Raiffeisen Bank International
Member of RBI Group

Group Security

Technical and Organizational Measures

Raiffeisen Bank International
Member of RBI Group

Content

Introduction

Security has top priority for Raiffeisen Bank International. Data from customers and partners are treated with utmost care. To ensure trust in its professional services, RBI has implemented several technical and organizational measures. The rapid changes in technology and its open nature require constant adaptation and improvement of security measures from a technical as well as an organizational point of view. This document provides an overview of what is being done at RBI to protect information as well as technical infrastructure.

Fundamental principles of security

Security aims at providing confidentiality, integrity, and availability of information. All technical and organizational measures at RBI are designed to protect these principles.

- *Confidentiality means that information is not made available to unauthorized individuals, entities, or processes.*
- *Integrity refers to accuracy and completeness of information.*
- *Availability means information being accessible and usable upon demand by an authorized entity.*

Security framework

In order to achieve the set goals, a framework is established and maintained to act as foundation for an efficient Security program. RBI's Security framework and its information security management system consist of the cornerstones identify, prevent, detect, respond, and recover.

RBI Head Office is officially certified according to ISO 27001, the de facto standard for Information Security Management. Therefore, RBI has processes and procedures in place to adequately address and continuously improve Security in a structured way throughout the entire company.

Strategic approach to security

RBI constantly develops and adapts its Security strategy to actively identify, evaluate and minimize new threats and risks.

Organizational measures

In addition to technical measures, processes and the people involved must be taken into account in order to address the issue of security in a holistic manner and appropriately throughout the company.

Security policies: There is a comprehensive framework for security policies defined and maintained. It reflects the requirements of a decentralized network of banking institutions and implements modern standards. The security policies are approved by the Board of Management and must be regularly reviewed to ensure that they are up to date.

Security risk management: Security risks are identified, assessed, prioritized, and addressed. Controls as well as risk mitigation plans are defined, implemented, and tested.

Contact with authorities and stakeholders: RBI is in regular contact and closely cooperates with relevant authorities and interest groups to stay abreast of the latest threats, security trends and regulations.

3rd party risk management: Third-party providers are assessed following a risk-based approach prior to commissioning. Security requirements are contractually agreed if a third-party service poses a potential information security risk.

Security awareness: All employees must regularly attend security awareness trainings. In addition, a variety of events, e-learnings, lectures, and other security awareness-raising measures are offered. The effectiveness of the program is checked, among others, by means of phishing exercises and clean desk checks.

Professional development: Regular training is essential to stay up to date with the latest technologies, standards, and best practices.

Security committees: Security committees, which include board members, the Chief Security Officer, the Chief Information Security Officer, and other relevant persons, meet regularly. These committees are used, among other things, to report and manage information security risks.

Technical (operational) measures

Information and cyber security

To ensure trust in its professional services, RBI protects its business and customer data from unauthorized access, hacking attempts, malware infections, DDoS attacks, ATM fraud, data leakages, phishing attempts, disclosure of sensitive information and other threats using technical measures. Mitigation measures are implemented to ensure an appropriate risk level concerning confidentiality, integrity, availability, and resilience of all systems.

Cyber Threat Intelligence (CTI): Information about new and upcoming threats are collected via threat intelligence providers and analyzed to derive appropriate security measures.

Network security: Systems within networks are protected by technical and organizational measures: The networks are segmented and resilient, network access is secured, and data traffic is analyzed, filtered, and controlled accordingly.

Cryptography: Cryptographic measures such as encryption are in place to protect the confidentiality and integrity of data.

Device security: The devices used, such as notebooks and smartphones, are encrypted and centrally managed. Access to the company network is restricted to authorized devices only.

Anti-malware and SPAM protection: Anti-malware solutions are used to detect, prevent, and report malware, suspicious behavior, and unwanted messages.

Access control, authentication, and authorization: As part of user lifecycle management, defined processes regulate the adding, modification and removal of users and their access rights. Rights are assigned according to the principles of "need-to-know", "need-to-do" and "need-to-have". Access rights are regularly reviewed and adjusted.

Password security: The complexity and length of passwords are set according to best practices. In order to meet the increased security requirements, measures such as two-factor authentication are used wherever possible.

Security testing: Systems accessible from the Internet and critical systems are regularly penetration tested by external, accredited, reputable security companies.

Secure Software Development: Software development follows defined secure software development and secure coding practices based on leading industry standards. Security tests are a mandatory part of the quality assurance process. Access to the source code is strictly limited.

Data classification: RBI has implemented a classification model for data that must be adhered to by all RBI employees. It specifies the level of protection and data processing requirements for each data class.

Data loss prevention: All devices are encrypted, and the use of external media is restricted to prevent data loss or leakage. Data in transit via public networks is encrypted. In addition, there are several measures to detect and block connections to malicious or unwanted websites and content.

Zero Trust: RBI pursues a Zero Trust strategy. Systems, applications, and users are not technically trusted by default. Instead, privileges and access permissions are contextually assigned depending on the current risk. This leads to micro-segmentation, which protects networks against threats such as "lateral movement".

Data masking (anonymization): Data in non-production environments such as test, and development environments is masked to prevent potential misuse.

Vulnerability and patch management: Internal and external vulnerability scans are performed regularly to ensure that vulnerabilities are detected in a timely manner and remediated according to their criticality.

Security monitoring: Security-relevant events from various internal and external sources (such as: server, firewall, IDS/IPS, application logs and indicators of compromise) are collected and correlated in a Security Information and Event Management (SIEM) system.
RBI's internal Cyber Defense Center is an important part of incident detection and supports the incident response process. It provides centralized capabilities to prevent, detect, and respond to cybersecurity incidents. Around the clock, activities on the systems and applications are analyzed for anomalous activity that could indicate a security incident.

Incident management: A defined incident management process is implemented to process security incidents in a timely manner. The process is regularly tested, and the lessons learned are used to improve the process. It is important to return to normal business as quickly as possible and to keep the impact as low as possible.

Business Continuity Management (BCM)

BCM is a framework for identifying an organization’s risk of exposure to internal and external threats.

In RBI, the objective of BCM is to create the ability to respond effectively to threats and to ensure that critical business activities continue to operate despite serious incidents or disasters in order to protect the bank´s business interests. The BCM lifecycle is a continuous cycle that controls the activities of the Business Continuity Program and increases organizational resilience with its implementation.

Policy and program management: The Business Continuity policy provides the framework around which the BCM program is designed and built. It is the key document defining scope and governance.

Embedding Business Continuity: Business Continuity is continually integrated into RBI’s day-to-day business activities and organizational culture through training and education.

Analysis: Objectives, processes, and constraints of the environment in which RBI operates are reviewed and assessed. The main technique used is the Business Impact Analysis.

Design: Appropriate strategies and tactics are identified and selected to determine how continuity and recovery from disruption can be achieved.

Implementation: The agreed strategies and tactics are executed through the process of developing Business Continuity and Response Plans.

Validation: Business Continuity Tests confirm that the BCM program meets the objectives set in the policy**.**

IT resilience: Information and communication technology is critical to all aspects of RBI's operations, both banking and non-banking. Disaster recovery plans ensure that IT systems and their data can be quickly recovered in the event of a disaster. In addition, the resilience of IT is regularly reviewed by executing scenario-based tests.

Crisis management: RBI has established a uniform crisis management standard throughout the Group. The definition of clear lines of communication and escalation makes it possible to react effectively to crises of any kind and to counteract accordingly.

Blackout: Automatic detection and alarm in case of a blackout. Implementation of technical, organizational and personnel measures, that are covered in a Scenario Response Plan (e.g., emergency power supply, satellite devices, guidelines, and manuals, etc.) as well as a respective awareness program for relevant target groups of critical and non-critical areas of the company.

Physical Security

Physical security management restricts physical access to RBI's premises in order to protect data and data systems with a mix of interacting organizational, constructional and technical measures in alayered defense approach.

Security zoning: Premises are categorized in various protection zones. A zone's security level depends on the criticality of assets in it.

Access control management and system: An access control system is used to grant and trace access to the protection zones as well as maintain access permissions.

Security personnel: Security staff is employed to detect or ward off problems at the earliest possible stage and acts as response team in the monitoring center.

Intruder alarm system: An intruder alarm system is used to detect unauthorized entry into any protection zones.

Video surveillance: Video surveillance supports security management in deterring, detecting, and documenting unauthorized access and any kind of inappropriate or unlawful activities.

Secure disposal: RBI enforces a secure waste management to securely eliminate sensitive data. Appropriate means are provided by external sources.