INFORMATION TECHNOLOGY SECURITY

Bank Mandiri navigates complex challenges in data security and cyber threats, given the complexity of technology integration and stringent regulatory requirements. To mitigate these risks, the Bank implements proactive measures such as process automation and stringent cybersecurity policies, supported by regular software updates and employee training. Moreover, a dedicated team is in place to monitor regulatory changes and ensure timely compliance. In addressing resource constraints, Bank Mandiri optimizes resource allocation, fosters strategic partnerships, and invests in IT talent development. These initiatives ensure the Bank remains resilient, innovative, and competitive in an ever-evolving industry.

It has also established a dedicated team to monitor regulatory changes and ensure timely compliance. Addressing resource constraints, Bank Mandiri optimizes resource allocation, fosters strategic partnerships, and invests in IT talent development. These measures ensure the Bank remains resilient, innovative, and competitive in a rapidly evolving industry.

Bank Mandiri has designated a dedicated risk management unit to identify cybersecurity risks, determine mitigation strategies, and monitor their implementation, including ensuring compliance with regulations and best practices in data security management. To raise awareness of the importance of data security and the potential risks of data protection failures, the risk management unit also conducts awareness programs for employees through facilities such as podcasts, posters, and other materials.

To ensure service availability and minimize downtime, Bank Mandiri conducts capacity planning as part of its proactive measures. In terms of cyber incident handling, the Bank has established comprehensive cyber incident response procedures and regularly tests its readiness through activities such as tabletop exercises, switchover simulations, and Adversarial Attack Simulation Exercises (AASE).

INFORMATION TECHNOLOGY SECURITY

As part of its commitment to improving information security quality, Bank Mandiri has developed and implemented a layered IT security strategy. This approach adheres to regulatory requirements (Bank Indonesia and OJK regulations, including POJK No. 11/POJK.03/2022 on IT Implementation by Commercial Banks), aligns with international standards (ISO 27001), and incorporates best practices such as the NIST Cybersecurity Framework, COBIT Framework, and PCI Security Standards. The Bank has also established a 24/7 operational capability to detect and respond to cyberattacks and conducts periodic cybersecurity resilience and security testing.

The implementation of this layered IT security strategy and the development of an information security management system are categorized into three main areas: People, Process, and Technology. A detailed concise explanation of these areas is as follows:

1. **People**
   a. **Security Awareness**
      The Security Awareness Program is carried out to foster awareness on information security in daily behavior which ultimately becomes the Bank's culture. Bank Mandiri conducts security awareness certification every year to all levels of employees in domestic and overseas offices. Routine security awareness campaign programs are also carried out in various media, namely newsletters (monthly), posters (quarterly), podcasts (quarterly), and phishing drills (quarterly). Security awareness campaign program delivered in the form of newsletters has been provided to Mandiri Group entities as a reference for implementing security awareness campaign. Some of the topics of security awareness campaigns include data security protection, maintaining data confidentiality, the latest cyber-attack trends, how to identify and avoid phishing, and online transaction security.

Bank Mandiri also continues to increase customer security awareness with educational programs through various official Bank channels such as websites, social media (Instagram, Facebook, Twitter), and other specific channels.

Campaign Security Awareness

b. Human Resource Development (HR)

Strengthening the people aspect is carried out by continuous skills development (capacity and capability) on human resources. Bank Mandiri provides training & certification to regularly develop soft skills and hard skills to all employees, and vendors/ contractors.

1. Training & certification for employees: CISM (Certified Information Security Manager), CISSP (Certified Information Systems Security Professional), CRISC (Certified in Risk and Information Systems Control), ISO 27001 Lead Implementer, ISO 27001 Lead Auditor, CISA (Certified Information Systems Auditor), CEH (Certified Ethical Hacker), CHFI (Computer Hacking Forensic Investigator), and product-based knowledge training to deepening and expertise on the Bank security system.
2. Training for vendors/contractors: Internal training for vendor employees who work for operational support.

Soft skill development is provided through training such as leadership mindset, strategic thinking, creative thinking, design thinking, problem solving, presentation skill, and negotiation skill.

Training & certification is provided through various methods, both onsite and online (virtual) training through public platforms.

2. Process

a. Three Lines of Defense (3LoD)

Bank Mandiri has implemented a risk management mechanism consisting of three levels of defense:

- 1st line of defense - CISO Office Group, responsible for bank information security through three main functions, namely:
  - Design, designing security architecture and security requirements that are embedded from the beginning of development, implementation to system/application operations.
  - Services, developing, reviewing and disseminating standard procedures, awareness programs and risk management. IT also implements security controls in the IT planning and development process.
  - Operations, conducting 24/7 monitoring, detecting attack threat anomalies and handling information security incidents which include identification, protection, detection, response and recovery of cyber security incidents.
- 2nd line of defense - Operational Risk Group, responsible for developing the bank-wide operational risk management framework.
- 3rd line of defense – Internal Audit, responsible for carrying out assurance functions on operational activities in accordance with internal and regulatory regulations.

b. Security Policy & Procedure

To continuously strengthen cybersecurity processes and infrastructure, Bank Mandiri has designed, implemented, and regularly reviewed its information security strategy through policies and regulations that not only comply with national regulations-such as those set by Bank Indonesia and the Financial Services Authority (OJK)-but also align with international standards and industry best practices, including ISO 27001, the NIST Cybersecurity Framework, CIS Benchmark, and PCI Security Standards.

These information security policies and procedures have also been disseminated to Mandiri Group entities as a reference to strengthen information security governance by tailoring the complexity of each entity's systems.

INFORMATION TECHNOLOGY SECURITY

c. Security Operation Center (SOC)

As part of its preparedness in facing cyber threats, Bank Mandiri has developed the capability to detect and respond to cyber attacks through its Security Operation Center (SOC), which operates 24/7. The Bank proactively monitors and mitigates risks related to cyber attack trends using reputable Threat Intelligence Services and conducts threat hunting on its brand and website to provide online protection against phishing, malware, ransomware, online scams, unauthorized access, and counterfeit threats. Bank Mandiri has also established a Computer Security Incident Response Team (CSIRT), registered with the National Cyber and Crypto Agency (BSSN), to ensure a swift and effective response to cyber incidents. The bank's cyber incident response mechanism is governed by internal policies in accordance with SEOJK No. 29/SEOJK.03/2022 on Cyber Resilience and Security for Commercial Banks, which includes the following stages:

i. Identification and analysis of the incident scope to determine appropriate countermeasures.
ii. Containment through mitigation measures to prevent further damage.
iii. Eradication and recovery, including actions to stop the incident and restore affected systems.

To mitigate the impact of incidents and restore system security, Bank Mandiri has developed a recovery strategy and business continuity management framework, which is governed by the bank's internal policies.

SOC proactively follows up on updates regarding cyberattack trends from reputable Threat Intelligence Services. Following our commitment to monitoring and mitigating cyber risks within Mandiri Group, we regularly share insights from reputable Threat Intelligence Services to all entities. Each entity is responsible for taking appropriate actions based on its specific operational needs and authorities. Furthermore, Bank Mandiri has built internal capabilities to conduct threat hunting, providing online protection for its brand and website against threats such as phishing, online scams, unauthorized access, and counterfeits.

d. Cyber Security Forum

Bank Mandiri's seriousness in monitoring information security is expressed by the direct involvement of the Board of Commissioners and Directors in this topic through the Risk Oversight Committee, Audit Committee and Integrated Governance Committee which are carried out regularly. The agenda of discussion at the committee meeting included reporting on ESG initiatives in the quarterly Privacy & Data Security aspect, multi-layer defense mechanism, and updates related to the cyber security posture fulfillment across Mandiri Group including the implementation of non-negotiable controls to prevent cyberattacks.

e. Cybersecurity Testing

To maintain and evaluate cyber resilience and security while enhancing incident response readiness, Bank Mandiri regularly conducts cybersecurity resilience testing in compliance with applicable regulations (SEOJK No. 29/SEOJK.03/2022 on Cyber Resilience and Security for Commercial Banks), covering:

1. Penetration Testing: Assessment based on vulnerability analysis of operational and business-supporting devices and applications.
2. Phishing Drill: A social engineering attack simulation targeting employees through phishing emails to evaluate their readiness in responding to phishing attempts securely.
3. Adversarial Attack Simulation Exercise (AASE): A real-life hacker attack simulation conducted by an independent consultant to identify potential security gaps in Bank Mandiri's IT operations.

f. Third Party Security Review
To anticipate information security risks from third parties (supply chain) collaborating with the Bank, Bank Mandiri routinely conducts reviews of the information security measures implemented by these third-party organizations (people, processes, and technology) according to the scope of their involvement with Bank Mandiri. These reviews are carried out through various methods, including questionnaires, interviews, and/or site visits.

Furthermore, to measure and evaluate the optimization of the information security process, Bank Mandiri conducted a series of assessment activities by the dependent external assessor, namely the State Cyber and Encryption Agency (BSSN) related:

a. Cyber Security Maturity (CSM) assessment with maturity level 5 – "Optimal" (highest score). CSM Assessment is an instrument from BSSN to assess the level of cybersecurity maturity of an organization, including the assessment of the maturity of management and protection of personal data confidentiality (data privacy).

b. Measurement of Incident Handling Maturity Level (TMPI) with the result of maturity level 5 – "Optimise" (highest value). TMPI is a tool to map the level of organizational readiness in responding to and recovering cybersecurity incidents, including detecting and responding if there is an incident of personal data leakage due to system security gaps.

3. Technology
Bank Mandiri maximizes the implementation of industry-leading security solutions to safeguard information and digital assets through a multi-layered architecture and best-in-class practices, including:

a. Applications accessed by customers and employees: Implementation of Multi-Factor Authentication (MFA) and Web Application Firewall (WAF).
b. Network security: Deployment of firewalls equipped with Intrusion Prevention System (IPS) and Network Access Control (NAC).
c. Endpoint protection (personal computers/ laptops, servers): Use of Endpoint Detection & Response (EDR), antivirus and antimalware solutions, and regular security patches.
d. Access management: Implementation of Identity Access Management (IAM) and Privileged Access Management (PAM) with Privileged Threat Analysis (PTA).
e. Data protection: Adoption of encryption and Data Loss Prevention (DLP) solutions.

As part of its commitment to continuous improvement, Bank Mandiri consistently enhances its IT security capabilities through strategic investments across all security layers, further strengthened by the utilization of artificial intelligence (AI) and machine learning technologies.