Privacy Management, Data Governance, and Information Security

The advancements of the digital era and the adoption of emerging technologies have not only created opportunities but also introduced risks to information security. These include data theft, manipulation, and misuse, which may compromise the confidentiality, integrity, and availability of information. Accordingly, Bank Mandiri places privacy and information security as core elements in the delivery of secure banking services, aimed at safeguarding the Company from potential financial losses, reputational damage, and legal exposures. [FN-CB-230a.2]

Responsibility for Privacy Management, Data Governance, and Information Security

Bank Mandiri assigns responsibility at the level of the Board of Commissioners and the Board of Directors for managing privacy (personal data protection in accordance with the Personal Data Protection Law), data governance, and information security (including personal data in accordance with the Personal Data Protection Law). This responsibility is supported by committees established to assist the Board of Directors in decision-making, in line with the company's internal provisions at the Policy and Standard Procedure levels.

Oversight by the Board of Commissioners and the Board of Directors through these committees is conducted strategically via a structured mechanism. Previously, a Personal Data Protection Steering Committee was established as a manifestation of the Company's commitment to data protection regulation. However, as these matters have now been integrated into Bank's business and operational processes, the performance of privacy management, data governance, and information security is formally discussed and reported within the following board-level committees:

1 Risk Monitoring Committee

This Committee assists the Board of Commissioners with conducting oversight and advisory functions to the Board of Directors. The objective is to obtain reasonable assurance that the implementation of the Bank's risk management remains adequate in terms of risk management procedures and methodologies. The Committee helps ensure that the Bank's business activities are conducted within acceptable risk limits and support a sustainable and profitable performance.

2 Audit Committee

This Committee assists the Board of Commissioners in carrying out its oversight function over the financial reporting process, the effectiveness of internal controls, the implementation of internal and external audits, and compliance with applicable laws and regulations, including matters related to privacy management and cybersecurity. The Audit Committee ensures that audit processes are conducted independently and objectively, and in accordance with prevailing standards, in order to safeguard the integrity and credibility of the Bank's reports.

3 Integrated Governance Committee

This Committee assists the Board of Commissioners in overseeing the implementation of integrated governance within Bank Mandiri's financial conglomeration. The Committee ensures the alignment of policies, strategies, and governance practices between Bank Mandiri and its subsidiaries, thereby ensuring that prudential principles and good governance are consistently implemented across all entities within the Group.

4 Risk Management Committee

This Committee assists the Board of Directors in implementing effective risk management processes and systems by ensuring the adequacy of risk identification, measurement, and monitoring. It also proposes risk management policies and strategies for subsequent approval by the Board of Directors.

Bank Mandiri has also established a Data Governance Body to support an efficient and effective data management strategy. This framework has been developed in accordance with best practices, external regulations, and Bank Mandiri's internal policies, and involves all work units to ensure integrated data management. Management-level oversight is carried out through the Data Steering Forum, which comprises the Director of Information Technology, the Director of Risk Management, the Director of Human Capital and Compliance, the Director of Operations, and relevant Directors/SEVPs. It is responsible for deliberating strategic issues for the Bank, including data governance frameworks, policies, and strategic compliance matters, as well as issues escalated by the Data Governance Council that require recommendations from the Board of Directors or Management.

Detailed information on the responsibilities of the Board of Directors and the Board of Commissioners in their oversight functions related to privacy and information security management is presented in the "ESG Risk Management" section.

Privacy, Data Governance, and Information Security Management Organization

To support comprehensive information security management and cyber resilience across all operational lines, Bank Mandiri has adopted the 3 Lines Model, as follows:

1st Line Model: Chief Information Security Officer (CISO) Office Group, Enterprise Data Analytics, and Data Protection & Fraud Risk Group

Responsible for managing cyber resilience and cybersecurity by implementing operational security controls, ensuring the application of data governance across the Bank, as well as ensuring protection, including controls over personal data processing and compliance with applicable regulations, in order to prevent data breaches and mitigate fraud risks.

1,5 Line Model: Senior Operational Risk Information Technology (SOR IT)

Responsible for conducting testing to assess the effectiveness of the implemented operational controls.

2nd Line Model: Operational Risk Group

Responsible for developing the operational risk management strategy and establishing the related cybersecurity framework.

3rd Line Model: IT Audit Group

Responsible for carrying out internal audit activities (assurance and consulting) to provide an independent assessment of internal controls, the implementation of IT risk management, and IT governance processes within the company's organization.

In 2018, Bank Mandiri established a dedicated unit, namely the Chief Information Security Officer (CISO) Office Group, to manage information security and cyber resilience, operating under the direct supervision of the Board of Directors/ executive management (C-level) to ensure the comprehensive implementation of information security and cyber resilience across all operational lines (bank-wide). The unit adopts a cyber resilience framework that is aligned with international standards and best practices.

In 2024, the Board of Directors approved the appointment of a Personal Data Protection Officer (PPDP) or Data Protection Officer (DPO), along with the establishment of a dedicated work unit, namely the Data Protection & Fraud Risk Group, to support privacy management function. Through this PPDP unit, Bank Mandiri coordinates the implementation of data protection across the Mandiri Group Financial Conglomeration through monitoring activities and guidance provided to its subsidiaries. Bank Mandiri adopts a collaborative approach across relevant work units to ensure optimal data protection.

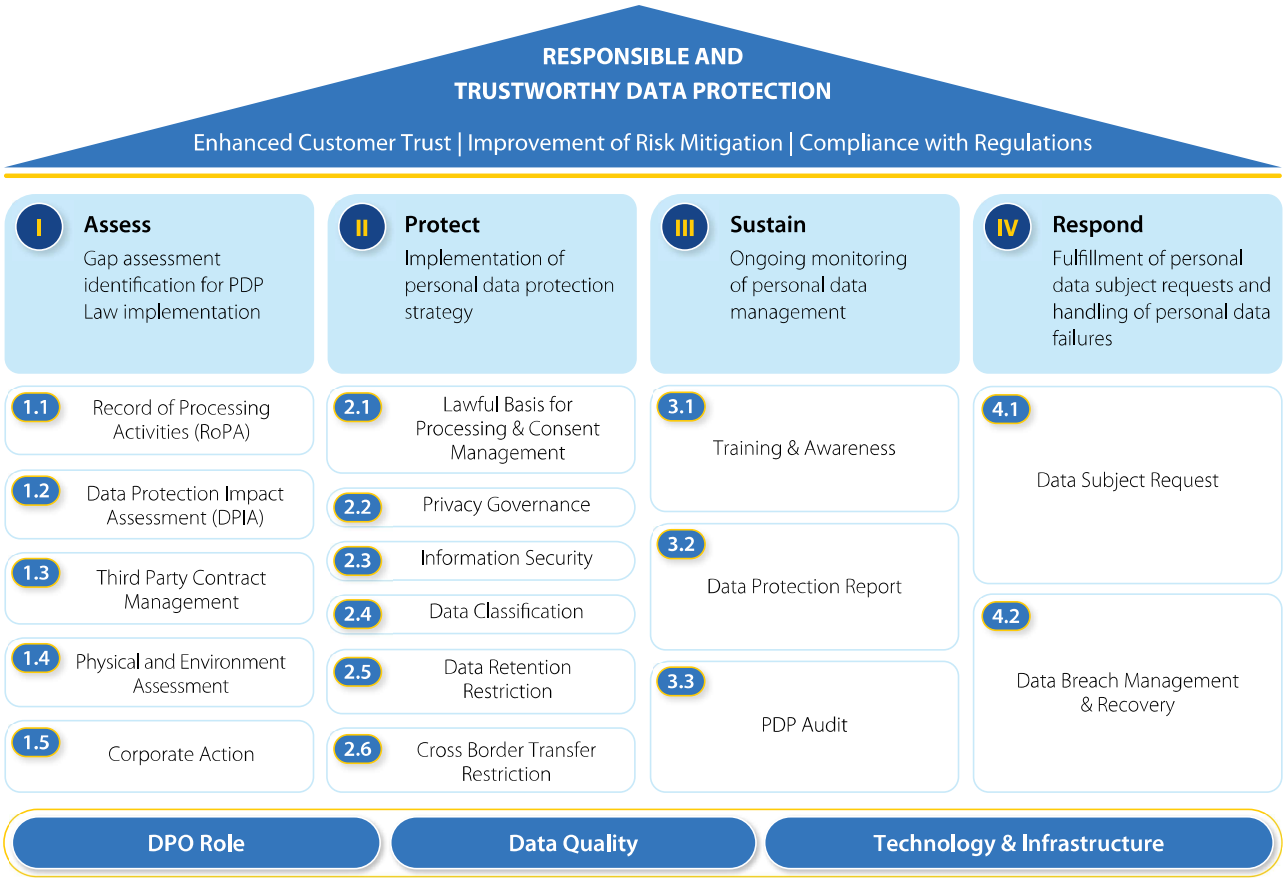
The duties and responsibilities of the unit responsible for privacy, data, and information security governance include the following elements:

Unit	Roles and Responsibilities
Chief Information Security Officer (CISO) Office Group	The management of information security and cyber resilience through: 1. Designing, implementing, and evaluating information security architecture. 2. Managing policies, standards, processes, and baselines related to information technology security in accordance with best practices and compliance with regulatory and government requirements. 3. Ensuring the effective implementation of security reviews in application design, application security testing, and penetration testing as part of information technology application system development requirements under the System Development Life Cycle framework. 4. Identifying and analyzing cybersecurity threats through continuous monitoring functions.
Data Protection Officer and Data Protection & Fraud Risk Group	Implementing risk mitigation measures and personal data protection through: 1. Providing reviews and recommendations to Work Units to ensure compliance with applicable laws and regulations on Personal Data Protection. 2. Monitoring and evaluating compliance with Personal Data Protection laws and regulations, as along with the Bank's policies and/or Personal Data Processors. 3. Advising on Personal Data Protection Impact Assessments and monitoring the performance of relevant Work Units in relation to Personal Data Processing, including other Personal Data Controllers and/or Personal Data Processors. 4. Coordinating and acting as the liaison for matters related to personal data processing. 5. Following up on and developing internal procedures to address requests related to Data Subject Rights, in accordance with applicable laws, regulations and business processes. 6. Issuing and submitting written notifications to Data Subjects and the Personal Data Protection Authority in the event of a personal data protection breach.

Unit	Roles and Responsibilities
Enterprise Data Analytics Group	The Group performs the Data Governance function and serves as Data Steward, by: 1. Ensuring that the Bank's business strategy, development, and policies are supported by accurate and timely data, with a strong orientation toward trends, patterns/data-driven. 2. Ensuring the availability of data management and data governance policies that support the quality of data services across Work Units, strengthening the implementation of data management to maintain data availability, integrity, and integration throughout the organization. 3. Ensuring the effectiveness of reporting provision activities and project initiatives to achieve and realize "Bank Mandiri Data Center /single source of truth within Bank Mandiri". 4. Overseeing work programs related to the development of data management strategies and policies for Bank Mandiri and its subsidiaries, in accordance with established requirements and timelines, and making effective adjustments where necessary to support continuous improvement.
Operational Risk Group	Conducts cyber risk management, by: 1. Providing input to management on the formulation, development, and review of the cyber risk management framework, including strategy, policies, and the adequacy of organizational structures and resources, as well as the implementation of cybersecurity risk management. 2. Monitoring the implementation of the cyber risk management framework established by the Board of Directors and approved by the Board of Commissioners. 3. Conducting testing to assess the impact of the implementation of cyber risk management strategies and policies on the Bank's overall risk profile. 4. Providing review and recommendations on the implementation of cyber risk management to the Board of Directors and/or other Work Units. 5. Developing and implementing a risk awareness program to foster a strong culture of cybersecurity risk management. 6. Coordinating, preparing, and submitting the Bank's Cybersecurity Assessment Report and the Information System Security and Cyber Resilience Report to the regulator on a periodic basis.
SOR IT Group	Performs an internal control function over cybersecurity risk management that is independent from business units, including conducting testing to assess the effectiveness of control implementation.
IT Audit Group	A third-line function that supports the President Director and the Board of Commissioners in carrying out their oversight responsibilities, by: 1. Planning the audit function and conducts internal audit activities focused on IT and cybersecurity, while ensuring the effectiveness of implemented controls. 2. Providing recommendations based on audit results and monitors the follow-up of internal and external audit findings related to IT and cybersecurity. 3. Identifying areas for improvement and enhances the efficient use of IT resources. 4. Providing improvement recommendations and objective information based on the evaluation of controls reviewed at all levels of management. 5. Delivering advisory services and assurance on strategic matters, both during the planning stage and throughout operational implementation.

Privacy Management and Information Security Framework

Personal Data Protection Implementation Framework



Bank Mandiri has established a framework to support the implementation of Personal Data Protection (PDP) with the vision of "Responsible and Trustworthy Data Protection," aimed at enhancing customer trust, strengthening risk mitigation, and ensuring regulatory compliance. In its implementation, the framework is underpinned by four key pillars, namely assess, protect, sustain, and respond.

Assess

1.1. Record of Processing Activities
Identification and documentation of personal data processing activities, including data flow mapping and other information required under applicable laws and regulations.

Protect

2.1. Lawful Basis for Processing & Consent Management
Establishment of the legal basis for personal data processing and the management of consent provided by personal data subjects.

Sustain

3.1. Training & Awareness
Socialization, awareness programs, and mandatory training on Personal Data Protection, taking into account the roles and responsibilities of each Work Unit in personal data processing activities. This includes

Respond

4.1. Data Subject Request
The Bank's response to accommodating the rights of Customer Personal Data Subjects in accordance with the procedures and timeframes stipulated under applicable laws and regulations.

Assess

1.2. Data Protection Impact Assessment (DPIA)
Impact analysis/ assessment conducted to evaluate personal data processing activities that pose high potential risk.

1.3. Third Party Contract Management
Incorporation of PDP clauses and data protection security standards within partnerships with third parties.

1.4. Physical & Environment Assessment
Covers risk management related to physical facilities and the surrounding environment against human threats, disasters, and environmental vulnerabilities, through the implementation of controls such as access cards, access control systems, alarms, and video surveillance (CCTV).

1.5. *Corporate Action*
In the event of mergers, demergers, acquisitions, consolidations, and/ or dissolution of legal entities, Bank Mandiri is required to provide notification to Personal Data Subjects and relevant authorities through Information Disclosure, in accordance with applicable regulations.

Protect

2.2. Privacy Governance
Development of internal policies and provisions related to Personal Data Protection, including the alignment and adjustment of existing regulations with the requirements of the Personal Data Protection Law.

2.3. Information Security
Ensuring the security of processed personal data through:
- The implementation of pseudonymization, encryption, and/ or data masking mechanisms.
- Regular testing and review of security control measures to ensure their effectiveness and sustainability.

2.4. Data Classification
Implementation of data classification mechanisms to protect sensitive and/ or personal data from unauthorized access.

2.5. Data Retention Restriction
Strategies for the deletion or destruction of personal data that has exceeded the retention period.

2.6. Cross Border Transfer Restriction
Policies governing the transfer of personal data outside the jurisdiction of the Republic of Indonesia.

Sustain

the establishment of internal regulations for employees to ensure compliance with the PDP Law, as well as the clarification of key do's and don'ts in the implementation of personal data protection.
Media: newsletters, podcasts, videos, online and offline training sessions, and pulse checks.

3.2. Data Protection Report
Periodic reporting to the Director of Risk Management in the form of a monthly report.

3.3. PDP Audit
Audit processes conducted by independent parties, both internal and external, on the implementation of PDP to ensure compliance with and alignment to applicable laws and regulations.

Respond

4.2. Data Breach Management & Recovery
Handling personal data protection incidents, including reporting to the PDP Authority and notification to affected Data Subjects, in accordance with applicable regulations.

This document subsequently focuses on providing further explanations of several initiatives, namely the Lawful Basis for Processing, Third-Party Contract Management, Data Subject Requests, Information Security, Data Breach Management and Recovery, Data Retention Restriction, and the PDP Audit.

Information Security Risk Management

In managing the bank's information security resilience and security, Bank Mandiri separates the cybersecurity risk management function from the operational management function for cybersecurity resilience and security. This separation is intended to ensure a more strategic, independent, and effective approach to addressing cyber threats. Bank Mandiri establishes the implementation of both functions through the Cybersecurity Risk Management Framework and the Operational Management Framework of Cybersecurity Resilience and Security.

Cybersecurity Risk Management

In order to strengthen the implementation of cybersecurity risk management processes, Bank Mandiri has developed, implemented, and periodically reviewed the Cybersecurity Risk Management Framework. This framework not only complies with national regulations issued by Bank Indonesia and the Financial Services Authority (OJK), but is also aligned with international standards and industry best practices, including ISO 27001, the NIST Cybersecurity Framework, CIS Benchmarks, and the PIC Security Standard.

This framework comprises 3 (three) main pillars. Pillar 1 covers the Cybersecurity Risk Management Strategy, Pillar 2 encompasses the organizational structure related to cybersecurity, and Pillar 3 includes cybersecurity-related policies, procedures, and risk limits, all of which are designed to achieve the cybersecurity objective of Zero Security Breaches.

Cybersecurity Risk Management Framework

Cybersecurity Risk Management Strategy

1. Scope of the Cybersecurity Risk Management Strategy
2. Roles and Responsibilities of Units Related to Cybersecurity
3. Communication of the Cybersecurity Risk Management Strategy
4. Periodic Review of the Cybersecurity Risk Management Strategy

Organizational Structure Related to Cybersecurity

1. Cybersecurity Organizational Structure
   a. Units responsible for cyber resilience and cybersecurity maintain cyber resilience
   b. SKMR is responsible for the implementation of MRKS
   c. The Internal Control Unit performs functions related to testing the effectiveness of controls and providing independent assurance
2. Review of Organizational Adequacy Related to Cybersecurity

Cybersecurity Policies, Procedures, and Risk Limits

1. Cybersecurity Policies and Procedures
2. Cybersecurity Risk Appetite, Tolerance, and Thresholds
3. Documentation and Communication of Policies, Procedures, and Limits
4. Periodic Review of Cybersecurity Policies, Procedures, and Risk Limits

Pillar 1

The Cybersecurity Risk Management Strategy encompasses six (6) key areas as follows:

1. **Comprehensive understanding of cyber risks** and their linkage to the Bank's business, including the level of exposure to cybersecurity-related risks and the Bank's current cybersecurity posture. To foster a strong cybersecurity risk culture, awareness programs are conducted consistently for all employees and customers through all communication channels.
2. **Identification, classification, and prioritization** of critical functions, information technology assets, and system interconnections to ensure a comprehensive and accurate understanding of the cyber risk profile.
3. **Identification of cyber threats and mitigation of cybersecurity issues,** including measures to address potential reputational risks to the Bank. Through Risk Control Self Assessment (RCSA) and robust risk testing, cyber risks are continuously evaluated and appropriate mitigation strategies are implemented. The Bank also conducts ongoing monitoring and undertakes preventive actions to address potential cybersecurity risks.
4. **Security controls** are implemented to protect the Bank's IT assets against evolving cyber threats. To protect IT assets from increasingly sophisticated cyber threats, the Bank implements data security management, endpoint security, and protection of software, hardware, and network infrastructure. In addition, data protection is ensured through effective user access management, whereby only authorized personnel are granted access to sensitive information.
5. **Timely detection of cyber incidents** through continuous oversight and monitoring. The Bank operates a Security Operations Center team to monitor suspicious anomalies or cyber threats perpetrated by cybercriminals, supported by the use of Security Information and Event Management (SIEM) systems and Threat Intelligence thereby strengthening Bank Mandiri's resilience against global cyber threats.
6. **Comprehensive cyber incident response** to support rapid and effective recovery from resulting impacts. This includes timely incident escalation, clear definition of team roles and responsibilities, post-incident analysis, and continuous testing to enhance resilience against future cyber risks.

Pillar 2

Organizational structures related to cybersecurity are established to support comprehensive information security management and cyber resilience across all operational lines. To this end, Bank Mandiri applies the 3 Lines Model.

Pillar 3

Cybersecurity policies, procedures, and risk limits comprise the policies and procedures established by the Bank as part of cybersecurity risk management, as stipulated in internal regulations. The Bank also defines a Risk Appetite Statement (RAS) for cyber risk as part of the operational risk of Risk Appetite Statement on a bank-wide basis. The RAS for cyber risk is further quantified into cyber risk thresholds and monitored on a regular basis.

The Cybersecurity Risk Management Framework is regularly reviewed for continued relevance to business strategy, cyber risk exposure, and the evolving cyber landscape. The review of Pillar 1 focuses on aligning its relevance with the prevailing business strategy and emerging risk developments. Pillar 2 covers the fulfillment of strategies to ensure adequate quantity and quality of human resources in cybersecurity risk management, including staffing, training, certification, talent management, and competitive remuneration. Pillar 3 includes periodic evaluations of the Risk Appetite, Risk Tolerance, and cyber risk thresholds, or ad hoc evaluations when specific conditions arise that require evaluation.

After the Cybersecurity Risk Management Framework was established, and to ensure the effective implementation of cybersecurity risk management, an Information System Security and Cyber Resilience Strategic Plan was developed, which includes a roadmap for the implementation of Cybersecurity Risk Management. The roadmap is subsequently implemented, with each implementation process governed by internal policies. A process-based approach embeds security into every phase, from the initial planning stage (Pre-Operational), to the operational and maintenance stage (Operational), and through to the termination stage (Post-Operational). This approach enables the Bank to act proactively in anticipating and managing risks from the beginning to the end of the process.

During the Pre-Operational stage, the Bank conducts security reviews of products and Information Technology infrastructure prior to launch or deployment. These security reviews are aligned with regulatory requirements and widely adopted IT security standards within the banking industry, as well as other relevant security standards, and continue to evolve in response to emerging risks. In addition, risk identification is carried out from the outset through risk assessments for product initiatives, including cybersecurity risks and third-party dependency risks.

During the Operational and Maintenance stage, cyber risk management is conducted through continuous monitoring of system availability, capacity, and potential vulnerabilities. The Bank maintains monitoring mechanisms and early warning systems to detect anomalies and indications of cyber incidents. Incident management processes are carried out in a structured manner, including impact classification, root cause analysis, and the development of lessons learned to prevent recurrence. To ensure service continuity, the Bank maintains a Business Continuity Plan (BCP), a disaster recovery site, and recovery time objectives aligned with system criticality levels. IT risk management also includes oversight of third-party IT service providers. Prior to engagement, the Bank conducts due diligence on the cybersecurity and resilience aspects of third parties. Risk controls are further strengthened through the inclusion of security clauses in service agreements, periodic compliance monitoring, and the evaluation of concentration and service dependency risks. This approach ensures that external risks do not significantly increase the Bank's overall risk exposure.

During the Post-Operational stage, cybersecurity risk management is conducted through reviews of products and IT infrastructure that are no longer in use and require decommissioning. At a minimum, this includes the deactivation of accounts and network connections of employees, third parties, or subcontractors deemed no longer secure, deletion of sensitive data, revocation of access rights, and termination of all related services.

In addition, as part of the implementation of its cybersecurity risk management strategy, particularly in strengthening cyber resilience and security operations, Bank Mandiri remains committed to continuously enhancing its cybersecurity posture through the implementation of a Comprehensive, Proactive, and Reactive Cybersecurity Framework, built upon three main pillars: Governance and Awareness, Protection, & Operations.

Operational Management of Cyber Resilience and Security

Bank Mandiri strengthens its cyber resilience posture through a comprehensive, proactive, and reactive Cyber Resilience Framework, which consists of three main pillars, namely Governance and Awareness, Protection, and Operations.

Cyber Resilience Framework

Governance and Awareness

1. **Security Awareness**
   Employee education is focused on cybersecurity practices and personal data protection and customer education covers digital transaction security as well as the prevention of fraud and cybercrime (cyber risk awareness).
2. **IT Security Policies & Standards**
   Fostering a strong security culture through the establishment of information security policies and standards that are aligned with applicable regulations and international standards, and consistently implemented across the organization.
3. **Organizational Structure and Personnel**
   Establishing a dedicated cyber resilience operations team through capacity fulfillment and the enhancement of personnel capabilities by obtaining up-to-date professional certifications.

Protection

1. **Defense Mechanisms**
   Digital asset protection using up-to-date technologies, including antivirus solutions, encryption, and access restrictions, as part of a multilayered defense mechanism to prevent cyber threats.
2. **Penetration Test**
   Periodic hacking simulations are conducted to ensure security controls operate optimally.
3. **Access Management**
   Restriction of access to data in accordance with with the prevailing authorities and regulations and the implementation of regular password changes.

Operations

1. **Security Operations Center (SOC)**
   Maintaining system resilience proactively and reactively against cyber threats through 24/7 Security Operations Center (SOC) monitoring.
2. **Cyber Threat Intelligence**
   The process of collecting, analyzing, and leveraging information related to threats and indicators of cyber threat actors to support the Bank in effectively preventing, detecting, and responding to cyberattacks.
3. **Vendor and Supply Chain Security Assessment**
   Evaluating security aspects, including the adequacy and competence of vendors.

Regulation: OJK Otoritas Jasa Keuangan; Bank Indonesia

International Standard: ISO 27001; ISO 17025

International Best Practice: NIST; PCI Security Standards Council; CIS Benchmarks

Bank Mandiri continues to enhance the quality of its cybersecurity risk management and operational cyber resilience management through Information Security Management Certifications, both at the national and international levels, the implementation of adequate internal controls by both internal and external parties, and the measurement and evaluation of information security controls to identify areas for improvement that can be implemented.

Data Governance, Personal Data Protection, and Information Security

Bank Mandiri regards the development of data and information protection as a core component of the corporate sustainability strategy. Bank Mandiri does not rent, sell, or disclose personal data to third parties for purposes other than transaction processing or service delivery, and minimizes risks related to data management through data backup arrangements, risk mitigation measures, and systematic documentation and monitoring. Bank Mandiri has refined its policies by mandating the application of personal data protection principles in accordance with the PDP Law.

Data and Personal Data Protection

Regarding privacy, Bank Mandiri has a comprehensive Personal Data Protection (PDP) policy in the form of Standard Operating Procedures and Operational Technical Guidelines for Personal Data Protection. Personal data protection at Bank Mandiri is also reflected in a detailed Privacy Policy that is accessible to Personal Data Subjects at bmri.id/KebijakanPrivasi, and comprises:

1. Privacy Policy for Individual Customers;
2. Privacy Policy for Corporate Customers

Internal regulations provide for the Personal Data Protection Operational Standards and Technical Operational Guidelines, which govern all aspects of Data Protection. This includes the legal basis for personal data processing, handling of data subject rights requests, recording of personal data processing activities, and reporting in the event of a personal data breach.

In terms of data governance, Bank Mandiri has established and continuously updates Data Management SOPs covering the governance of all data stored in Bank Mandiri's database systems that affect assets and liabilities, including commitments and contingencies. These SOPs regulate data management activities and data governance as the foundation for end-to-end data management processes, encompassing:

1. Data Input Management
2. Data Architecture Management
3. Metadata Management
4. Master Data Management
5. Data Quality Management
6. Data Storage Management
7. Data Development Management
8. Data Modeling Management
9. Data Security Management
10. Data Integration and Interoperability Management
11. Data Provisioning Management
12. Big Data Analytics Management
13. Data Backup Management
14. Content and Document Management
15. Risk Mitigation, Documentation, and Monitoring

Standards and Procedures related to Personal Data Protection and Data Management also stipulate several prohibitions regarding the management of customer data. Examples include:

1. Using personal data of prospective customers whose applications have been rejected, except where there is written or electronic consent from the customer or where required by applicable laws and regulations.
2. Disclosing customer personal data and/or information to third parties.
3. Requiring prospective customers to share personal data as a condition for entering into a product/service agreement.

As part of harmonization with its subsidiaries, Bank Mandiri applies the Mandiri Subsidiaries Management Principles Guideline (MSMPG), which governs information technology and data management practices adopted and aligned across Bank Mandiri's subsidiaries. Oversight of subsidiaries is conducted through Progress Report Monitoring on key PDP activities, including Privacy Governance, Consent Management, and Record of Processing Activities.

Bank Mandiri Privacy Policy

Bank Mandiri informs customers of the purposes and legal bases for personal data processing, with any consent given knowingly and based on a clear understanding. Bank Mandiri discloses its Privacy Policy, which includes details on the legality of personal data processing, the legal basis and purposes of processing, the types and relevance of personal data to be processed, the retention period for documents containing personal data, detailed information on the data collected, the duration of personal data processing, and the rights of personal data subjects.

1 Legal Basis for Personal Data Processing

Bank Mandiri has established legal bases for personal data processing as stipulated in its internal provisions on Personal Data Protection, which include:

1. Consent of the Personal Data Subject to the Privacy Policy, provided through an inseparable consent form.
2. Agreements with the Personal Data Subject.
3. Compliance with applicable laws and regulations.
4. Protection of the vital interests of the Personal Data Subject.
5. Carrying out duties in the interest of public service.
6. Fulfillment of other legitimate interests, taking into account a fair balance between Bank Mandiri's interests and the rights of Personal Data Subjects.

Bank Mandiri manages customer consent for personal data processing by prioritizing transparency and compliance with Law No. 27 of 2022 on Personal Data Protection. The consent management system enables customers to grant, modify, or withdraw their consent.

2 Purposes of Personal Data Processing

In processing personal data, Bank Mandiri only carries out such processing based on the applicable legal bases and purposes that have been approved by the Personal Data Subject.

The purposes of personal data processing and the types of data processed have been comprehensively identified and are set out in Bank Mandiri's Privacy Policy, which include:

1. Management of Bank Mandiri's products, services, and/or offerings, including profiling and scoring, to enhance customer service and support Bank Mandiri's risk management.
2. Provision of Bank Mandiri promotions or programs, which may involve partnership with other parties, for products and/or services already used by customers.
3. Marketing and/or offering of Bank Mandiri's products, services, and/or offerings and/or those of other entities within the Mandiri Group and/or third parties partnering with Bank Mandiri, for products and/or services not yet used by customers.
4. Compliance with applicable laws and regulations, as well as instructions from regulators, law enforcement authorities, and other competent authorities.

3 Types and Relevance of Personal Data to Be Processed

The collection, use, and storage of customer information are carried out in accordance with the principles of prudence and transparency. All data collected by Bank Mandiri is determined based on applicable transaction requirements. Nevertheless, Bank Mandiri is committed to minimizing requests for personal data and ensuring that the data collected is relevant and in compliance with regulatory requirements. The types of personal data processed are set out in Bank Mandiri's Privacy Policy.

4 Personal Data Retention Period

Personal data retention periods are decided in accordance with applicable laws and regulatory requirements.

5 Details of Information Collected

Details of information collected are disclosed under the categories of personal data collected and set out in Bank Mandiri's Privacy Policy. Personal data that may be processed by Bank Mandiri includes identification data, correspondence details, education and employment information, family data, financial data, digital activity data, and personal preferences, which are obtained directly from customers or through third parties in accordance with applicable provisions.

6 Duration of Personal Data Processing

Bank Mandiri processes personal data from the point at which a lawful basis is obtained. Such processing continues for the duration of the use of Bank products, services, and/or offerings, or in accordance with applicable laws and regulations.

Rights Granted to Customers to Control Their Data (Individual/Personal Data Subject Rights)

Bank Mandiri guarantees customers' rights of access, rectification, deletion, correct, destroy, and obtain individual/personal data in accordance with applicable regulations. Bank Mandiri ensures the fulfillment of customers' rights related to individual/personal data management, as set out in its Privacy Policy, which includes the following:

1. **Right to Information and Access**
   Individual/Personal Data Subjects are entitled to obtain information regarding the identity of parties requesting individual/personal data, the purpose of such requests, and access to copies of their individual/personal data.

2. **Right to Data Rectification**
   Individual/Personal Data Subjects have the right to complete, update, and/or correct inaccurate or incorrect individual/personal data.

3. **Right to Obtain, Use, and/or Transfer Individual/Personal Data to Another Party**
   Individual/Personal Data Subjects have the right to obtain, utilize, or transfer individual/personal data held by Bank Mandiri to third parties, provided that the communication systems used by Bank Mandiri and such third parties are secure.

4. **Right to Termination of Processing, Deletion and/or Destruction of Individual/Personal Data**
   Individual/Personal Data Subjects have the right to termination of processing of their individual/personal data, as well as to request deletion and/or destruction of their individual/personal data. Individual/Personal Data Subjects agree to allow Bank Mandiri a reasonable period of time to process the termination of processing, deletion, and/or destruction of individual/personal data to the extent necessary for Bank Mandiri.

5. **Right to Withdraw Consent**
   Individual/Personal Data Subjects have the right to withdraw consent previously granted to Bank Mandiri for the processing of individual/personal data. Individual/Personal Data Subjects agree to allow Bank Mandiri additional time to process the termination of individual/personal data processing, as necessary.

6. **Right to Object to Automated Processing Results**
   Individual/Personal Data Subjects have the right to object to decisions resulting from automated individual/personal data processing that produce legal effects or have a significant impact on the Individual/Personal Data Subject, including profiling and/or credit scoring.

7. **Right to Delay or Restrict Processing**
   Individual/Personal Data Subjects have the right to delay or restrict the processing of individual/personal data in a proportionate manner in accordance with the purposes of such processing. To exercise this right, Individual/Personal Data Subjects may contact Bank Mandiri through the communication channels specified in section H of the Privacy Policy.

8. **Other Rights in Accordance with Applicable Laws and Regulations**
   Individual/Personal Data Subjects are entitled to exercise other rights related to the processing of individual/personal data as provided for under applicable laws and regulations.

Bank Mandiri communicates the mechanism for fulfilling its obligation to respond to requests from Individual/Personal Data Subjects by providing the contents of its Privacy Policy through branches, the corporate website, and other channels that serve as touchpoints for Individual/Personal Data Subjects.

Information Security

In the area of information security governance, Bank Mandiri establishes and regularly updates policies and procedures governing the requirements and mechanisms for managing information security across all of the Bank's information technology systems. These policies and procedures are designed to protect information assets, including customer data, transactions, and operational systems, while ensuring compliance with national regulations, such as those issued by Bank Indonesia and the Financial Services Authority (Otoritas Jasa Keuangan/OJK), as well as international best practices, including ISO 27001, the NIST Cybersecurity Framework, CIS Benchmarks, and the PCI Security Standards. These policies regulate information security activities on an end-to-end basis, covering risk identification, access control, threat mitigation, and continuous monitoring. In detail, Bank Mandiri's information security governance encompasses:

1 Governance

Bank Mandiri establishes and implemts supporting internal policies related to information security management, including:

1. Internal policies on information technology security and cybersecurity, which set out minimum requirements for data and information technology protection, as well as end-to-end security controls.
2. Internal policies on data management, covering governance aspects including data retention, applied bank-wide.
3. Internal policies on monitoring and response for handling cyber incidents.

2 Identify

Bank Mandiri routinely conducts security risk assessments to identify vulnerabilities, potential threats, and mitigation priorities.

3 Protect

Bank Mandiri implements various security controls, including:

a. Network Security
b. Endpoint and Server Security
c. Application Security
d. Identity and Access Management
e. Vulnerability and Patch Management
f. Encryption and Data Loss Prevention
g. System and Configuration Hardening
h. Security Awareness and Training
i. Third-Party Security (Vendor Security)

4 Detect

Bank Mandiri utilizes real-time security monitoring systems supported by a Security Operations Center (SOC) team that operates 24/7. System activities and logs are regularly analyzed to detect anomalies or indications of breaches, enabling fast and structured response actions.

5 Respond & Recovery

Bank Mandiri establishes procedures governing incident handling mechanisms, covering identification, isolation, mitigation, root cause analysis, incident post-mortem (lessons learned), and incident reporting. In addition, the Bank has procedures in place for the recovery of critical systems to ensure service availability is maintained following an incident. Bank Mandiri also conducts cybersecurity testing, including incident response simulations, to ensure team readiness, minimize potential impacts on customers and operations, and strengthen the Bank's capability in managing cyber risks.

Bank Mandiri has Personal Data Protection Policy, Privacy Policy, and Information Security that apply across all business lines/ operational activities Mandiri, covering all financial products delivered through both branch networks and digital platforms. These policies provide protection for customer and vendor data, both domestically and at Bank Mandiri's overseas branches. In particular, overseas branches of Bank Mandiri are also required to comply with the applicable local laws and regulations in each country of operation. In addition, all third parties that cooperate with Bank Mandiri and/or act on behalf of the Bank are required to comply with the security and data protection standards and requirements established by Bank Mandiri in connection with such third-party engagements.

Bank Mandiri conducts evaluations of all internal provisions at least once a year (annual review), or in accordance with regulatory requirements, and at any time there are changes in external regulatory provisions that affect internal policies, or changes in business/operational needs. Bank Mandiri provides an internal platform/application accessible to all employees for obtaining information on applicable policies and procedures.

Artificial Intelligence Management

Bank Mandiri has implemented comprehensive Artificial Intelligence (AI) governance covering traditional AI, generative AI, and next-generation AI. This implementation is regulated under internal provisions on Artificial Intelligence Governance, requiring every AI model to be systematically documented, subjected to rigorous feasibility testing, and monitored on a regular basis. Through this approach, the deployment of AI at Bank Mandiri is conducted in a secure, ethical, transparent manner and in alignment with applicable regulations.

Bank Mandiri has established AI governance framework based on three primary aspects, namely Compliance, Risk Management, and the AI Lifecycle. These three aspects are further reinforced by the foundational pillars of Data Governance, Data Privacy & Protection, Technology & Infrastructure, Cybersecurity, and AI Competency, thereby ensuring that AI implementation within the Bank remains controlled, value-driven, and aligned with sound governance principles.

a. AI Foundation

The AI Foundation comprises the essential components that must be fully established and integrated to support compliance, risk management, and a robust AI lifecycle. The elements of the AI Foundation include:

1. Data Governance: Adequate data governance, including data quality and quantity as well as data security, constitutes a fundamental prerequisite for reliable and responsible AI implementation.
2. Data Privacy & Protection: Any AI system development involving the processing of personal data is required to apply the principle of privacy by design, ensuring that personal data protection is embedded from the planning stage through to system implementation.
3. Technology & Infrastructure: The Bank establishes policies and manages the role of technology and infrastructure to ensure that AI implementation operates securely, efficiently, and in accordance with operational standards.
4. Cybersecurity: Cybersecurity principles are comprehensively applied across all AI systems to safeguard against potential threats and to ensure that such systems operate securely, reliably, and in line with their intended objectives.
5. AI Competency: AI competency is a critical prerequisite in governance, ensuring that the roles and responsibilities of each unit are clearly defined, including the segregation of duties to support effective oversight and management, drive business enhancement, and ensure compliance with applicable regulations.

b. Aspect 1: Compliance

(1) AI Ethics Principles

AI must be developed and utilized in an ethical manner through the following principles:

a. Reliability: AI must be reliable and accurate, and subject to periodic testing to maintain performance quality.
b. Transparency & Explainability: AI-driven decisions must be clearly explainable through proper documentation and informative user interfaces.
c. Security & Resilience: Systems must be designed and operated in a reliable manner and be resilient against disruptions and cyber threats.
d. Accountability: All AI processes and decisions must be traceable through comprehensive documentation and activity logs.
e. Data Privacy: AI must implement privacy by design, encryption, access controls, and comply with personal data protection regulations.
f. Inclusivity, Ethics & Fairness: AI must be developed and applied ethically, without bias that could disadvantage certain groups.
g. Human Oversight: Significant decisions remain under human supervision through mechanisms such as human-in-the-loop, human-on-the-loop, and human-in-command.
h. Sustainability: AI development must take into account resource efficiency and environmental impact.

(2) Regulatory Compliance

AI implementation must comply with all applicable regulations.

(3) Audit

AI audits serve as an oversight instrument to manage risks arising from the use of AI by ensuring that technological implementation is conducted transparently, accountably, securely, and in compliance with applicable regulations.

c. Aspect 2: Risk Management

(1) Risk Identification and Assessment

AI-related risks are identified and assessed to determine the level of risk exposure.

(2) Risk Monitoring

The Bank is required to implement periodic and systematic risk monitoring across all stages of the AI lifecycle, with reference to the established risk identification and assessment results.

(3) Risk Control and Mitigation

Risk control is carried out preventively through the implementation of applicable policies and procedures, as well as through the follow-up of control weaknesses identified during the monitoring process or as a result of incident evaluations.

d. Aspect 3: AI Lifecycle

The AI Lifecycle encompasses the end-to-end management of AI, beginning with strategy formulation and development stages, followed by operational implementation and periodic evaluation, and continuing through enhancement or decommissioning processes based on monitoring results, to ensure performance, security, and regulatory compliance.

Implementation of Personal Data Protection and Information Security within Bank Mandiri

Data Management and Personal Data Protection

Personal Data Management and Protection

Bank Mandiri ensures that any use of data is supported by valid consent or other lawful bases, subject to periodic review. Personal data processing is carried out in a limited manner and strictly in accordance with its intended purposes, while ensuring the accuracy, completeness, and reliability of information. Bank Mandiri also safeguards personal data against loss, misuse, unauthorized disclosure, and alteration or destruction, while clearly informing customers of the purposes of data collection and related processing activities.

Bank Mandiri is committed to managing data independently, including the processing and deletion of data that is unlawful or unintentionally collected. This commitment is implemented through the application of data security management practices that encompass monitoring of asset management, protection during data migration and transfer processes, and data destruction in accordance with applicable procedures. Additional security measures implemented include:

1. Implementing data classification mechanisms to protect sensitive data from potential access by unauthorized parties.
2. Implementing access restrictions and controls over data repositories based on the principle of least privilege to ensure that only authorized parties can access such data.
3. Implementing Data Loss Prevention (DLP) mechanisms across all of the Bank's IT assets that support business activities to prevent the loss of sensitive data or information.
4. Secure file-sharing mechanisms integrated into data management technologies covering data collection, processing, storage, and transfer.
5. Security awareness and risk awareness programs for all employees to ensure adequate human resource capabilities in safeguarding and managing data.
6. Conducting data backups, switch-over, and disaster recovery training to ensure the resilience of data and business-supporting IT assets.

Personal Data Processing Consent Management

Bank Mandiri manages customer consent for personal data processing by prioritizing transparency and compliance with Law No. 27 of 2022 on PDP. A consent management system enables customers to grant, modify, or withdraw their consent at any time as required. Customer consent applies to the offering of the Bank's products and services as well as the selection of communication channels in accordance with customer preferences. Consent provided by customers also serves as the legal basis for personal data processing activities, including the collection, use, storage, updating, and deletion of personal data. Bank Mandiri informs customers of the purposes and legal bases for personal data processing, ensuring that consent is given knowingly and based on a clear understanding. In addition, Bank Mandiri does not use customer data for secondary purposes beyond the scope of approved transactions.

Data Collection, Use, Storage, and Retention

The collection, use, and storage of customer information are carried out in accordance with the principles of prudence and transparency, with all data collected by Bank Mandiri determined based on applicable transaction requirements. Bank Mandiri is committed to minimizing requests for personal data and ensuring that the data collected is relevant and compliant with regulatory provisions, both general personal data and specific personal data.

General Personal Data

1. Full name
2. Gender
3. Nationality
4. Religion
5. Marital status
6. Other personal data that may be combined to identify an individual

Specific Personal Data

1. Health-related data and information
2. Biometric data
3. Genetic data
4. Criminal records
5. Children's data
6. Personal financial data
7. Other data as regulated under applicable laws and regulations

The use of customer data is strictly limited to legitimate banking transaction purposes, in accordance with applicable security and data protection regulations and customer consent. Such data is utilized to support the smooth execution of banking transactions, enhance service quality, fulfill legal obligations, and deliver an improved customer experience through the provision of relevant product and/or service offerings. All data usage is subject to strict oversight and remains in full compliance with applicable data protection regulations.

Referring to Law No. 27 of 2022 on Personal Data Protection (PDP) and internal provisions in the form of Operational Technical Guidelines (PTO) on Data Retention, Bank Mandiri retains personal data in accordance with a retention policy of 30 years after the End of Business (when the customer no longer holds any active products or services with Bank Mandiri). Upon the expiration of the retention period, personal data is destroyed. Bank Mandiri also does not collect personal data from third parties, except where required by law.

Bank Mandiri manages personal data through various channels, including branch offices, call centers, and the Livin' by Mandiri application. Bank Mandiri applies data masking features to sensitive data in accordance with internal provisions set out in the Technical Guidelines on Security Baselines. In addition, Bank Mandiri implements data transmission limitations through Data Loss Prevention (DLP) tools, in line with internal provisions governed by the Technical Guidelines on Data Loss Prevention.

Disclosure and Control of Data to Suppliers and Business Partners (Third Parties)

To safeguard the confidentiality and security of personal data, Bank Mandiri does not rent, sell, or provide personal data to third parties for purposes other than the completion transactions or services, in accordance with applicable laws and regulations. Bank Mandiri also minimizes the disclosure of personal data based on transactional necessity and retains personal data only as permitted under prevailing regulations. Bank Mandiri has established stringent policies governing the disclosure of customer data to ensure regulatory compliance and protect customer privacy, as stipulated in its internal Personal Data Protection provisions issued in 2024.

These policies restrict data disclosure to legitimate purposes only, such as fulfilling legal and regulatory obligations and supporting the execution of banking transactions or services.

Data disclosure is conducted in a limited and consistent manner in accordance with the Company's Privacy Policy and is made only to relevant third parties, including suppliers, regulators, law enforcement authorities, or business partners with appropriate authorization. The policy also governs disclosures to parties such as joint controllers, processors, or other counterparties, subject to strict oversight. In particular, requests for data from law enforcement authorities or regulators are managed in accordance with data management policies governing disclosures related to anti-money laundering (AML), counter financing for terrorism (CFT), or specific audit requirements. Any third-party receiving customer data is required to enter into a confidentiality agreement or Non-Disclosure Agreement (NDA) to ensure the continued protection of such data.

As part of risk mitigation measures related to partnerships with suppliers and business partners (third parties), Bank Mandiri has implemented the following actions:

1. Inclusion of Personal Data Protection clauses in partnership agreements with third parties
2. Establishment of personal data protection security standards as an integral part of partnership agreements, with a focus on security aspects in personal data processing
3. Incorporation of Personal Data Protection implementation requirements into procurement processes through the Partnership Assessment Criteria (PAC)

Data Protection Programs Covering Suppliers and Business Partners (Third Parties)

Bank Mandiri conducts and reviews data security and Personal Data Protection risks related to third parties, including suppliers and business partners, to ensure compliance of the Bank's management of third party cooperation and to strengthen risk controls. Through the CISO Office Group, Bank Mandiri routinely inspects the security performance of third parties in protecting customers' personal information, covering aspects of human resources, processes, and technology to verify their compliance. These inspections are carried out through questionnaires, interviews, and on-site visits to third-party locations.

In addition, as part of Personal Data Protection measures, the Data Protection & Fraud Risk Group implements security safeguards by incorporating contractual clauses related to personal data processing and applying Partnership Assessment Criteria (PAC) in accordance with internal provisions prior to entering into partnership with third parties. This is intended to ensure that third parties use Bank Mandiri's customer information lawfully and in compliance with applicable requirements. The Partnership Assessment Criteria as referred to above include:

1. The existence of internal policies and provisions of prospective vendors related to personal data protection
2. Restrictions on the purposes of personal data processing by prospective vendors
3. Recording of personal data processing activities conducted by prospective vendors
4. Measures for safeguarding and maintaining the confidentiality of personal data by prospective vendors

This is to ensure that third parties use the Bank's customer information legally and in accordance with regulations.

Personal Data Protection Program

One of Bank Mandiri's efforts to ensure compliance with the Personal Data Protection Policy is a personal data protection strengthening program, which is embedded into the Bank's compliance governance, risk management, and technical operational systems through the Personal Data Protection Program (PPDP). In addition, Bank Mandiri periodically evaluates the policies and procedures implemented by relevant units and conducts internal audits as well as audits by independent third parties to assess compliance with the Personal Data Protection Policy.

The comprehensive personal data protection program has been developed by the Data Protection and Fraud Risk Group in coordination with related units, including the CISO Office Group, Enterprise Data Analytics Group, IT Application Support Group, Operational Risk Group, and Human Capital Strategy & Talent Management Group. The personal data protection program covers:

1. Improvement of business processes
2. System development
3. Refinement of internal provisions
4. Organizational strengthening

Bank Mandiri's personal data protection strengthening program covers not only customer personal data, but also the personal data of employees and third parties partnering with the Bank. During the reporting period, Bank Mandiri reviewed its internal regulations and appointed PDP officers, provided Records of Processing Activities, and conducted Data Protection Impact Assessments. The programs implemented included metadata management, data quality improvement, and adjustments to customer requirements, supported by personal data protection training delivered through the Mandiri University Group.

Bank Mandiri also conducted a comprehensive review of its personal data protection program to ensure operational compliance with the PDP Law. In addition, Focus Group Discussions (FGDs) with various associations in Indonesia, international institutions, and consultants to discuss best practices in personal data protection were organized.

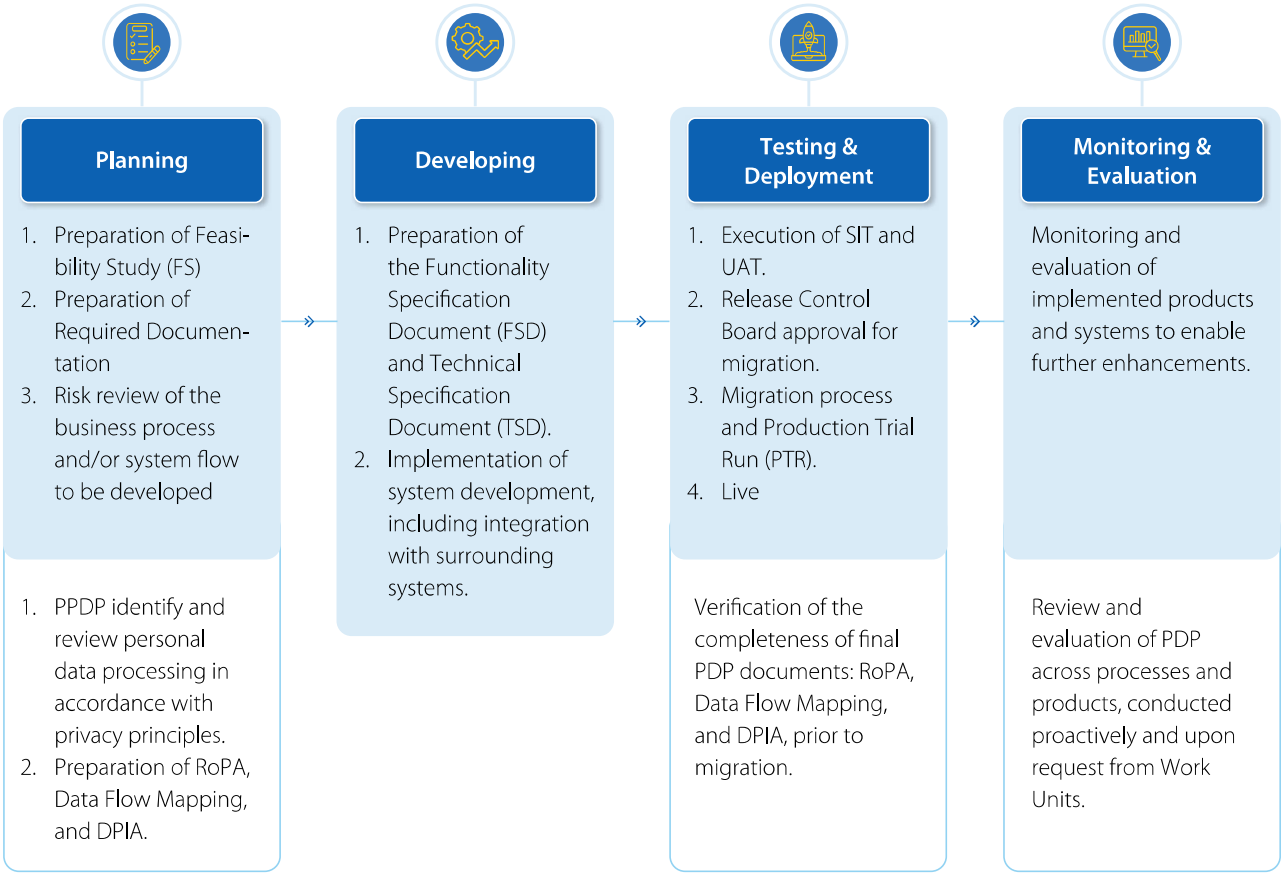
Integration of Data Protection in Product and Service Development

Bank Mandiri integrates data protection into the development of products and services to ensure data security across all business processes, from planning through implementation. Minimum security requirements and standardized security controls to mitigate vulnerabilities during the development stage have been implemented in accordance with internal provisions set out in the Technical Guidelines on Security Baselines, under which every information technology initiative and application development is required to meet established security requirements.

Bank Mandiri has also implemented the Privacy by Design concept, whereby personal data protection is integrated from the development stage. Privacy by Design encompasses 7 main implementation principles, namely:

1. **Proactive not reactive**, personal data protection is implemented to prevent incidents or personal data protection failures.
2. **Privacy by default**, personal data is minimized from the outset of processing by limiting processing to data that is strictly necessary.
3. **Privacy embedded into design**, personal data protection is embedded into the design and planning of products and services.
4. **Full Functionality**, personal data protection does not restrict functionality for services that are not related to personal data processing.
5. **End-to-end security**, data security is applied comprehensively throughout all stages of personal data processing.
6. **Visibility & transparency**, personal data processing is conducted in a transparent and accountable manner.
7. **Respect for user privacy**, personal data processing is user-centric and oriented toward Personal Data Subjects.

Privacy by Design aims to ensure compliance with the Personal Data Protection Law throughout all stages of processing, mitigate the risk of data breaches that may adversely affect the Bank, and optimize the operational effectiveness of personal data protection.



Remarks:

1. Record of Processing Activities (RoPA) is an inventory of personal data processing activities within a product or activity.
2. Data Flow Mapping refers to the mapping of data flows for a specific product or activity.
3. Data Protection Impact Assessment (DPIA) is an assessment of personal data protection related to high-risk personal data processing activities, including the associated mitigation measures.

Information Security Implementation

Bank Mandiri implements various security measures, including encryption, access controls, and regular security audits. The Personal Data Processing Unit ensures the security of customers' personal data by applying physical and electronic data security controls, data retention mechanisms, strict access management, and measures to prevent personal data protection failures. The unit is also responsible for managing data storage locations and media, following up on requests for data copies from data subjects, and recording and adjusting data storage processes as necessary.

Strengthening Information Security

Bank Mandiri adopts a multi-layered defense strategy to ensure information security by protecting applications, networks, and systems using advanced technologies that are continuously updated. The Bank implements a robust cybersecurity system with 24/7 continuous monitoring through an intelligence-driven Security Operations Center (SOC), leveraging machine learning and AI technologies. This monitoring covers endpoints, networks, applications, and servers to detect, prevent, and anticipate cyber threats, including potential data breaches and advanced persistent threats (APTs). The system also enables rapid and effective incident response to minimize impacts on operations and data protection. In addition, Bank Mandiri utilizes Cyber Threat Intelligence services to monitor and detect emerging cyberattack trends, including potential exposure of the Bank's data on the dark web. The Bank also proactively conducts threat hunting activities and takes down fraudulent websites impersonating Bank Mandiri to mitigate cybersecurity risks and protect customer data.

Bank Mandiri's IT security capabilities are enhanced through strategic investments across all security layers, including endpoints, networks, applications, data, and infrastructure. Network and account anomaly detection is strengthened using artificial intelligence and machine learning, while layered and best-in-class security architectures are implemented to safeguard the Bank's systems and data and to identify and block security anomalies at every layer.

1 Endpoint Security

Bank Mandiri implements stringent security measures to address potential vulnerabilities in user endpoints through the application of various security controls, including the use of Virtual Private Networks (VPNs), Network Access Control (NAC), antivirus and anti-malware protection, Endpoint Detection and Response (EDR), disk encryption, and Multi-Factor Authentication (MFA). With respect to server security, both branch servers and data center servers are protected through the application of security patches and anti-malware solutions to ensure system integrity and prevent potential cyber threats. These endpoint security measures are implemented consistently and are continuously monitored and updated.

2 Network Security

Internal network security is strengthened through the deployment of layered and redundant security devices, including Intrusion Prevention Systems, Anti-DDoS solutions, Antispam, Virtual Patch, and Web Application Firewalls. These controls are deployed at both the Data Center and the Disaster Recovery Center to ensure service availability and readiness in emergency situations in accordance with the Business Continuity Plan.

3 Application Security

To identify and address potential security gaps, Bank Mandiri conducts security assessments for all applications under development. The Bank implements a Secure System Development Life Cycle at every stage of system and application development to identify and mitigate security vulnerabilities at an early stage. Bank Mandiri also adopts Agile Development to respond swiftly to business needs. Both approaches are reinforced through Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST). Source code management is carried out centrally through the use of repositories, version control, and secure source code reviews. The Bank also performs penetration testing to assess system resilience against potential real-world attacks, ensuring that vulnerabilities are identified and remediated before new applications or features are deployed.

In addition, Bank Mandiri has digital forensics capabilities to support security incident investigations, post-incident recovery, and the enhancement of its overall security posture. Furthermore, applications accessed by customers and employees are equipped with Multi-Factor Authentication (MFA) and PIN-based transaction security to strengthen protection against unauthorized access and digital transactions.

4 Encryption and Data Protection

Data at Bank Mandiri is protected through encryption during Data-in-Use and Data-in-Transit to prevent unauthorized access. These measures include Secure Managed File Transfer (MFT) for data transfers, Advanced Encryption Standard (AES) for electronic data, and Transport Layer Security (TLS) for communications. Personal data is also safeguarded through Data Loss Prevention (DLP) and Identity and Access Management (IAM), as well as de-identification techniques such as anonymization and pseudonymization.

5 Infrastructure Security

The IT infrastructure is strictly managed through routine activities such as vulnerability analysis, including patching and hardening, penetration testing, and cyberattack simulations.

6 Identity and Access Management

User access rights are managed centrally through Identity Management, while high-privilege access is governed through Privileged Access Management (PAM), which is equipped with Privileged Threat Analytics (PTA) to detect potential threats and generate alerts in accordance with predefined rules.

7 Third-Party IT Security

Bank Mandiri recognizes the information security risks arising from third-party IT service providers engaged by the Bank. Accordingly, the Bank implements risk-based third-party risk management to ensure the adequacy and capability of third-party IT resources across people, process, and technology aspects. Prior to and throughout the engagement, the Bank requires the execution of Non-Disclosure Agreements (NDAs) and conducts vendor security assessments coordinated by the CISO Office. Information security reviews are performed based on the level of vendor involvement and criticality, using methods such as questionnaires, interviews, and/or site visits, to ensure that appropriate security controls are implemented by third-party IT providers.

Encryption is used as a protective measure to prevent unauthorized access to sensitive and personal data. And applied in data management processes, both during data transmission (Data-in-Transit) and when data is at rest (Data at Rest), ensuring that data remains secure from unauthorized parties. Encryption controls include:

1. Data Transfer, using Secure Managed File Transfer (MFT) for data exchange with third parties.
2. Drive Encryption, applying encryption controls to data storage media.
3. Advanced Encryption Standard (AES), encrypting electronic data.
4. Communication Encryption, encrypting communication channels through the implementation of Transport Layer Security (TLS).

User access rights are centrally managed through the Identity Management system. For the management of highly privileged access (power users), Bank Mandiri uses Privileged Access Management (PAM) equipped with Privileged Threat Analysis (PTA) features to detect and generate notifications in accordance with established rules.

Information Security Testing

Bank Mandiri routinely maintains its IT infrastructure security tools by taking into account the technological lifecycle and any obsolescence in the systems in use. Security enhancements are carried out through periodic activities such as vulnerability analysis conducted by independent third parties, including penetration testing and simulated hacker attacks.

To maintain and evaluate cybersecurity resilience and security, as well as to train readiness in incident response processes, Bank Mandiri periodically conducts cybersecurity resilience and security testing in accordance with SEOJK No. 29/SEOJK.03/2022 on Cybersecurity Resilience and Security for Commercial Banks.

1 Vulnerability-Based Testing

Penetration testing for every new application development and periodically for internet-facing and or highly critical applications, at least once a year. Penetration testing is performed by independent external parties holding internationally recognized certifications.

2 Scenario-Based Testing

Scenario-based testing through various activities, including the following:

a. Table-top Exercise

Discussion-based testing involving cross-functional personnel from relevant work units. Each unit discusses response and mitigation measures for cyber incidents in accordance with their respective roles and responsibilities. Tested scenarios include ransomware attacks, illegal hacking, unauthorized access, data breaches, and email-based threats

b. Phishing Drill

Social engineering attack simulations in the form of phishing emails designed to prompt employees to disclose sensitive information, such as passwords. These simulations are carried out using phishing email training tools that automatically distribute simulated phishing emails to all employees. The simulations aim to help employees identify and report phishing emails under conditions closely resembling real-world scenarios.

c. Adversarial Attack Simulation Exercise (AASE)

Real-life hacker attack simulations performed by independent parties to test cyber resilience and to identify potential security gaps and vulnerabilities from people, process, and technology perspectives at Bank Mandiri. One form of its implementation is the Adversarial Attack Simulation Exercise (AASE), which involves attack simulations conducted by independent third parties on the Bank's internal systems. AASE includes testing of third-party connections that interact with the Bank's systems and data through best practices adoption in cybersecurity testing, in line with the prudential principle.

Examples of tested scenarios include unauthorized access, theft of source code from code repositories, interception of unencrypted API communications, disabling of defense systems, and theft of confidential data from data centers. Identified vulnerabilities, including third-party attack surfaces that could be exploited to compromise the Bank's systems and data, become a key focus of Bank Mandiri's continuous improvement program for cybersecurity controls.

Simulation results indicate that attack objectives are not achieved across all scenarios, with all security control aspects receiving a "Good" rating. Reports on the results of cyber resilience and cybersecurity testing are submitted to the Board of Directors and regulators in accordance with applicable requirements. Through these simulations, Bank Mandiri successfully reduces risks arising from third-party attack surfaces while strengthening its overall cybersecurity posture.

Information Security Breach Management

Bank Mandiri uses Data Loss Prevention (DLP) tools, Identity and Access Management (IAM), and Multi-Factor Authentication (MFA) to prevent both intentional and unintentional data leakage. In addition, personal data is safeguarded through de-identification techniques such as anonymization and pseudonymization, ensuring that data cannot be directly identified without authorized access. These proactive measures prevent threats and enable effective incident response, thereby ensuring that customer data protection remains in line with the highest security standards. [GRI 3-3]

Bank Mandiri has the capability to detect and respond to cyber-attacks through a Security Operations Center (SOC) that operates 24/7. The SOC is consistent, effective, and measurable, a reactive response to information security incidents. As a proactive measure, Bank Mandiri conducts continuous monitoring and risk mitigation in response to evolving cyber threats using leading Threat Intelligence Services, and has developed internal through cyber security defender to protect its brand and websites from phishing threats, online fraud, unauthorized access, and impersonation.

Bank Mandiri has a Computer Security Incident Response Team (CSIRT), registered with the National Cyber and Crypto Agency (BSSN), to facilitate collaboration, coordination, and information sharing in the handling of cyber incidents. CSIRT conducts regular testing and security incident simulations to strengthen preparedness in responding to incidents. The SOC team, together with CSIRT, responds swiftly and effectively by carrying out response actions, remediation, or mitigation in accordance with the cyber incident response framework, which generally includes:

1. Identification and analysis of the incident scope and determination of appropriate response measures.
2. Containment, through mitigation processes to prevent further damage.
3. Eradication and recovery, comprising actions to terminate the incident and restore affected systems.

Bank Mandiri not only focuses on incident responses through the CSIRT, but also strengthens early reporting by implementing a clear and documented escalation process through the designated email service provided. This can be used by employees when identifying anomalies related to information security and data protection. Information regarding this reporting channel has been regularly communicated to all employees through posters, newsletters, and podcasts.

Bank Mandiri has also developed recovery and business continuity management strategies to mitigate impacts and restore the security of systems and networks, which are specifically governed under internal policies. Bank Mandiri also maintains digital forensic capabilities to support security incident investigations, facilitate post-incident recovery, strengthen its security posture, and prevent the recurrence of similar incidents. The cyber incident response framework is continuously enhanced based on lessons learned from previously resolved incidents. In addition, Bank Mandiri has mechanisms for handling Personal Data Protection failures (data breaches), as stipulated in internal regulations.

Data Breach Handling Mechanism

Identification	Analysis	Containment	Response and Recovery	Reporting and Lessons Learned
Collecting basic information related to PDP failure incidents based on complaint reports.	Detecting and verifying indications and/or complaints related to incidents based on classification.	Initial mitigation actions in response to indications and/or reports of incidents, based on the results of impact and risk analysis on Personal Data Subjects, to prevent the disclosure of personal data.	Handling and recovering PDP failure incidents based on incident classification and analysis results.	Delivering written notifications to regulators, personal data subjects, and the public in the event of personal data disclosure, as well as submitting reports and documentation to regulators related to PDP failure incidents, whereby such reports are also submitted to the relevant Director and SEVP (board-level committee).

The allocation of roles to work units as module users in handling PDP failures includes the following:

1. Users with the Super Admin and Organization Admin roles are assigned to the CISO Office Group – IT Security Services & Subsidiary Support.
2. Users with the Operator role are assigned to the IT Applications Support Group (Application SMEs) – IT Information and Data Services, IT Wholesale and Supporting Applications, IT Delivery Channels, IT Onboarding and Servicing, and IT Core Banking Systems.
3. Users with the Data Protection Officer (DPO) role are assigned to the Data Protection and Fraud Risk (DFR) Group – Data Protection Operations and Data-Fraud System Monitoring.

During the reporting period, Bank Mandiri recorded no cases of breaches or misuse of customer data and privacy. In over three consecutive years (2023–2025), there have been no information security breaches, resulting in zero impact on customers, clients, or employees. Any complaints related to privacy breaches are followed up in accordance with the applicable incident handling procedures at Bank Mandiri. [GRI 418-1]

In the event of a customer personal data breach, Bank Mandiri promptly handles the incident in accordance with its internal policies governing cyber incident handling and its internal policies on the management of personal data protection failures which include breach notification of the personal data protection failure to regulators and the affected data subjects, as well as other relevant Technical Guidelines.

In the event of a personal data breach, Bank Mandiri undertakes prompt and structured handling in accordance with internal provisions governing the management of personal data protection failures. If the breach is caused by a cyber incident, Bank Mandiri immediately activates the cyber incident response mechanisms as stipulated in the relevant internal regulations.

As stipulated in the Bank's internal regulations on cyber incident handling, the CISO Office Group is responsible for coordinating and managing all stages of cyber incident response, ranging from identification, analysis, isolation, eradication, and recovery, to the conduct of post-incident evaluation and lessons learned once the incident is formally closed. Throughout the incident handling process, Bank Mandiri assesses the impact and urgency level of the incident, which serves as the basis for determining escalation requirements as well as the appropriate form and mechanism of reporting.

This approach reflects a commitment to safeguarding data security, strengthening information technology risk governance, and continuously enhancing cyber resilience.

Awareness and Training on Privacy and Data Security [GRI 404-2] [OJK F.22]

Mandatory training and capability development provided to all employees, vendors, and contractors at least once a year strengthens the management of personal data protection and information security. The training and certifications cover both technical and non-technical competencies, including Certified Information Privacy Manager (CIPM), Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Offensive Security Certified Professional (OSCP), eLearn Security Junior Penetration Tester (eJPT), Computer Hacking Forensic Investigator (CHFI), Palo Alto Networks Certified Network Security Engineer (PCNSE), Certified Network Defender (CND), Certified SOC Analyst (CSA), Certified Encryption Specialist (ECES), cybersecurity awareness training, as well as product knowledge enhancement to deepen understanding of the Bank's security systems.

Personal Data Protection, Information Security, and Cybersecurity Awareness

Information security awareness programs are conducted regularly on a bank-wide basis to enhance understanding and foster a work culture oriented toward information security. These programs include information security campaigns delivered through various media, such as monthly bulletins, quarterly posters, quarterly podcasts, and quarterly phishing simulation exercises. Topics covered include data protection and confidentiality, emerging cyberattack trends, phishing identification and prevention, and secure digital transactions. In addition, Bank Mandiri conducts annual cyber risk awareness certification programs for all employees, vendors, and contractors.

Bank Mandiri implements mandatory learning programs on information security and data protection in the form of e-learning for all employees as part of employee compliance evaluations. The implementation and completion rates of these trainings are systematically monitored to ensure employees' understanding of and compliance with applicable security policies and standards. The programs that have been implemented are as follows:

Phishing Drill

The implementation of information security is key elements in employee performance assessments, evaluated through employees' understanding and responses during training, vigilance in phishing simulations, compliance with information security policies, and awareness of potential cyber threats. The results of this phishing simulation serve to enhance employees' understanding of phishing cyberattacks via email and to strengthen the security culture within the workplace.

Bank Mandiri routinely conducts phishing drills, which are social engineering simulations designed to train employees in recognizing and reporting phishing emails. These simulations use emails containing messages intended to manipulate employees into entering credentials (such as usernames, passwords, or corporate personal email information). Therefore, this is expected to build employees' muscle memory and readiness in responding to real attacks.

During the reporting period, Bank Mandiri implemented various training and awareness programs on personal data protection to enhance employees' knowledge and awareness. All employees, regardless of position or function, are required to participate in training related to information security and data protection. The programs that have been implemented include the following:

Personal Data Protection Awareness Activities

Personal Data Protection awareness is governed under the Operational Technical Guidelines on Personal Data Protection – Awareness. The implementation of awareness activities includes:

1 Personal Data Protection (PDP) Poster

A one-page poster containing quotations or call-to-action messages encouraging employees to be more vigilant regarding potential risks and mitigation measures related to the implementation of personal data protection.

2 Newsletter

Articles/infographics providing comprehensive explanations of risk issues and tips related to personal data protection.

3 Personal Data Protection (PDP) Cartoon

Short, cartoon-style comics featuring light and contemporary content that depicts daily work activities.

4 Personal Data Protection (PDP) Narrative Video

Short-duration videos containing information, calls to action, and awareness messages regarding the implementation of personal data protection, including applicable sanctions.

5 Personal Data Protection (PDP) Pulse Check

Surveys/checklists consisting of short questions for employees regarding readiness for the implementation of personal data protection in each work unit, both at the Head Office and Regional Offices.

6 Personal Data Protection (Consent) Education

Education for customers through social media in the form of videos and posters on Meta, TikTok, Google Android and iOS, and X. Video campaigns are conducted on Meta (consent), TikTok, and Google.

7 Personal Data Protection Guidebook

A summary of policies related to Personal Data Protection, distributed to all employees in the form of a booklet to enhance understanding of the key aspects of Personal Data Protection implementation.

Cybersecurity Awareness Activities

Cybersecurity awareness activities are governed by the Operational Technical Guidelines on Risk Awareness (OPERA) and the Operational Technical Guidelines on Security Awareness. The implementation of awareness initiatives includes:

1 Posters on Operational Risk (including cybersecurity-related risks)

One-page posters containing key messages or reminders encouraging employees to understand and internalize controls over cybersecurity-related risks.

2 Newsletters

Articles or infographics providing explanations of risk issues and corresponding controls related to cybersecurity risks, serving as guidance for all employees.

3 Comics/Cartoons

One-page comic or cartoon articles featuring fictional characters and addressing current operational risk themes, including cyber risks, to reinforce employee awareness.

4 Clips

Short videos highlighting operational risk issues and mandatory controls that employees are required to implement.

5 Checklists

Surveys or checklists consisting of brief questions to assess employees' readiness in implementing personal data protection measures across both Head Office and Regional Offices.

6 Learning Programs

Operational risk management learning modules delivered through online and offline training sessions, e-learning platforms, and employee handbooks.

7 Forums

Broadcasts or live video streaming sessions featuring current operational risk topics, including cybersecurity risk issues, followed by interactive question-and-answer sessions to enhance employee understanding.

Vendor Training and Capability Development

In 2025, Bank Mandiri once again held its annual Vendor Meeting under the theme "Synergizing Growth through Strategic Partnership" to strengthen collaboration with strategic partners. The forum was conducted on 4 December 2025 and attended by 493 vendors, comprising 168 construction vendors, 208 non-IT vendors, and 117 IT vendors.

During the forum, several key topics were presented, including:

1 Vendor-Related Refreshment

A refreshment session on vendor management at Bank Mandiri, including the importance of updating vendor data, ensuring data entry accuracy, and evaluating vendor data that is not updated on a regular basis.

2 Implementation of the Personal Data Protection Law (PDP Law)

A refreshment session on the completion of the Personal Data Protection Partnership Assessment Criteria (PAC), which vendors are required to complete during registration as Bank Mandiri vendors and when undertaking assignments related to Personal Data Protection.

3 Gratification Control and Whistleblowing System Letter to CEO (WBS-LTC)

A refreshment session on anti-gratification provisions as well as the Whistleblowing System - Letter to CEO (WBS-LTC) at Bank Mandiri, including the steps for their implementation within Bank Mandiri.

In addition, Bank Mandiri has developed a Personal Data Protection Playbook for Vendors to facilitate vendors in carrying out their responsibilities within the scope of cooperation related to the processing of personal data, thereby ensuring data security and compliance with the Personal Data Protection Law (PDP Law).

Privacy and Data Security Training in 2025 [GRI 2-24, 404-2] [OJK F.22]

Training Scope

Certified Information Privacy Manager (CIPM), Certified Ethical Hacker (CEH), Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Offensive Security Certified Professional (OSCP), eLearn Security Junior Penetration Tester (eJPT), Computer Hacking Forensic Investigator (CHFI), Palo Alto Networks Certified Network Security Engineer (PCNSE), Certified Network Defender (CND), Certified SOC Analyst (CSA), Certified Encryption Specialist (ECES), Personal Data Protection Law (PDP Law) E-Learning, Implementation of the Personal Data Protection Law in the Banking Industry, Record of Processing Activities (RoPA), Cyber Risk Awareness, product knowledge enhancement to deepen understanding of the Bank's security systems, and other relevant programs.

Number of Training Titles	Total Training Hours	Number of Training Participants
186 Titles	93,220 Hours	42,697 Participants

Discipline and Sanctions for Violations

Provisions on compliance with personal data protection incorporated into the Employee Integrity Pact, under which employees commit to protecting and safeguarding the confidentiality, reputation, credibility, and interests of Bank Mandiri. This also includes an active role in supporting the implementation of personal data protection and preventing the misuse of personal data that could cause harm to individuals or other parties.

Bank Mandiri imposes sanctions on employees who violate and/or fail to fulfill their obligations as stipulated in regulations related to Personal Data Protection. Sanctions are imposed in accordance with the Employee Disciplinary Regulations as governed under the relevant Human Resources Standard Operating Procedures.

Bank Mandiri classifies violations related to privacy, data security, or cybersecurity as breaches of the Code of Ethics. Employees who commit such violations are subject to disciplinary actions in accordance with the Employee Disciplinary Regulations, as stipulated in the Human Resources Standard Procedures (SPSDM). Disciplinary measures may range from a first written warning to termination of employment. For levels and sanctions for Code of Ethics violations, refer to the chapter on Strengthening Governance and Sustainability Commitment.

In addition, Bank Mandiri refers to Law No. 27 of 2022 on Personal Data Protection, Articles 25–46, which regulate administrative sanctions for data controllers. These sanctions include:

1. Written warnings.
2. Temporary suspension of personal data processing activities.
3. Deletion or destruction of personal data.
4. Administrative fines of up to 2% of annual revenue or income, depending on the nature and severity of the violation.

All employees are responsible for information security and personal data protection at Bank Mandiri, as stipulated in the relevant information security and data protection policies and procedures, including:

1. Internal provisions related to information technology and cybersecurity safeguards are applicable to all employees. They include, but are not limited to, the use of strong passwords, the use of standardized work devices, secure network usage, and the obligation to maintain the confidentiality of the Bank's data and information. In addition, all employees are expected to play an active role in preventing cyber risks by promptly reporting any suspicious activities to the CISO Office Group or via email at lapor.ciso@bankmandiri.co.id.
2. Operational Technical Guidelines on Personal Data Protection, covering:
   a. Lawful Basis for Processing (Personal Data Processing Grounds)
   b. Third-Party Contract Management
   c. Records of Processing Activities and Data Protection Impact Assessments
   d. Data Subject Requests
   e. Data Breach Management

Personal Data Protection and Information Security Audit

[GRI G4 FS9]

As part of the Bank's commitment to implementing the principles of Good Corporate Governance and supporting the sustainability of its business operations, Bank Mandiri conducts reviews of information security controls. Subsequently, the audit results are reported to the Board of Commissioners and the Audit Committee.

In 2025, the Internal Audit function conducted audits aimed at ensuring cybersecurity and data security across critical business process areas, namely:

Information Security and Data Privacy Audit

The Information Security and Data Privacy Audit focused on evaluating the adequacy and effectiveness of the information security control framework and personal data management.

Personal Data Protection Audit

The Personal Data Protection Audit directed at assessing the safeguarding of personal data management implementation within business processes, as well as compliance with the Personal Data Protection Law (UU PDP).

Information Security Safeguard Audit

The Information Security Safeguard Audit assessed the effectiveness of security controls and the strengthening of cybersecurity across critical information technology assets and applications, as well as overall cyber resilience capabilities.

The implementation of these audits was designed based on an analysis of key risks that formed the basis for the 2025 Annual Audit Plan (AAP). Accordingly, the audit scope was aligned with the Bank's risk profile, the need to strengthen cyber resilience, strategic priorities, and applicable regulatory requirements.

External Audit [GRI G4 FS9]

Based on the 2025 Annual Audit Plan (AAP), a Data Privacy Audit conducted by an independent external auditor was carried out to evaluate the adequacy and effectiveness of Personal Data Protection controls (Privacy Data Security) and Information System Security, including applications of Payment Service Providers (PJP), as well as cyber resilience.

External independent audits are conducted at least once a year, in accordance with PADG No. 24 of 2024 on Information System Security and Cyber Resilience (KKS), covering a number of critical application systems. This included payment application systems, the standards for which are also governed by Bank Indonesia Regulation No. 23/6/PBI/2021 on Payment Service Providers.

Audits conducted by external parties form part of the independent assurance mechanism over the effectiveness of security controls and cyber resilience. This includes validation of the level of compliance, the effectiveness of the risk management system, and the implementation of personal data protection practices.

The scope of the external audit examination includes the following areas:

1. Governance and Risk Management

The design of operation and risk management controls within policies, standard procedures, and operational mechanism of service systems.

2. Operation and Infrastructure

IT RASS (reliability, availability, scalability, and security) of service systems, infrastructure, and networks in accordance with the business impact analysis.

3. Business Continuity Plan and Disaster Recovery Plan

Disaster recovery planning and testing for critical service systems.

4. Consumer Protection

The design and implementation of controls for handling customer complaints.

5. Information Security and Data Protection

The design of controls over application user access and the safeguarding of superuser accounts in accordance with the principle of least privilege.

6. Fraud Management

The identification of potential fraud at the account, transaction, and network levels, as well as the implementation of anti-money laundering and counter-terrorism financing measures.

7. Management of Goods and/or Services Providers

Security controls over the due diligence process, personal data protection clauses, and the periodic evaluation of vendor performance.

8. Cyber Incident Prevention and Response

The identification of security vulnerabilities, the implementation of detection controls, and the follow-up response to cyberattacks.

Internal Audit [GRI G4 FS9]

Through its Internal Audit function, Bank Mandiri has conducted Personal Data Protection (PDP) Audits and Information Security Safeguard Audits. These evaluated the adequacy and effectiveness of personal data protection safeguards, information security controls, and cyber resilience, particularly across information technology assets and applications that are critical to the Bank's operations, including those of its subsidiaries, as follows:

Personal Data Protection Audit

In 2025, through its Internal Audit function, Bank Mandiri conducted a Personal Data Protection (PDP) Audit to evaluate the adequacy of policies, processes, and controls in the management of personal data. The PDP Audit was carried out with reference to Law No. 27 of 2022, with the audit scope covering the implementation of personal data protection across head office operations, regional/branch offices, and subsidiaries.

The audit was conducted in a phased and risk-based manner, taking into account the characteristics of personal data processing activities within critical business processes. The examination was divided into two (2) phases, as follows:

Phase – 1

The audit focused on assessing the appropriateness of the legal basis for personal data processing and consent mechanisms, as well as the effectiveness of education programs and efforts to enhance understanding (training and awareness) related to PDP implementation.

Phase – 2

The audit focused on evaluating the implementation of PDP within operational processes, including the management of data retention periods and data minimization, the recording of personal data processing activities, and the conduct of initial risk assessments through Data Protection Impact Assessments (DPIA).

In addition, the audit also reviewed the management of third parties involved in personal data processing, as well as the adequacy of personal data information security controls across the stages of data management, storage, and distribution of customer personal data.

Information Security Safeguard Audit

Bank Mandiri has conducted Information Security Safeguard Audits with a focus on strengthening cybersecurity and assessing the adequacy of information security controls. These were carried out based on the risk profile and the criticality level of information technology assets.

Phase – 1

Information Security Safeguard Audit of the Sharia Subsidiary. This examination covered the evaluation of security controls over internet-facing IT assets, particularly business-supporting applications, as well as the adequacy of endpoint security, including servers, laptops, and desktop computers.

Phase – 2

Information Security Safeguard Audit at the Head Office. This focused on Cyber Threat Intelligence, including the evaluation of activities for detecting potential data leakage, identifying external cyber threats, and monitoring and following up on incident alerts.

Phase – 3

This examination covered the evaluation of security controls over internet-facing IT assets of subsidiaries, particularly mobile banking applications, security operations, the implementation of security controls on endpoints, Core Banking Systems projects, and the adequacy of cyber resilience and cybersecurity governance.

Certification

Information Management Systems Certification

ISO/IEC 27001:2022

Bank Mandiri is committed to implementing an Information Security Management System in accordance with ISO/IEC 27001:2022 by applying the principles of confidentiality, integrity, availability, reliability, continuity, and compliance, while emphasizing effectiveness and efficiency through the bank-wide implementation of internal information technology policies.

Bank Mandiri obtained Information Security Management System (ISMS) certification in accordance with the ISO/IEC 27001:2022 standard. In 2025, Bank Mandiri renewed its certification covering information security services provided by the Security Operations Center (SOC) for managing cybersecurity threats across banking systems and cyber operations, the provision of application development and IT operations related to Livin' by Mandiri and Kopra by Mandiri, as well as the provision of Data Center and Disaster Recovery Center infrastructure and operations.

ISO/IEC 17025:2017

Bank Mandiri operates a digital forensic laboratory managed by the CISO Office Group and has obtained certification for compliance with ISO/IEC 17025:2017, as assessed and issued by the National Accreditation Committee (KAN). Examinations are conducted on digital evidence through process stages that include identification, collection, acquisition, and preservation. Through the conduct of investigations and the operation of the digital forensic laboratory, Bank Mandiri has been able to identify the causes, impacts, and risks of incidents affecting the Bank's systems and applications.

Policy Alignment with Subsidiaries

Bank Mandiri aligns with its subsidiaries through the Integrated Governance Committee (KTKT), one of whose key agendas is to ensure consistency in the implementation of Personal Data Protection and information security across subsidiaries, including through the adoption and application of established frameworks and standards. In the area of personal data protection, Bank Mandiri's Personal Data Protection Officer (PPDP)/Data Protection Officer (DPO) also aligns data protection implementation across the Mandiri Group Financial Conglomeration through monitoring and assistance provided to subsidiaries to ensure readiness in implementing personal data protection in accordance with Bank Mandiri's standards. Throughout 2025, Bank Mandiri organized 4 (four) personal data protection forums for all subsidiaries to ensure that personal data protection has been implemented comprehensively and in compliance with applicable laws. In addition, all Bank Mandiri subsidiaries have established privacy policies published on their respective corporate websites.

From cybersecurity risk management aspects, in 2025, Bank Mandiri through its Operational Risk Group, conducted socialization sessions on the Cybersecurity Risk Management Framework with its subsidiaries to align the cyber risk management framework between the Bank and its subsidiaries In addition, the Bank harmonized the cyber maturity assessment methodology with its subsidiaries. This initiative was undertaken to standardize the evaluation mechanism for cyber maturity reports that are regularly submitted to the regulator, thereby eliminating gaps in the assessment process and ensuring that the maturity scores of Bank Mandiri and its subsidiaries are comparable. With comparable results in place, the evaluation of the implementation of risk management practices across Bank Mandiri and its subsidiaries can be conducted effectively and optimally.

In the area of information security, the CISO Office Group works in synergy with subsidiaries on information resilience and security by establishing Mandiri Group information security standards that include non-negotiable controls to anticipate cyber-attacks, while taking into account the system complexity of each subsidiary. Compliance with these standards and controls is monitored and periodically reported to the Boards of Commissioners and Directors of Bank Mandiri and its subsidiaries.

In 2025, the CISO Office Group organized knowledge-sharing forums to further strengthen cyber resilience and information security across the Mandiri Group. In general, information security policies at subsidiaries refer to the information security policies applicable at Bank Mandiri, while remaining tailored to the operational conditions of each entity.

Information Security and Personal Data Protection Policies at Subsidiaries

Mandiri Taspen | https://www.bankmandiritaspen.co.id/article/en-privacy-policy/en

PT Bank Mandiri Taspen (hereinafter referred to as "Bank Mandiri Taspen"), as the Personal Data Controller, is committed to ensuring security and protection to provide a safe and comfortable transaction experience.

With full responsibility, this Privacy Policy details the definitions, types, legality, and purposes of personal data processing. In addition, Bank Mandiri Taspen explains the management and transfer of personal data, the duration of processing, and the procedures for amending the privacy policy.

Bank Syariah Indonesia | https://www.bankbsi.co.id/kebijakan-privacy/bsi

The Privacy Policy of PT Bank Syariah Indonesia regulates provisions related to the acquisition, collection, and other activities concerning Customer Data, including the Personal Data of customers of PT Bank Syariah Indonesia Tbk.

The BSI Privacy Policy applies to all customers and forms an integral part of the terms and conditions applicable to each BSI product and service.

Mandiri Utama Finance | https://www.muf.co.id/kebijakan-privasi/

MUF ensures that customers are informed about how MUF collects, uses, and protects Personal Data when they agree to use the products and/or services provided.

The processing of Personal Data by MUF is intended to facilitate financing applications or product management processes, including profiling, scoring, credit analysis, surveys, and assessment of creditworthiness, conducted in accordance with the principles of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD).

Mandiri Tunas Finance | https://www.mtf.co.id/id/kebijakan-privasi-mtf1access

The MTF Privacy Policy applies to each product and/or service offered by MTF that can be utilized, used, or accessed by customers through financing facilities for any type of financing.

MTF makes every effort to ensure that customers' personal data remains secure and confidential, in accordance with the applicable laws and regulations on personal data protection.

AXA Mandiri Financial Services | https://www.axa-mandiri.co.id/en/web/customer/kebijakan-privasi

AXA Mandiri innovates to enhance customer transaction experiences while safeguarding personal data through tailor-made protection, simplified information, and streamlined procedures. AXA Mandiri is responsible for maintaining the security and confidentiality of customers' personal data in accordance with applicable laws and regulations.

AXA Mandiri is committed to protecting customer data by implementing physical, technical, and organizational measures to prevent unauthorized access, use, or disclosure. Personal data will not be provided or disclosed without consent, and customer identities are verified prior to any access to or modification of data.

Mandiri Sekuritas | https://www.mandirisekuritas.co.id/en/privacy-policy

Mandiri Sekuritas safeguards the privacy and security of customers' and prospective customers' personal data in accordance with applicable laws and regulations. The privacy policy covers various aspects of personal data management, ranging from data collection and use to data disclosure when customers use or access Mandiri Sekuritas' electronic systems. The policy also includes detailed provisions regarding customer preferences, including data collection, use, and tracking, cookies, data transfer and disclosure, data security, the use of third-party service providers, links to other websites, and the applicability of the privacy policy.

Mandiri Capital Indonesia | https://mandiri-capital.co.id/kebijakan-privasi

MCI provides information on its privacy policy on its website, including the collection and use of personal information such as names, addresses, and email addresses that are voluntarily provided by visitors. Such personal data is used to enhance services for customers in accordance with applicable laws and regulations. While customers are not required to provide all personal data, the absence of certain information may affect access to features on the website. MCI also collects data through cookies and statistics to understand visitor behavior and improve service quality. Users have the right to disable cookies when accessing the website.

Bank Mandiri (Europe) Ltd. | https://www.bkmandiri.co.uk/media/2024/12/2-Privacy-Policy.pdf

Bank Mandiri (Europe) Limited protects customer privacy through the implementation of a clear privacy policy. This policy outlines procedures to safeguard data confidentiality, including the use of cookies, and ensures that all communications and personal identification information are not disclosed without consent or beyond the provisions set out in the privacy policy. Any inquiries related to privacy are also governed under this policy to ensure the security of customer data.

Mandiri International Remittance Sdn. Bhd. | https://www.mandiriremittance.com/privacy-policy/

The Privacy Notice of Mandiri International Remittance Sdn. Bhd. (MIR) explains the use of customers' personal data. MIR ensures that the processing of personal data complies with the Personal Data Protection Act 2010. This notice applies to personal data voluntarily provided by customers when accessing MIR services, as well as to the website and all products and services offered. The policy governs the purposes and types of personal data, disclosure, security, storage, integrity, and the principles of access to personal data processed by MIR.