Raiffeisenlandesbank
Niederösterreich-Wien

Information Security & Resilience

Version 1 / 31.12.2025

Information Security Goals

The objective of Raiffeisenlandesbank Niederösterreich-Wien is to ensure and continuously enhance the security of the company's information, as well as that of its employees, business partners, and customers. To achieve this, the following security objectives are ensured from both a technical and organizational perspective:

- Confidentiality, integrity, availability, and authenticity of information and data, as well as its systems and processes
- Exclusive access to information, data, and systems by authorized, authenticated, and traceable users
- Compliance with laws, standards, and regulations
- Identification, assessment, and management of information security risks
- Detection and structured remediation of information security breaches

Information and data are among the company's most important intangible assets. To protect them, information systems are designed and organized from both technical and organizational perspectives. The goal is to minimize risks regarding confidentiality, integrity, availability, and authenticity of information. These measures follow the principle of proportionality, ensuring that protection is appropriate to the level of risk.

Roles and Responsibilities

Information security is implemented in accordance with the three lines of defense model to ensure the principle of segregation of duties.

Information Security Management Framework

The ISMS (Information Security Management System) of Raiffeisenlandesbank Niederösterreich-Wien is designed in line with regulatory requirements, especially following the Digital Operational Resilience Act (Regulation (EU) 2022/2554), and is aligned with recognized standards such as COBIT and ISO 27001.

Key elements for managing information security include:

Strategy

Information security and digital operational resilience strategies that take internationally recognized security standards and security principles into account.

ICT risk management

An ICT risk management framework is applied for the identification, assessment, and treatment of critical ICT risks. An appropriate control system for ICT risks is ensured and integrated into the overall control system.

Policy documents

Policy documents define risk-based security requirements to ensure the objectives of information security. These requirements are regularly reviewed for relevance and to make sure they are up to date.

Education and Training

To promote security awareness among employees, the company implements a targeted awareness and training program. Employees are required to regularly complete web-based training (WBT).

Reporting

Regular reporting on the topics of information security and digital operational resilience is provided to the management body.

Processes for managing ICT-related incidents

To enable a rapid response to ICT-related incidents, policies for ICT incident management have been established, along with processes and corresponding incident response plans that define the necessary steps for incident handling on a case-by-case basis.

Crisis Management

Crisis and emergency plans, as part of the company's business continuity management, are designed to address a wide range of scenarios

Audits and Assessments of Information Security

Being a financial institution, Raiffeisenlandesbank Niederösterreich-Wien is subject to extensive regulatory requirements. As a result, compliance with regulations is audited multiple times per year by various auditing bodies in order to identify deviations and define corrective measures. Audits and assessments are conducted regularly, both internally and externally. The OSINT tool in use enables continuous assessment of the institution's security posture based on publicly available data and supports the early identification and timely remediation of vulnerabilities, compliance risks, and potential attack vectors.

Testing

The regulatory requirements from DORA mandate regular testing to ensure digital operational resilience. These tests are planned, managed, and executed accordingly.

Continuous improvement

The ISMS is continuously updated and improved based on insights gained from its implementation and monitoring. To assess the effectiveness of information security management, key activities and results related to information security are recorded, analyzed, evaluated, appropriate measures are defined and monitored, and represented through key performance indicators. The ISMS is regularly reviewed for effectiveness, and the respective maturity level is determined.

Raiffeisenlandesbank
Niederösterreich-Wien

Contact
Raiffeisenlandesbank Niederösterreich-Wien
Friedrich-Wilhelm-Raiffeisenplatz 1
1020 Wien
E-Mail: info@raiffeisenbank.at
www.raiffeisenbank.at