Storebrand

Policy for Digital Operational Resilience in the Storebrand Group

Adopted by:	The Board of Directors of Storebrand ASA
Adopted:	January 14, 2025

Contents

1. Purpose and background 2
2. Legal basis 2
3. Roles and responsibilities 3
4. Digital operational resilience 3

1. Purpose and background

The strategic value of customer-oriented and scalable digital solutions (ICT services), combined with safe and secure information management, is constantly increasing for the Storebrand Group (the Group). To meet the expectations and requirements of the Board of Directors, customers, shareholders, society and applicable legislation, the Group's ICT services shall be developed, maintained and operated with a high degree of operational resilience. This will ensure a continuous ability to prevent, detect, manage and recover from ICT-related incidents and security incidents.

This policy is a public version of Storebrand's internal guidelines for digital operational resilience. The document describes how the Group works with ICT risk management and digital resilience. Some details have been omitted or simplified for reasons of confidentiality and internal governance processes.

For the purposes of this policy, ICT services are understood broadly and include digital and data-driven services that are provided via ICT systems and that continuously serve one or more internal or external users. This is the sum of the Group's digital products, technology platforms and the overall portfolio of systems and applications that the business chooses to use for the collection, transfer, processing, storage and presentation of data. ICT services also include ICT consultancy and data providers. The guidelines apply to all ICT services, both those that are outsourced internally in the Group and to external suppliers.

2. Legal basis

Since 2003, Norway has had the ICT Regulations ("IKT-forskriften"), which regulate the areas covered by the guidelines. The ICT Regulations are further elaborated by guidelines for ICT security and risk management prepared by EIOPA, EBA and ESMA.

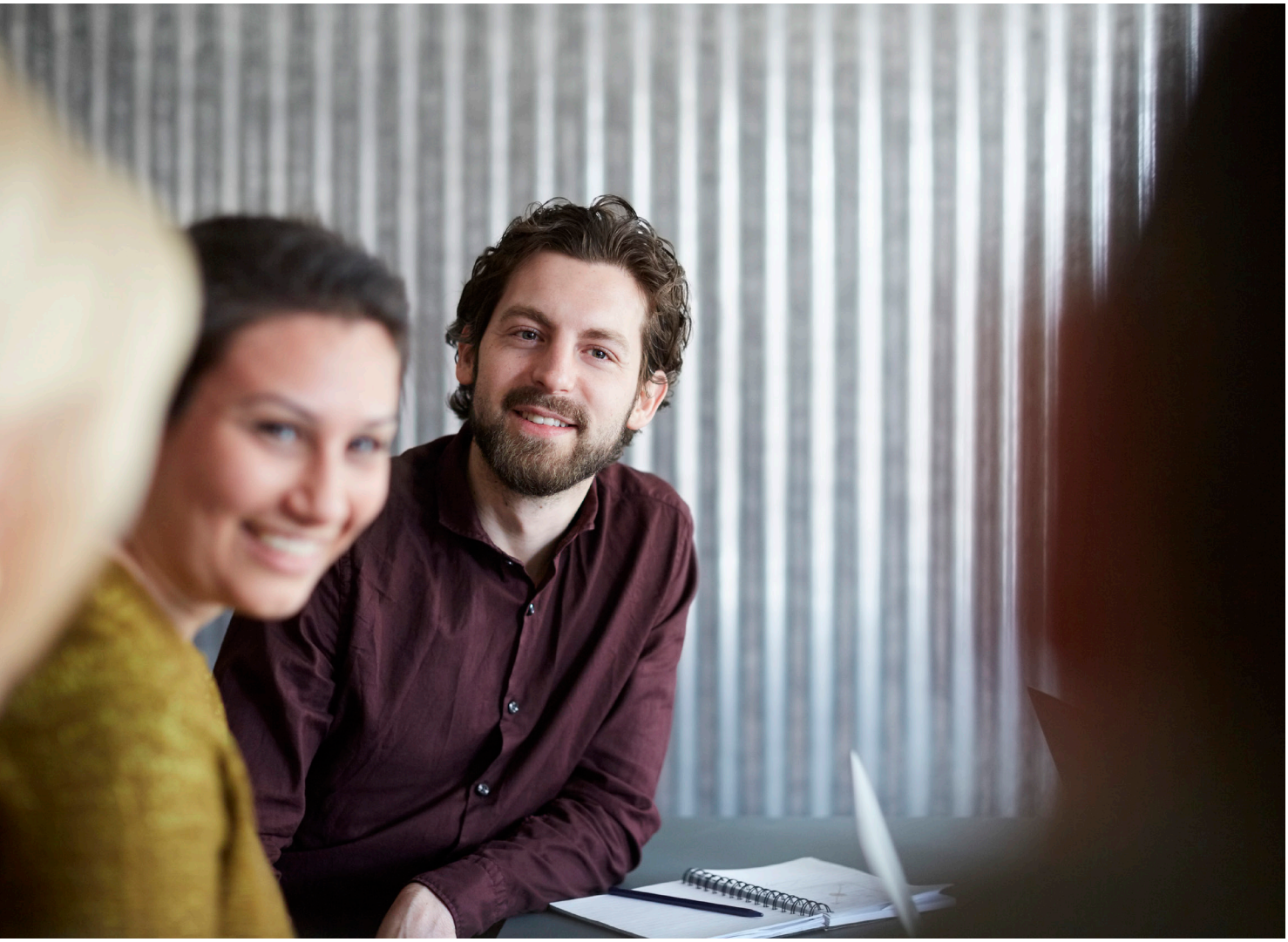
In addition, the Digital Operational Resilience Act (DORA) entered into force on 16 January 2023 and will apply from 17 January 2025 in the EU, and in Norway during 2025. The regulation contains pan-European rules and requirements for the financial sector's management and assessment of ICT risk, with the main purpose of strengthening the digital operational resilience of the sector. This guideline is based on the regulatory requirements set out in DORA.

3. Roles and responsibilities

The Board of Directors of Storebrand ASA (the Board) has the overall responsibility for ensuring that the Group has an adequate and effective management system for ICT risk. The ICT risk management system shall ensure that information is handled and protected in a responsible and secure manner, and that ICT services are developed, operated and maintained in accordance with applicable laws, regulations, agreements, as well as established risk management practices and security requirements. The Board follows up the business through periodic Business Reviews, reviews of the status of risk and compliance by the independent control functions (Chief Information Security Officer (CISO), Chief Compliance Officer (CCO) and Chief Risk Officer (CRO)), as well as from the internal audit's independent investigations.

Storebrand has consolidated the strategic and operational responsibility for the development and operation of ICT services into a separate area of responsibility in the Group Executive Management - Storebrand Digital in Storebrand Livsforsikring AS. Other legal entities under Storebrand ASA have fully or partially outsourced IT development and operations to Storebrand Livsforsikring AS.

Storebrand has gathered responsibility for independent reporting on ICT risk to the Board of Directors and the CEO of the Group and all the Group's subsidiaries in a separate area of responsibility in Group Security in Governance, Risk & Compliance (GRC), led by the CISO. The boards of directors of the group entities have mandated the CISO to design the group's framework for ICT risk management with associated requirements and controls in accordance with the board's risk appetite and objectives in force at any given time.



4. Digital operational resilience

The ICT strategy and the entitys' framework for ICT risk management shall support the entity's and the Group's business strategy and objectives. The ICT strategy must reflect the entity's risk appetite.

The ICT strategy shall include the Group's strategy for digital operational resilience and strategy for managing ICT third-party risk.

4.1 ICT risk management and security

The entity shall have a comprehensive, efficient and well-documented management system and framework for ICT risk management, integrated as part of the overall risk management framework. The framework will ensure that ICT risks are managed quickly, efficiently and holistically, and contribute to maintaining a high level of digital operational resilience.

ICT risk includes threats and vulnerabilities related to information security, cyber security, system availability, technical stability and operation, data integrity, quality of service and compliance with regulatory requirements.

The ICT risk management framework shall include:

- Identification: Regular mapping of critical systems and risks associated with ICT services, platform, infrastructure and data.
- Prevention: Implementation of preventive measures
- Detection: Early warning and detection mechanisms for abnormal activities, including violations of security guidelines.
- Response and recovery: Defined procedures for rapid response and continuous improvement after ICT incidents.

Risk associated with ICT services must be documented and linked to internal controls and is part of operational risk management. The scope and level of detail in the risk assessments shall be adapted to the results of the entities' business impact assessments (BIA) and reflect the importance of ICT services for the business' important and critical business functions.

In addition, risk assessments must be carried out in the event of significant changes in ICT activities.

Information security work must follow the framework for ICT risk management and be based on risk assessments, maturity assessments and established security controls. This must be documented and integrated as part of the operational risk management.

The independent control functions shall establish independent risk-based controls. The results of these are included in the functions' follow-up of the business and board reporting.

4.2 Information management and access control

All information processed in Storebrand shall be assessed and classified based on criticality and need for protection. Classification of information, processes and ICT services shall be carried out in accordance with requirements set out in the management systems for security and emergency preparedness.

Information shall be ensured regarding confidentiality, integrity, continuity, availability and traceability, in accordance with applicable laws and regulations. Technical security measures shall be established to protect information against unauthorised and unlawful access, alteration, manipulation, disclosure and deletion, in accordance with the classification of the information.

All employees have a duty of confidentiality and must know what kind of information they are processing and how it can be handled. If the information concerns personal data, guidelines for the processing of personal data must be followed. The transmission of information, whether physical or electronic, shall take place in a secure manner, in accordance with the classification of the information.

Access to the Group's information shall be managed based on business needs. The person who has the authority to approve access is also obliged to remove these when the need changes or ceases. It shall be checked regularly, at least annually, that access is limited only to current needs.

Deletion of information must be done in a secure manner, to prevent unauthorised disclosure of information.

4.3 Security awareness and training

A programme will be established and maintained with the aim of building and continuously strengthening a positive security culture throughout the Group. The program will use a wide variety of tools to create understanding, competence, and commitment to information security among employees to increase their resilience to possible threats, as well as to reduce information security risks associated with the human aspect. The impact and effectiveness of the programme shall be measured to an extent and with a frequency that is deemed appropriate.

As a minimum, the programme shall include a common course where employees gain a basic understanding of common issues related to information security, are briefed on the current and relevant threat and risk landscape and are informed about common guidelines and procedures related to information security and emergency preparedness, as well as where they can turn to acquire further information and support. The course must be compulsory and must be completed annually. All employees must also annually read through and digitally sign an abbreviated version of the security regulations.

4.4 Development and maintenance
All development of ICT systems, whether it is carried out internally or via suppliers, must follow a documented development process for the area in question. Development shall always be carried out in accordance with the Group's requirements and processes for secure development in force at any given time. To ensure quality and compliance, the development work shall be systematically monitored and regularly revised to identify areas for improvement. All actors involved in the development process have a responsibility to maintain security and quality requirements throughout all stages of the process.

4.5 Change management
The entity shall establish and maintain principles for change management that ensure that all changes to ICT services, applications, platforms and infrastructure are planned, implemented and monitored in a structured and controlled manner. Change management must ensure the availability, authenticity, integrity and confidentiality of data and applications, while minimising the risk of operational disruptions. The change process should include clear roles and responsibilities for planning, testing, approval, and implementation. Joint processes shall contribute to transparency to address the need for coordination, planning and effective handling of undesirable incidents that may arise in connection with changes that have been made.

4.6 Handling, classification and reporting of ICT-related incidents, including security incidents and cyber threats
A group-wide process will be established for handling ICT-related incidents. This process will ensure effective monitoring, reporting and follow-up, with the aim of minimising consequences, preventing recurrence and strengthening operational resilience. Critical incidents must be reported to the relevant authorities in accordance with the applicable requirements. The process should include mechanisms for continuous improvement based on learning points from events.

The Group entity may, on a voluntary basis, notify relevant authorities of significant cyber threats, if these are deemed to be relevant to the financial system, users or customers.

4.7 Digital operational resilience testing
The business will establish, implement and maintain a robust and comprehensive programme for testing digital operational resilience. The programme shall ensure the Group's ability to resist, respond to and recover from ICT-related incidents, including security incidents.

The test program will:
- cover critical and essential functions, including third parties and vendors.
- be carried out by independent parties, either internal or external, based on a risk-based approach.
- include vulnerability assessments, security analyses, performance tests, scenario-based tests and, if designated by national authorities, advanced threat-led penetration testing (TLPT).
- be documented, and findings must be reported to relevant governing bodies with an action plan for identified vulnerabilities and deficiencies.

Processes will also be established to ensure that experience gained from testing is used to strengthen ICT risk management and ensure effective risk management through regular updates of the framework.

Testing shall be carried out at least annually for ICT services that support important and critical business functions.

4.8 Continuity and preparedness
To ensure safe and stable operation of digital services, the business must establish and maintain robust emergency preparedness and crisis management procedures. Risks must be identified and assessed continuously to enable targeted measures that reduce the consequences of serious incidents. Clear lines of communication and responsibilities will be established to ensure a rapid and coordinated response to crisis situations.

Contingency plans must be updated and tested regularly to ensure that they are relevant, effective and adapted to different types of digital threats, including cyber-attacks and business interruptions. The plans shall describe procedures for handling critical incidents and the division of roles and responsibilities in emergency situations.

The business must also ensure that all employees have the necessary training and awareness related to emergency preparedness and incident management, so that roles and responsibilities can be taken care of effectively in the event of serious incidents. This will help strengthen the organisation's overall digital resilience.

The Group also has its own guidelines for crisis management, emergency preparedness and continuity planning, as well as a Group Emergency Preparedness plan. The Group's ICT services are covered by these.

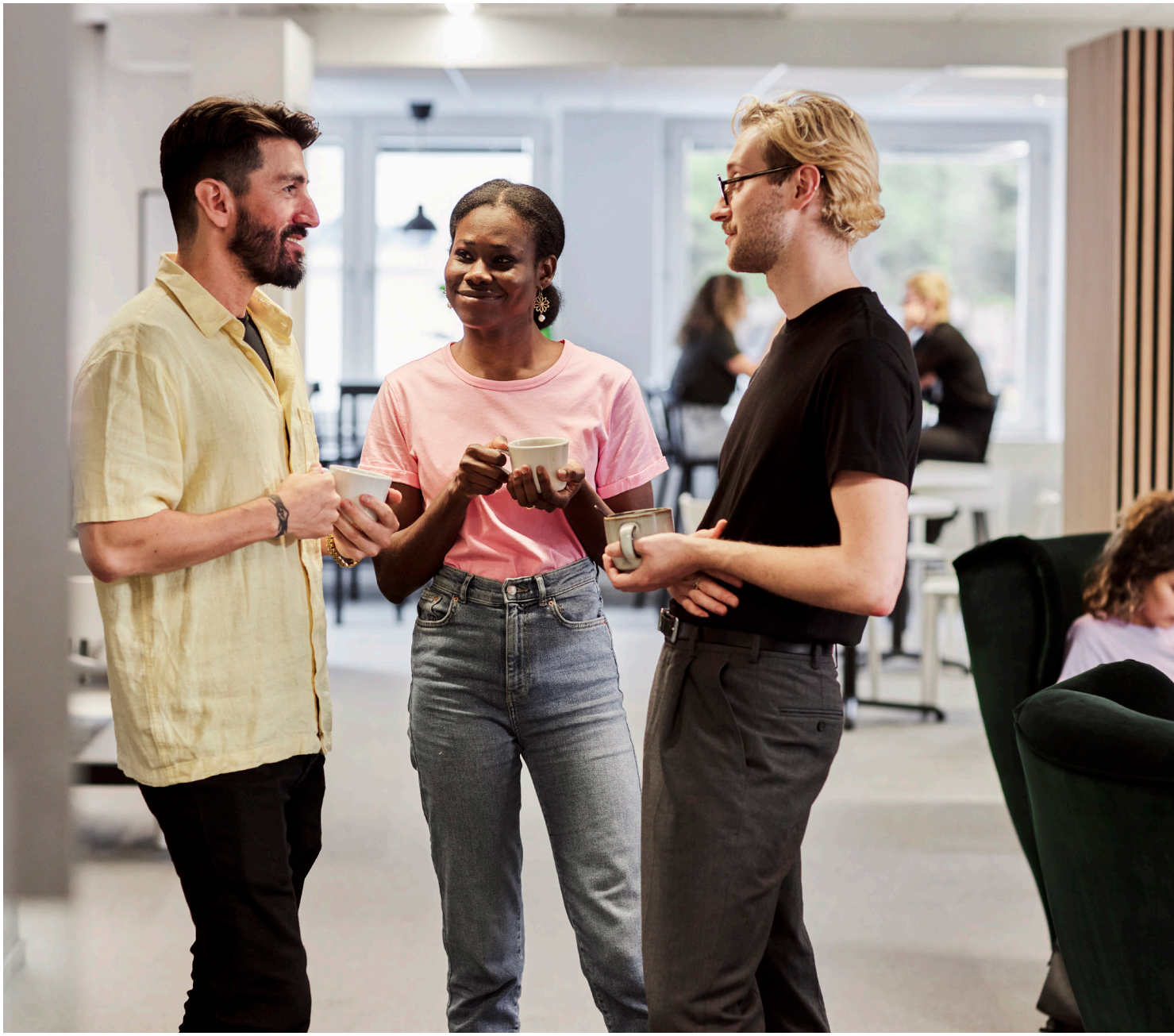
4.9 ICT third-party risk
To ensure digital operational resilience also when using outsourced ICT services, thorough and documented due diligence and risk assessment must be carried out before entering a contract. Outsourcing includes both Group internal and external supplier relationships. The assessments shall consider the criticality of the service, identify necessary security measures, and assess the consequences that deviations, fraud or compromise may have for the business' ability to secure Storebrand and our customers' data, as well as maintain secure and stable operations. All suppliers shall meet defined security requirements and regulatory obligations and shall be systematically monitored to ensure continuous compliance. Clear agreements must be established that regulate the division of responsibilities, requirements for information security, and plans for preparedness and recovery in the event of any security breaches.

Furthermore, regular assessments and audits of the supplier's security shall be carried out, and the security requirements in the agreements shall be updated as necessary. This will ensure that supplier relationships always support the business' overall digital resilience. The Group also has its own guidelines for outsourcing, which cover both internal and external outsourcing. Procurement and follow-up of ICT services are covered by these guidelines. The main points of the guidelines include requirements for:

- Risk and supplier assessment
- Entering into contracts and drafting agreements
- Exit and contingency plans
- Follow-up, monitoring and reporting
- Termination of contract

4.10 Collecting, sharing, and reporting information

The entity shall establish and maintain systematic information registers, as well as effective mechanisms and processes for information sharing with relevant authorities and other financial institutions. Information sharing and registration shall include significant risks, ICT-related incidents and cyber threats, as well as ICT providers. The entity is also responsible for ensuring that all required information is available to the authorities upon request.



86186 06/2025