT risk*

➢ *NFR are responsible for relevant risk based monitoring and control of criticality assessments*

Principle 4 IT risks must be identified, assessed and mitigated

IT risks must be identified and Inherent Risk assessed based on Criticality of the Application and Service, taking into consideration the threat landscape. The Inherent Risk for identified risks must be aligned to the Non-Financial Risk assessment matrix, with the rationale for the outcome clearly justified.
IT Risk identification includes but is not limited to risk identified as part of risk assessments, incidents or events, audits ,projects and risk scenarios
To mitigate the identified risks, controls must be implemented as stated in control requirements and instructions. The overall effectiveness of controls must be assessed based on the design and operating effectiveness in mitigating the identified IT risk, with the Residual Risk calculated by taking into account the effectiveness of controls. The Residual Risk for identified risks must be aligned to the Non-Financial Risk assessment matrix, with the rationale for the outcome clearly justified.
IT risk assessments must be performed and documented on a regular basis on a risk-based approach, and reviewed annually at a minimum. The outcome of IT Risk assessments must be reported to impacted Process Owners, with IT Risks mitigated in order to keep risk at an acceptable level.

Roles & Responsibilities

➢ *System and Service Owners are responsible for identifying and assessing IT risk for their Application and Service, and reporting the output to impacted Process Owners*

➢ *Process Owners are responsible for managing IT risk associated with their Business Process*

➢ *The IT and Security Functions is responsible for monitoring and controlling the identification, assessment and mitigation of IT risk*

➢ *NFR are responsible for defining Non-Financial Risk assessment matrix and Non-Financial risk assessment requirements*

➢ *NFR are responsible for relevant risk based monitoring and control of IT risk assessments*

Principle 5 Controls must be identified, implemented, assessed and monitored to protect assets

Controls must be identified and implemented to protect assets based on control requirements aligned with regulatory requirements.
The effectiveness of controls must be assessed and recorded based on their design and operating effectiveness in mitigating IT risks. Where controls are less than effective, the IT risk must be assessed and mitigated in order to keep risk at an acceptable level.
Controls must be monitored at an ongoing basis to ensure they remain effective in mitigating the risk.
Controls must, at a minimum, be considered in the context of the following areas:
1. IT and Security Governance and Strategy Implementation (including Architecture , IT & Security Organisation, Management and People, Staffing & Skills Management)
2. IT Risk Management & Security Policy Implementation (including Information Risk Assessment and implementation of IT and Security Risk and Control Frameworks)
3. Logical Security (including System Access)
Physical Security (including Data Centres, Comms facilities & Physical Asset Management)
5. IT Reliability (covering IT Operations Security and including Networks and Communications)
6. Security Monitoring (including Threat Management)
7. Testing and review of IT security
8. IT operations management (including IT Asset Management)
9. Management of IT incidents and problems (including Security Incidents)
10. Use of third parties (including suppliers and considering supply chain)
11. IT project management
12. Acquisition and development of IT systems (including System Development, Business Application Management and System Management)
13. IT change management
14. Data Management
15. Contingency procedures: Business Continuity Management
16. Contingency planning: Business impact assessments
17. Contingency planning: Business continuity plans
18. Contingency planning: Recovery plans
19. Contingency planning: Plan testing
20. Contingency planning: Crisis communication
21. IT Security Training and Awareness
22. Follow-up of Audit Recommendations

Roles & Responsibilities

➢ *System and Service Owners are responsible for implementing and assessing the effectiveness of controls*

➢ *The IT and Security Functions is responsible for monitoring and controlling the identification,*

implementation and assessment of controls

➢ *System, Service and Process Owners are accountable for the self-assessment of controls for the assets they own*

➢ *NFR are responsible for setting policy and control requirements for IT risk*

➢ *NFR are responsible for relevant risk based monitoring and control of control management activities*

Principle 6 The status of IT risk, controls, incidents and events must be reported to appropriate levels of the organisation

IT risk assessments must be recorded in a manner that allows a complete and accurate view of the overall profile of IT risk.

The status of IT risk, controls, incidents and events, including those in relation to IT services supporting critical or important functions provided by ICT third-party service providers, must be reported to the Board of Directors and appropriate levels of management to ensure it has, at all times, sufficient insight into IT risks. Incidents and events including ICT Incidents must be categorised and escalated based on Criticality. **Roles & Responsibilities**

The IT and Security Functions is responsible for monitoring and controlling escalations and reporting to appropriate levels of the organisation

➢ *NFR and GC are responsible for reporting relevant risk based monitoring and control to appropriate levels of the organisation*

Principle 7 Risk assessments must be performed on any major changes to technology

Risk assessments must be performed when there is a major change to technology that may influence the underlying Business Processes, Applications or Services and change the profile of IT risk.

Current IT risk assessments must be updated to reflect the output of the risk assessment.

A framework must be established and implemented to detail how risks associated with initiatives related to technology are managed, mitigated and reported.

Roles & Responsibilities

➢ *The IT and Security Functions is responsible for overseeing initiatives (i.e. projects) and changes related to IT to ensure IT risk assessments are undertaken*

➢ *NFR are responsible for relevant risk based monitoring and control of IT risk assessments*

4. Escalation

The owner of the Policy must report to Executive Management on significant breaches to the Policy. Significant breaches include, but are not limited to:

• Failure to adhere to set tolerances
• Inappropriate or insufficient approvals
• Inappropriate or insufficient reporting
• Unmanaged changes in risk exposures

The owner of the Policy must escalate any breaches of the standards and requirements set in the Policy to the appropriate governing body, including if the maintenance of the Policy is not able to be completed in accordance with the governing document framework.

5. Review

This Policy must be revised when needed and at least annually.

Appendix B

The following terms used in this Policy:

Availability Services and information is available and useable when required

Application A representation of a system that is exposed to users. Applications can be, for example, mobile apps, web portals, collaboration tools, advisory tools, development tools.

Assets Assets include, but are not limited to:

- Hardware
- Software
- Applications, including End User Computing
- Technology Infrastructure
- Technology Processes
- Facilities
- Premises
- Information, whether tangible or intangible
- Services hosted internally or externally, including Cloud services
- Networks and Information systems

Which are found in and relevant to the business environment and worth protecting.

Authenticity Risk The risk of compromised trustworthiness of the system or data source

Board of Directors Is the highest Management Body of the separate legal entity in the Group. In the event that a subsidiary does not have a Board of Director, the responsibilities placed upon the Board of Directors by this Policy, falls upon the Board of Management of that subsidiary.

Business Process A defined set of Activities that represents the steps required to achieve a business objective being a specific outcome to a stakeholder. It includes the flow and use of information and resources.

A Business Process provides an end-to-end view including front to back, back to front relationships.

Confidentiality Information only available, or disclosed to, authorised individuals, entities or processes.

Controls Any action/activity, designed to manage risks, that might otherwise impact the achievement of the objectives of the process/product/system/regulation.

Control Requirements A high-level description of the controls to be implemented aligned to regulatory requirements.

Critical or Important Functions (CIFs)

Critical or important function means a function the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.

This means a function that is:

- BRRD critical processes (as per Bank Recovery & Resolution Directive)
- Processes critical from a Business Impact Analysis (BIA) assessment perspective
- Regulatory processes or other processes deemed critical

Criticality An assessment which considers, at a minimum, the confidentiality, integrity, availability and authenticity requirements aligned to the non-financial risk matrix.

Criticality of an application or service should consider the criticality of the business process that it supports.

End User Computing (EUC) Defined as user-developed applications including the use of spreadsheets and databases that are not maintained and operated by IT.

Executive Leadership Team (ELT)

Executive Leadership Team of NordBank or the subsidiary equivalent.

IT and Security Event Threats that have been exploited or realised resulting in risks that have caused a financial loss/gain or have had a non-financial impact towards the bank's reputation, regulatory compliance or customer experience.

Group Means NordBank and its Group Entities

IT Incident Unplanned interruption to an IT service or reduction in the quality

of an IT service of failure of a Configuration Item that has not yet impacted an IT service. This includes ICT-related Incident i.e. a single Event or a series of linked Events unplanned by the Group that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data

Inherent Risk The realistic worst outcome of a potential failure in a process, system, activity, project or product. Inherent risk rating is the measurement of the gross risk exposure without taking existing controls or mitigating actions into consideration. Inherent Risk for IT Risk is a function of threat and impact.

Integrity Information and information processing is accurate, complete and consistent.

IT Asset IT & Security Risks Security Function Service Service Owner System System Owner Third Party Level of Control Non-Financial Risk Process Owner Privileged Access Third Party Arrangement Internal- NordBank

Hardware or software, irrespective of where it resides, that provides value to business activity. This includes for example computer programs, applications, cloud services, software modules, software tools, networks, websites, electronic databases and devices.

L2 Risk types further specifying the L1 Risk type Information Technology (IT) and Security risk.

Interpretation note: IT risks are intended to be synonymous with Information Communication and Technology (ICT) and security risks referred to in related regulatory guidance (e.g. the EBA Guidelines on ICT and Security risk management).

The function, independent from IT operations processes, responsible for establishing, implementing, monitoring and controlling adherence to the Security Risk management frameworks.

A coherent, ready-to-use deliverable that combines assets, components, processes, and resources needed to deliver a specific outcome which brings value to a service recipient while hiding implementation and technical complexity. Different service classes include business service, application service, and technical service. Services can be internal, offshored, intra-Group outsourced, or third party outsourced. This includes ICT Services i.e. means digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services.

The person accountable for the management of a Service and its execution during its lifecycle.

A set of IT assets used to process, store, maintain and operate data and information, which supports and controls business processes.

The person accountable for the management of an Application and its execution during its lifecycle

A separate legal entity or company. The Third Party may also be a Subsidiary. This also includes ICT Third Party Service Provider i.e. a Third Party providing Information Communication and Technology-services. Can also be Outsourcing. An ICT Third Party Service Provider can be deemed as critical by the ESAs (European Supervisory Authorities)

The design of the control aligned to control requirements which mitigates risk to an acceptable level

Risk of financial losses or gains, regulatory impact, reputational impact or customer impact resulting from inadequate or failed internal processes, people and systems or from external events, including legal and compliance risks.

The person accountable for the management of a Business Process and its execution during its lifecycle. By default, this also includes the underlying Activities of the Business Process as well as the related Operational Guidelines and SOPs.

Administrator Access Right to any technical infrastructure (server, database, network, storage, workstations, etc.). Administrator Access Right to an application, which manages infrastructure, is also privileged Access Right. Administrator accesses inside other applications are not defined as privileged Access Rights.

is an arrangement with a Third Party that provides goods and/or services to NordBank and/or its Subsidiaries or to NordBank A/S's and /or its Subsidiaries Customers on behalf of or in association with NordBank or its Subsidiaries. Third Party Arrangements include but are not limited arrangements for procuring products or services from suppliers and vendors, ICT

Third Party Service Provider, Outsourcing, Cloud Services, engaging consultants, Agents, Business Partners, referral and affiliate arrangements, brokers, correspondent banks, sponsorships, joint ventures, exchanges, trading venues, and financial infrastructures.

Threat Any cause of an incident or event that could negatively impact an asset.