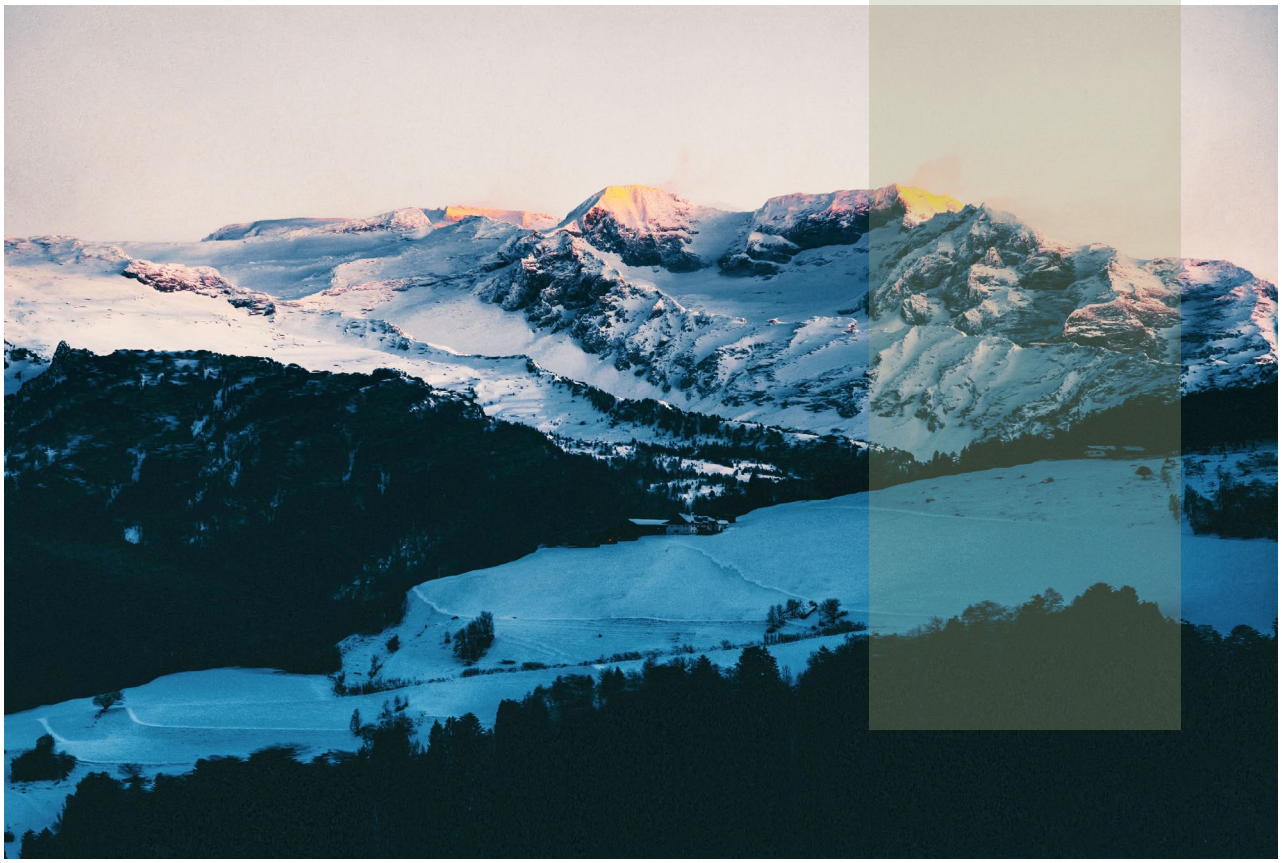

riskpoint

rp underwriting

THE RISKPOINT GROUP

DIGITAL RESILIENCE

THE RISKPOINT GROUP FRAMEWORK FOR ICT COMPLIANCE

Management Summary

The Digital Operational Resilience Act (DORA) is a piece of regulation by the European Union aimed at ensuring that financial entities can withstand, respond to, and recover from Information Communications Technology (ICT) related disruptions and threats. DORA contains rules which outlines the required ICT security levels for financial institutions. The RiskPoint Group must comply with DORA, which takes precedence over other EU ICT legislations, such as NIS2.

This document outlines the policies and procedures that the RiskPoint Group has implemented to comply with DORA. It further provides a comprehensive guide for how the RiskPoint Group ensures digital resilience through various technical and organizational measures.

The RiskPoint Group has designated certain applications as being core applications which are crucial for underwriting, storing documents, and collaborating with brokers & stakeholders. DORA contains heightened requirements for how these are treated.

This document details how the RiskPoint Group have implemented measures and policies based on Business Impact Analysis', Risk Assessments and best practices using methodologies as outlined in DORA. These measures are continuously assessed and updated to ensure they meet the required standards.

The RiskPoint Group has established ICT oriented policies for vendor management, change management, incident response, business continuity and disaster recovery, data protection, and IT. These policies helps ensure that all risks are identified, assessed, and mitigated effectively. The RiskPoint Group conducts regular awareness and training programs for employees to ensure they are well-informed about digital resilience and cybersecurity practices.

Table of Contents

1. INTRODUCTION

This document describes how the RiskPoint Group obtains digital resilience. It outlines how the RiskPoint Group's Risk Profile is established by IT Compliance, approved by IT Management, and monitored by Compliance. It describes the applicable policies and procedures in place to achieve compliance with DORA, including the design of certain controls and measures.

The content of the measures is based on:

- Legal requirements as outlined in DORA ((EU) 2022/2554)
- The RiskPoint Group Business Impact Analysis and Risk Assessments

To ensure the RiskPoint Group's long-term IT compliance, measures are designed to outline that applicable prerequisites are in place, all major steps needed to achieve the desired level of risk mitigation, and the output that is achieved by performing the measure.

A key aspect of DORA are the Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS). These are tools the DORA legal regime uses to continuously update required standards and are published regularly.

1.1. Security Board

The Security Board at the RiskPoint Group is established to oversee and ensure the effectiveness of the company's digital resilience and cybersecurity measures. The board is responsible for reviewing and approving security policies, assessing risks, and ensuring compliance with regulatory requirements such as DORA. It consist of IT Management and IT Compliance, and meets at least quarterly. The highlights of the Security Board's actions are further communicated to the Management Body.

The Security Board's responsibilities include the following:

- Review and approve ICT policies and procedures
- Review control deficiencies, risk assessments, the status of disaster recovery plans
- Review ICT awareness and training programs
- Accept or mitigate risks identified in the Risk Register and ensures that proposed measures comply with regulatory requirements
- Review ICT Vendor Register of Information
- Approve scope of BIA and list of ICT assets in same
- Stay continuously informed about relevant RTS and ITS's for which for process-changes are proposed, and approve same

1.2. Defining Risk Profile and Appetite

The RiskPoint Group's Risk Profile is shaped by being an insurance distributor doing business on a global level with headquarters in Denmark and offices around the world. The company is internally set up using a matrix structure meaning each office has its own management within its region. All offices use the same ICT infrastructure and systems, which are controlled by a dedicated IT team in close collaboration with the RiskPoint Group compliance body.

The nature of the business means that there is a high volume of policies and claims, which makes the RiskPoint Group vulnerable to data loss.

Due to the abovementioned structure and fast-paced nature of the business, the company depends on IT support at all times during business hours. It also makes it important to have aligned processes from an availability and service perspective, since vulnerabilities can then be mitigated effectively. Utilizing cloud infrastructure additionally plays a key role, but also creates further security demands on third party ICT vendor management.

Data is at the core of the RiskPoint Group's business including within the area of claims handling. As such, data integrity is critical to the business, which translates into a requirement for strong measures ensuring that data has not been tampered with.

Risk Appetite is the tolerance the RiskPoint Group has for ICT Risks. It is important to establish this, as it guides to which degree DORA-measures are implemented. On an overall level, it sets out how the RiskPoint Group assesses risk.

The Risk Appetite is established with the help of the RiskPoint Group Risk Register. The Risk Register is maintained by IT Compliance and consists of all identified ICT risks. The Security Board evaluates the relevant risks from the Risk Register and determines which risks are crucial and should be mitigated, which are acceptable, and which should be presented to the Management Body. The outcome of this is the accepted Risk Appetite.

1.3. The RiskPoint Group ICT Infrastructure

It is important to define which ICT systems are used for critical business processes as these take on a higher importance than other applications. Based on the Business Impact Analysis (BIA), described in Section 2, the RiskPoint Group have determined that the following are core applications:

- **Navins** – ERP System: Insurance and General Ledger for policy administration, claims handling, as well as financial management and bookkeeping. This system is a vertical solution in Microsoft Business Central. The system is hosted in a private Azure cloud managed by MB Solutions. Software is delivered by Diastasys.

- **Datawarehouse** – Datawarehouse for business control purposes and business analytics. This technical platform is hosted by MBS. It is an internally developed tool and data is fully managed by the RiskPoint Group.

Additionally, based on the BIA, the RiskPoint Group cloud infrastructure has been determined to hold special significance. It supports the business processes and consist of the following:

- Office 365 / SharePoint for office collaboration.
  This is a cloud service delivered via MB Solutions by Microsoft.

- Azure Virtual Desktop for secure access to resources.
  This is a cloud service delivered via MB Solutions by Microsoft.

- Office network and VPN connections to service providers.
  These networks are services as part of housing agreements.

2. ICT RISK MANAGEMENT FRAMEWORK

This section describes the RiskPoint Group's framework for identifying and assessing risk. It highlights the main tools used for this, and how these interconnect throughout the RiskPoint Group's ICT landscape.

2.1. Business Impact Analysis (BIA)

This section describes what a BIA is and how it is utilized within the RiskPoint Group. A BIA is a tool used throughout IT Compliance. It is used to identify and classify risks in ICT applications. These can then be defined and it can established whether mitigation is or should be in place to reduce the impact of the consequence of the risk.

A BIA is performed on an annual basis by IT Compliance and its conclusion flow through and is used in the revision of all ICT policies. The BIA process consists of qualitative user interviews to identify business processes and the ICT applications which support these. Following this, the applications are classified as to their business criticality – how long the business can function without it.

Based on the results, potential risks can be discovered which flow into the ICT Risk Register, and ideal recovery time for the applications is found, which is further used in Business Continuity Plans.

In addition to being a requirement under the DORA regime, performing an annual BIA is crucial for ensuring the resilience and continuity of business operations. By identifying potential vulnerabilities and their impacts, the RiskPoint Group can proactively implement measures to mitigate risks, thereby safeguarding our reputation and maintaining the trust of our partners.

The list must be updated and approved annually or in case of major changes to ICT assets or infrastructure. The Security Board provides all approvals.

2.2. ICT Risk Register

The Risk Register consists of specific risks and is used to create an overview that can then be further assessed. Risks are identified via different sources, including but not limited to the BIA, vulnerability scans, penetration tests, and anti-virus scans.

An ICT risk assessment is used to determine the likelihood and severity of each identified risk. Based on this each risk obtains a risk score which is documented on the Risk Register. The register is updated continuously and all risks are evaluated at least annually. In case of any ICT incident, the register is reviewed to ensure robustness. This process enhances digital resilience, supports business continuity, improves trust, and facilitates informed decision-making.

IT Compliance presents the highest scoring risks to the Security Board on a monthly basis. IT Management, as part of the Security Board, decides whether to accept or mitigate each of these risks, and what the mitigation should be.

At the RiskPoint Group, it is essential that management has full transparency regarding the risks identified by the organization. Therefore the list of highest scoring risks, including decisions from the Security Board is presented to the Management Body following the Security Board meeting by IT Management.

IT Compliance updates the Risk Register with the findings of the Security Board and controls that the mitigation is done.

The Risk Register ensures that all identified risks are documented, monitored, and managed effectively. This process not only supports compliance with legal requirements but also enhances risk management practices, promotes accountability, and facilitates informed decision-making.

3. RTS AND ITS

Regulatory Technical Standards (RTS) and Implementation Technical Standards (ITS) specify any updates or changes to ICT requirements under the DORA regime. They are continuously formulated and released by the EU Regulator. Their purpose is to account for an ever-changing ICT landscape and make the DORA requirements dynamic in nature.

The DORA regime mandates that the RiskPoint Group implements specific initiatives to comply with these as they are released. As such, IT Compliance continuously monitors for new releases and changes.. When new RTS and ITS are released or existing have been revised, they are implemented accordingly by IT Compliance. The Security Board is always informed of this plan before initiation.

4. OPERATIONAL CONTROLS

The RiskPoint Group actively implements ICT controls to ensure operational effectiveness of business processes and security measures. This includes regular testing and validation of implemented ICT controls to ensure they continue to meet required standards and help mitigate risks. The purpose of this section is to give an overview of certain ICT controls.

ICT Controls are designed and implemented by IT Compliance with involvement of vendors when deemed necessary. In the cases where controls are performed by a vendor, the RiskPoint Group's IT is responsible for setting the requirement and monitoring the effectiveness of the vendor implementation.

A monthly report is delivered by IT Compliance to The Security Board specifying whether any ICT control deficiencies have occurred and how they were handled.

4.1. Monitoring ICT Infrastructure

The RiskPoint Group monitors ICT infrastructure to uncover and quickly respond to incidents. It also ensures the identification and resolution of potential issues before they evolve into incidents, thereby maintaining the security and resilience of systems. Data gathered via such control is used

for documentation purposes. Monitoring practices are differentiated by type – servers, core applications, and devices – each with their own practices and documentation.

The baseline for the monitoring is partially established by relying on the Risk Register, in combination with advice from ICT third party vendors regarding current market practices.

Incidents involving servers and devices are documented monthly for reporting purposes.

Server Monitoring
Servers are continuously monitored via a third party providing Security Operations Center services overseen by RiskPoint IT. This monitoring includes but is not limited to checking whether regular backups are performed, and that Site-to-Site connections are stable. Where critical ICT Systems feed data into the server, this is also monitored. Third party is able to act quickly if any incidents are uncovered via the process described in the ICT Incident Management Policy.

Application Monitoring
All core applications utilize an identity management procedure for internal users. This encompasses linking a user account to a specific employee and documenting same upon creation. On an annual basis this documentation is reviewed and validated. Validation consists of confirming whether users are still active and require access to the application.

Depending on the core application, user activity is monitored to various degrees. Activity can be tracked and documented.

User rights are granted on a need-to-know basis with only relevant employees receiving access to an applicable application. Accounts are managed by internal application administrators who hold special accounts.

Login authentication follows industry best practices – for more please refer to the IT policy in Section 6.6.

Device Monitoring
All laptops & non-office computers are tracked via their unique identifier which is linked to a named employee. Computers are continuously monitored via endpoint protection done by a third party service provider overseen by RiskPoint IT. This monitoring is done via a device management portal through which device status and user logins are tracked. Computer security is monitored via a centralized anti-virus application. All mobile phones are similarly physically tracked by linking their unique identifiers to a specific employee.

4.2. Testing Program

The RiskPoint Group has a comprehensive testing program that includes a variety of testing protocols, including but not limited to Threat Led Penetration Tests, Vulnerability Scans, and Simulated Phishing Attacks.

The purpose of the testing program is to use the tests as controls to verify that the RiskPoint Group's policies are effective.

Vulnerability Scanning
The RiskPoint Group's IT department conducts continuous vulnerability scanning on IT-infrastructure. This scanning is executed via antivirus software and takes user activity, software, devices, and network into account. The scanning uses data gathered to give recommended actions to remediate risks and vulnerabilities.

At least annually the RiskPoint IT department conducts a more extensive vulnerability scanning via a third party provider. The purpose of conducting multiple vulnerability scans is to increase chances of discovering potential risks. Relevant discovered risks are documented on the internal risk assessment and presented to the Security Board.

Threat Led Penetration Test (TLPT)
A TLPT is an intrusion test conducted on IT systems to simulate how a real hacker would attempt to breach the RiskPoint Group's systems.

TLPT involves conducting comprehensive tests that simulate real-world cyberattacks to identify vulnerabilities and assess the effectiveness of security measures. This includes all critical ICT assets and systems, to which both external and internal penetration tests are conducted to cover

all potential attacks. By adhering to these requirements, the RiskPoint Group aims to enhance its digital resilience and ensure robust protection against cyber threats.

The RiskPoint Group conducts a TLPT at least once every 3 years to ensure that the IT-infrastructure has an appropriate security level and confirm that no exploitable vulnerabilities threatens the digital resilience of the organization.

Phishing Campaign

Phishing campaigns are conducted continuously. The purpose of these campaigns is to train employees against real phishing attacks and therefore reduce the risks of an actual attack being effective. The campaigns mimic real emails from well-known companies with the purpose of simulating a real phishing attack.

The phishing campaign, based on user behavior, adapts subsequent campaign's difficulty to the individual user. This campaign can reveal specific users that pose a significant threat to the RiskPoint Group's overall security and, if necessary, IT management will escalate the issue to the management body for actions needed.

5. AWARENESS TRAINING ON DIGITAL RESILIENCE

ICT Awareness training is the education of employees on the importance of Digital Resilience. At the RiskPoint Group, it is crucial that all employees are aware of the requirements of operating within the boundaries of business and business rules.

To perform this training, a third party platform is used to provide the training and track attendance and progress.

Training is performed by all employees to ensure company-wide mandatory obligations. Training modules are conducted continuously throughout the year via company email at least once per month.

On a quarterly basis, an email will be sent to employees who have not responded to at least 50% of the training emails. The email lets them know that participation is mandatory. That it is a regulatory requirement and is being tracked. They are told that they must respond to at least 50% of the questions. If they continue to not respond, a list of applicable employees is presented to The Security Board that will determine what further action is necessary.

6. POLICIES RELATED TO DIGITAL RESILIENCE

The below policies make up the rest of the framework relevant for achieving Digital Resilience for the RiskPoint Group. The purpose of the policies is to have a workflow that is based on the Risk Appetite of the RiskPoint Group while living up to all applicable legal requirements. All ICT policies are submitted by IT Management to The Management Body for approval.

6.1. ICT Vendor Management

A significant portion of the RiskPoint Group's ICT landscape and infrastructure is managed by external vendors. Therefore, effective vendor management is crucial to ensure that appropriate controls are in place for these vendors. As such, the RiskPoint Group has enacted an ICT Vendor Management Policy outlining our strategy, policy, and procedures on this area.

It includes classifying ICT vendors, specifying requirements, and the putting in place of continuously monitoring of the relationship.

For more information please refer to the Vendor Management Policy.

6.2. ICT Change Management

At the RiskPoint Group, it is crucial that all systems are well-controlled and that the level of risk associated with a change is transparent to the organization. By maintaining robust change management practices, the RiskPoint Group aims to enhance system stability, ensure compliance with regulatory requirements and support continuous improvement of systems and services.

For more information please refer to the Change Management Policy.

6.3. ICT Incident Management

ICT Incident Management includes identifying, documenting, and managing ICT incidents. In addition, it means having established clear lines of communication. Having these in place allows the RiskPoint Group to respond to incidents promptly and be able to support informed decision-making. In addition, a crucial step of this is the RiskPoint Group Incident Response Plan which specifically outlines what to do in case of a cyber incident.

For more information please refer to the Incident Management Policy.

6.4. Business Continuity

The RiskPoint Group's commitment to business continuity and disaster recovery ensures minimal downtime during disruptions and supports a stable operation. Business continuity plans are in place for all office locations and critical business processes. This also includes a disaster recovery plan for IT infrastructure.

For more information please refer to the Business Continuity Policy.

6.5. Data Protection

A main goal of having robust IT security is to protect data - both personal and corporate. As such, the RiskPoint Group has a comprehensive data protection policy, covering, among other things, data processing.

For more information please refer to the Data Protection Policy.

6.6. IT

A crucial factor of the RiskPoint Group's digital resilience is IT security. As such there are comprehensive measures to secure this, and well as procedures in place to confirm the effectives of these measures.

For more information please refer to the IT Policy.

RELATED DOCUMENTS

This Code of Conduct should be read in conjunction with the following policies and procedures:

- ICT Vendor Management Policy
- ICT Change Management Policy
- ICT Incident Management Policy
- Business Continuity Policy
- Data Protection Policy
- IT Policy

Version: 1
Last Updated: February 5, 2025