shopping method to evaluate the consistency of Bank Mandiri's service standards across all contact points.

Bank Mandiri's service performance in 2024 showed growth with a Customer Satisfaction Score (CSAT) of 86.11, a Net Promoter Score (NPS) of 67, and a Service Excellence Survey (SES) score of 91.52.

To further improve complaint handling quality, the Company, in collaboration with independent parties, also conducted customer satisfaction surveys regarding complaint handling within Bank Mandiri and the industry. Two specific indicators were measured in detail, with the survey results as follows:

Customer Satisfaction Scores

Indicator	Bank Mandiri	Industry*
Satisfaction score for complaint handling	8.6	8.6
Satisfaction score for the duration of complaint resolution	8.5	8.4

*Bank Group Based on Core Capital Tier IV

The results of the survey indicate that Bank Mandiri's customer satisfaction score is higher than the average satisfaction level in the banking industry.

Bank Mandiri is committed to consistently making improvements to continue providing the best services to customers, thereby enhancing customer satisfaction and loyalty.

Privacy Management, Cybersecurity, and Data Protection

The ease of transactions enabled by the digital era and the adoption of the latest technologies brings not only opportunities but also risks to information security. These risks include theft, manipulation, and misuse of data, which can threaten the confidentiality, integrity, and availability of information. Bank Mandiri places privacy and information security as key elements in delivering secure banking services. The topic of Customer Data Security and Privacy has been selected as one of the primary material topics, reflecting its significant impact on business sustainability and stakeholder trust. To address this, Bank Mandiri continuously mitigates these risks to safeguard against potential financial losses, reputational damage, and legal actions. [FN-CB-230a.2]

Responsibilities for Managing Privacy, Cybersecurity, and Data Protection

Bank Mandiri has established responsibilities at the Board-Level Committee for managing Privacy, Cybersecurity, and Data Protection (including personal data in accordance with the Personal Data Protection Law), as stipulated in the company's internal regulations at the Policy and Standard Procedure level. These responsibilities include overseeing Committees Under the Board of Directors, which are formed to assist the Board of Directors in making decisions aligned with the vision, mission, and strategy of Bank Mandiri.

Oversight by the Board of Directors and Board of Commissioners related to the Management of Privacy, Cybersecurity, and Data Protection:

1. Risk Management Committee
   This committee is formed to assist the Board of Directors in implementing effective Risk Management processes and systems by ensuring adequate identification, measurement, and monitoring of risks, as well as the establishment of risk management policies and strategies.

Structure of Risk Management Committee

Chairperson	Vice President Director
Secretary	Group Head of Credit Portfolio Risk
Alternate Secretary	Group Head of Market Risk
Permanent Voting Member	1. Vice President Director 2. Director of Compliance & Human Resources 3. Director of Network & Retail Banking 4. Director of Operations 5. Director of Finance & Strategy 6. Director of Information Technology 7. Director of Risk Management 8. SEVP of Information Technology 9. SEVP of Wholesale Risk
Non-Permanent Voting Member	Members of the Board of Directors and SEVPs related to the subject matter attending as invitees

2. Risk Monitoring Committee
This committee was established to assist the Board of Commissioners in carrying out its supervisory duties and providing advice to the Board of Directors. Its role is to ensure that the Bank's risk management implementation remains aligned with adequate procedures and methodologies. By maintaining proper risk management practices, the committee helps ensure that the Bank's business activities remain within acceptable and profitable limits.

Members, Duties & Responsibilities of the Risk Monitoring Committee

Member	1. Risk Monitoring Committee consists of at least three (3) members, comprising Independent Commissioners and Non-Commissioner Independent Parties. 2. The composition of the Risk Monitoring Committee includes at least 1 (one) Independent Commissioner serving as Chairperson and member, with expertise in finance, risk management, and/or business, 1 (one) Non-Commissioner Independent Party with expertise in finance, 1 (one) Non-Commissioner Independent Party with expertise in risk management.
Duties and Responsibilities	1. Monitoring and evaluating risk management policies (including implementation and compliance with regulations). 2. Reviewing risk profile reports, bank health reports, and other types of risk reports. 3. Providing recommendations to enhance the effectiveness of risk management. 4. Conducting regular meetings with relevant work units. 5. Reporting supervision results periodically to the Board of Commissioners. 6. Preparing and reviewing work guidelines regularly.

3. Steering Committee for Personal Data Protection
This committee was established as a commitment to compliance with data protection regulations. It is responsible for formulating strategies and defining measures to fulfill obligations under the Personal Data Protection Law.

Members, Duties & Responsibilities of the Steering Committee for Personal Data Protection

Members	1. Director of Compliance & Human Resources 2. Director of Information Technology 3. Director of Risk Management 4. Members of the Board of Directors, SEVP, Group Heads, and Department Heads related to the subject matter, attending as invitees
Duties and Responsibilities	1. Providing guidance on strategy and the effectiveness of Personal Data Protection implementation Bankwide. 2. Conducting mapping, assessment, and all necessary actions to align Bank Mandiri's operations/activities with the provisions of the Personal Data Protection Law.

Active Oversight by the Board of Directors and the Board of Commissioners

Strategic oversight by the Board of Commissioners and the Board of Directors is carried out through a structured mechanism. Every quarter, data security and privacy performance is discussed and formally reported in the Risk Monitoring Committee, Audit Committee, and Integrated Governance Committee forums. These discussions include ESG achievements related to data privacy and security, the effectiveness of layered security systems, and compliance with Mandiri Group security standards. This mechanism ensures holistic information security management aligned with the Company's strategic objectives.

In addition, the Steering Committee for Personal Data Protection has been established as a testament to Bank Mandiri's commitment to data protection regulations. The Steering Committee is responsible for formulating strategies and establishing measures to fulfill obligations under the Personal Data Protection Law (PDP Law).

Furthermore, Bank Mandiri has established a Data Governance Body to support the corporate strategy through the implementation of an effective and efficient data strategy. This data governance framework is structured based on best practices, external regulations, and Bank Mandiri's internal policies. Additionally, this governance framework involves all business units within Bank Mandiri to ensure integrated and optimal data management.

To support the comprehensive management of information security and cyber resilience across all operational lines, Bank Mandiri implements the 3 Lines of Model, which includes:

1st Line of Model: Chief Information Security Officer (CISO) Office Group

Responsible for managing cyber resilience and security by implementing operational security controls.

1.5 Line of Model: Senior Operational Risk Information Technology (SOR IT)

Responsible for testing the effectiveness of implemented operational controls.

2nd Line of Model: Operational Risk Group

Responsible for developing the framework and strategy for cybersecurity risk management.

3rd Line of Model: IT Audit Group

Responsible for conducting independent assurance, including periodic verification and review of the implementation of cybersecurity risk management.

In 2018, Bank Mandiri established a dedicated unit, the Chief Information Security Officer (CISO) Office Group, to manage information security and cyber resilience. This unit operates under the direct supervision of executive management (C-level) to ensure comprehensive implementation of cybersecurity resilience across all operational lines of the Company (bank-wide). In its operations, the unit adopts a cyber resilience framework based on international standards and best practices, ensuring readiness to face the ever-evolving cyber threats.

Furthermore, to support the implementation of the PDP Law at Bank Mandiri, the Board of Directors has approved the appointment of a Personal Data Protection Officer (PDPO) or Data Protection Officer (DPO) and the establishment of a dedicated work unit to support the functions of the PDPO.

In line with efforts to comprehensively manage information security, data privacy, and cyber resilience, Bank Mandiri adopts a collaborative approach across relevant work units to ensure optimal data protection. The information and data security governance structure at Bank Mandiri includes the following key elements:

Unit	Duties and Responsibilities
Chief Information Security Officer (CISO) Office Group	Managing information security and cyber resilience by: • Designing, implementing, and evaluating information security architecture. • Managing regulations, standards, processes, and baselines based on best practices and compliance with information technology security requirements from regulators and the government. • Ensuring the effective implementation of security reviews in application design, application security testing, and penetration testing within the IT application system development framework under the System Development Life Cycle. • Identifying and analyzing cybersecurity threats through continuous monitoring functions.
Data Protection Officer and Data Protection & Fraud Risk Group Work Unit	• Review and provide advice to Work Units to ensure compliance with the provisions of laws and regulations regarding Personal Data Protection. • Monitor and evaluate compliance with laws and regulations on Personal Data Protection, as well as the Bank's policies and/or Personal Data Processors. • Provide recommendations regarding the impact assessment of Personal Data Protection and monitor the performance of Work Units related to Personal Data Processing, including other Personal Data Controllers and/or Personal Data Processors. • Coordinate and act as the point of contact for matters related to Personal Data processing. • Follow up and develop internal procedures to address requests from Personal Data Subjects' Rights while adhering to applicable laws and regulations as well as business processes. • Declare and deliver written notifications to Personal Data Subjects and the Personal Data Protection Authority in the event of a Personal Data Protection failure.
Enterprise Data Analytics Group	The work unit responsible for carrying out tasks and duties as Data Governance and Data Steward. • Supporting the accurate and timely implementation of strategies, development, and business policies of the bank, while being trend-oriented and data-driven. • Ensure the data management and data governance provisions that guarantee the quality of data provided to other work units. • Ensure the effectiveness of reporting activities and project initiatives aimed at achieving and realizing the Bank Mandiri Data Center / single source of truth at Bank Mandiri. • Ensure that bank business strategies, development, and policies are data-driven, focusing on trends or data patterns, so that strategy implementation becomes more accurate and timely. • Oversight the work program related to the development of strategies and policies for data management at Bank Mandiri and its subsidiaries, in accordance with the specified requirements and schedules, and make necessary adjustments for improvement.
Operational Risk Group	Work unit responsible for managing cybersecurity risk. • Provide input to management in the formulation, development, and enhancement of the cybersecurity risk management framework, including strategy, policies, and organizational adequacy. • Develop and refine procedures and tools for implementing cybersecurity risk management. • Design and implement necessary controls to strengthen cybersecurity measures. • Monitor the implementation of the cybersecurity risk management framework as established by the Board of Directors and approved by the Board of Commissioners. • Conduct assessments to evaluate the impact of cybersecurity risk management strategies and policies on the Bank's overall risk profile. • Provide recommendations for cybersecurity risk management implementation to the Board of Directors and/or other relevant units. • Prepare and submit periodic cybersecurity risk management maturity assessment reports to regulators. • Review proposals for new products and emerging technologies developed by specific units within the Bank, focusing on assessing their potential impact on the Bank's overall cybersecurity risk exposure.

Privacy and Data Protection Policy

To ensure compliance with regulations and safeguard personal data, Bank Mandiri implements a Personal Data Protection (PDP) Policy and Privacy Policy, as outlined in internal policies in the form of Memorandum on Personal Data Protection. This policy governs all relevant business lines/operations of Bank Mandiri, including overseas branches, customers, and vendors. This policy also applies to all financial products, whether account openings are conducted through branch offices or digital platforms. To harmonize data management across subsidiaries, including data privacy and security, Mandiri Subsidiary Management Principle Guideline (MSMPG) establishes data management provisions that can be adopted and aligned by subsidiaries. A component of Bank Mandiri's Privacy Policy, namely the Individual Customer Privacy Policy and the Privacy Policy of Customer of Entity, can be accessed at the following link: bmri.id/KebijakanPrivasi.

All internal policies of Bank Mandiri are reviewed as needed, at a minimum of once per year (annual review), or in accordance with regulatory requirements. Reviews are also conducted whenever there are provisions or changes issued by external regulators that impact Bank Mandiri's internal policies or when there are changes in business or operational needs. To ensure implementation across all employees regarding privacy and cybersecurity, as well as to raise awareness of the threats and the importance of these issues, Bank Mandiri has established internal policies in the form of standard procedures on information technology and data management as the primary guidelines. These are further supported by internal policies in the form of technical guidelines on data retention and security baseline, serving as operational technical guidelines. Internal policies in the form of standard procedures related to information technology also regulate various aspects of information technology security and cybersecurity. Meanwhile, internal policies in the form of standard procedures related to data management focus on data governance across all Bank units, both domestically and internationally. Specifically for overseas branch offices, in addition to adhering to the provisions of these standard procedures, they are also required to comply with the regulations applicable in each operational country.

Personal Data Protection Strengthening Program

The personal data protection strengthening program is integrated into Bank Mandiri's bank-wide compliance governance system, risk management, and technical operations through its Personal Data Protection Program (PPDP) to ensure adherence to regulatory standards and internal policies. Periodic evaluations are conducted on the policies and procedures implemented by relevant units, along with internal audits and audits by independent third parties to ensure compliance with the bank's Personal Data Protection Policy.

To enhance data security, Bank Mandiri implements various protection measures, including encryption, access control, and regular security audits. Through the Personal Data Storage Implementation Unit, Bank Mandiri ensures the security of customer personal data by applying physical and electronic data security controls, data retention mechanisms, strict access management, and prevention of data protection failures. This unit is also responsible for managing storage locations and media, addressing requests for data copies by data subjects, and recording and adjusting storage processes as needed.

The complexity of implementing personal data protection impacts all operational activities, including those involving customers, employees, and third parties. A comprehensive personal data protection program has been developed in collaboration with the Data Protection and Fraud Risk Group, CISO Office Group, Enterprise Data Analytics Group, IT Application Support Group, Operational Risk Group, and Human Capital Strategy & Talent Management Group. The program focuses on four key areas:

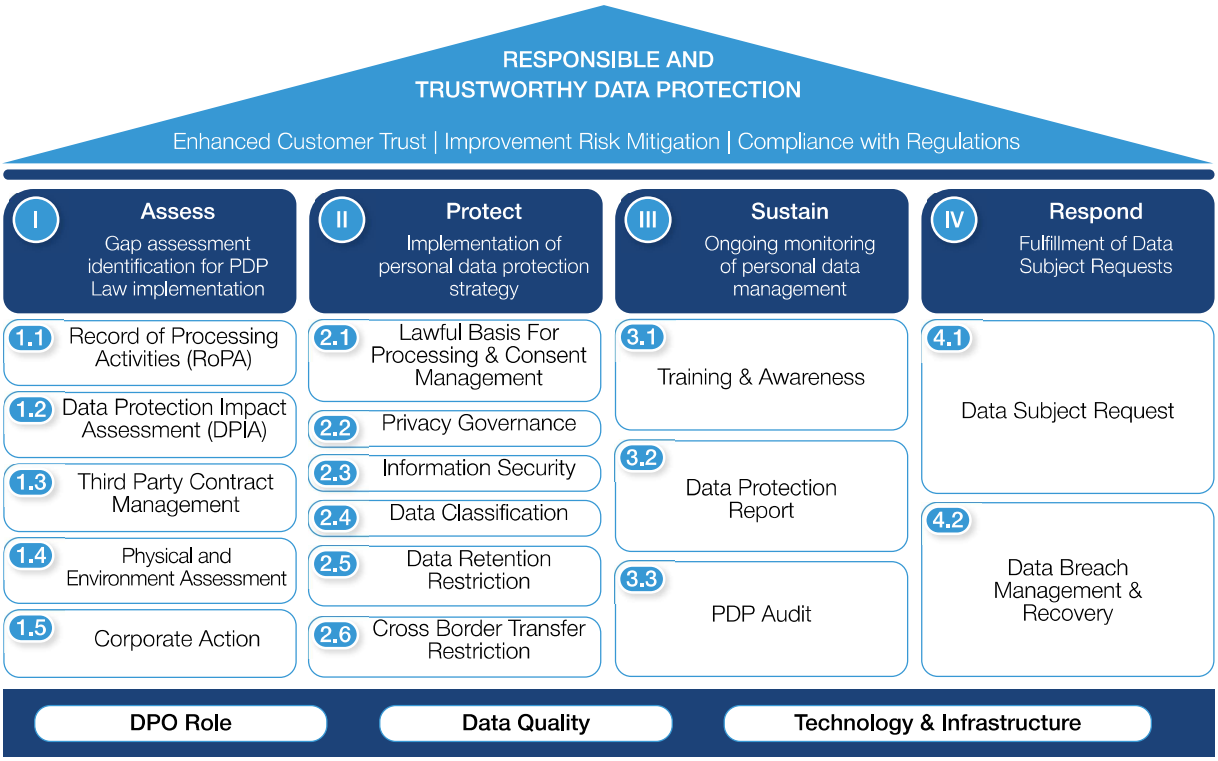
1. Business process improvement;
2. System development;
3. Enhancement of internal regulations, and
4. Organizational strengthening.

Bank Mandiri's personal data protection strengthening program covers not only customer personal data but also employee and third-party data associated with the bank. The personal data protection strengthening program is integrated into Bank Mandiri's compliance governance system, risk management, and technical operations through PPDP, ensuring adherence to regulatory standards and internal policies. To enhance security, Bank Mandiri implements various protective measures, including encryption, access control, and regular security audits.

During the reporting period, Bank Mandiri reviewed internal regulations, appointed Personal Data Protection (PDP) officers, provided a Record of Processing Activity (ROPA), and conducted Data Protection Impact Assessments (DPIA). The implemented programs included metadata management, data quality improvement, and adjustments to customer requirements, supported by personal data protection training through the Mandiri University Group.

Bank Mandiri continuously conducts comprehensive reviews of its personal data protection program to ensure operational compliance with the Personal Data Protection Law (PDP Law). Bank Mandiri also organizes focus group discussions (FGDs) with various associations in Indonesia, foreign institutions, and consultants to discuss best practices in personal data protection.

Framework for the Implementation of Personal Data Protection



Bank Mandiri has established a framework to support the implementation of Personal Data Protection, with the vision of "Responsible and Trustworthy Data Protection." The framework aims to enhance customer trust, improve risk mitigation, and ensure compliance. In its implementation, this framework is supported by four main pillars: assess, protect, sustain, and respond.

The four supporting pillars in the data protection framework implemented by Bank Mandiri are:

Assess

1.1. Record of Processing Activities
Identification of the processes for recording personal data processing, including mapping data flows and other detailed information as required by law.

Protect

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

Sustain

3.1. Training & Awareness
Socialization, awareness, and mandatory training on Personal Data Protection, considering the involvement of each work unit in personal data processing activities.

Respond

4.1. Data Subject Request
A response from the Bank in accommodating the rights of Data Subject customers in accordance with the procedures and timeframes set by the applicable laws and regulations.

Assess

1.2. Data Protection Impact Assessment (DPIA)
An analysis/ assessment conducted to evaluate personal data processing activities with high potential risks.

1.3. Third Party Contract Management
Adding PDP clauses and security protection standards in agreements with third parties.

1.4. Physical & Environment Assessment
Includes risk management for physical facilities and environments against threats and vulnerabilities, such as human factors, disasters, and environmental risks, by implementing controls like access cards, access control, alarms, and video surveillance (CCTV).

1.5. Corporate Action
In the event of mergers, splits, acquisitions, consolidations, and/ or the dissolution of legal entities, the Bank must notify the Data Subjects and relevant authorities through information transparency.

Protect

2.2. Privacy Governance
The creation of internal provisions related to Personal Data Protection and the adjustment of existing provisions to comply with the Personal Data Protection Law.

2.3. Information Security
Ensuring the security of processed personal data through:
- Pseudonymization, encryption, and/or data anonymization mechanisms
- Routine testing and review of security control measures to ensure effective and ongoing activities.

2.4. Data Classification
Implementing data classification mechanisms to protect sensitive data (including personal data) from being accessed by unauthorized parties/ individuals.

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

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

Sustain

The establishment of internal regulations for employees to comply with the provisions of the PDP Law, highlighting the do's and don'ts in the implementation of personal data protection.

Media: Newsletter, Podcast, Video, Online & Offline Training, Pulse-check.

3.2. Data Protection Report
A periodic report to the Director of Risk Management in the form of a monthly report, and reports to Management in the Data Protection Steering Committee.

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

Respond

4.2. Data Breach Management & Recovery
Handling personal data protection failures and reporting them to the PDP Authority, as well as notifying the Data Subjects of the personal data protection failure.

Privacy Governance in Information Security and Data Protection

In line with technological advancements and the increasing risks to information security, Bank Mandiri continues to enhance data and information protection as part of its corporate sustainability strategy. Bank Mandiri does not rent, sell, or provide data in any form to third parties, except for the purpose of financial transactions/services. The bank minimizes data backup management, risk mitigation, as well as documentation and monitoring. As a concrete step, Bank Mandiri has refined its policies to mandate the application of personal data protection principles in accordance with PDP Law. The scope of the policy and the implementation of personal data protection principles are outlined in the internal policy through the Memorandum of Procedure on Personal Data Protection.

Bank Mandiri consistently updates its SOPs for Data Management, which regulate the processing of personal data. This includes processing data in accordance with the purposes agreed upon by customers, data retention periods, processes for receiving and sending data to external parties, and data deletion. The data protection policies outlined in the SOPs cover all data stored within Bank Mandiri's database systems, which impact assets and liabilities, including commitments and contingencies. These SOPs govern data management activities and establish data governance as the foundation for an end-to-end process, encompassing:

- Data initiation management;
- Metadata management;
- Master data management;
- Data quality management;
- Data storage management;
- Data development management;
- Data security management;
- Data provisioning management;
- Big data analysis management;
- Data backup management.

Internal policies, which include Standard Operating Procedures related to Data Management and Personal Data Protection, also regulate several prohibitions concerning the management of customer data. Some of these prohibitions include:

1. Prohibiting the disclosure of customer data and/or personal information to third parties;
2. Forcing potential customers to share data as a condition for product/service agreements; and
3. Using personal data of potential customers whose applications have been rejected. Exceptions apply only if there is written or electronic consent from the customer or based on legal provisions.

All policies and procedures related to information security and data protection are internally available for all employees. To support this, Bank Mandiri provides internal access through its POPCORN (Policy and Procedure Corner) online platform. This platform facilitates easy access for employees to applicable policies and procedures, ensuring consistent and comprehensive implementation in maintaining information security and data protection.

Information Security and Data Protection Implementation at Mandiri Group

Bank Mandiri has developed the Mandiri Subsidiaries Management Principles Guideline (MSMPG), which includes provisions governing collaboration on information technology and data management with its Subsidiaries. This guideline aims to create sustainable value while adhering to the principles of good corporate governance and the Articles of Association of each subsidiary. All policies and procedures are periodically reviewed to ensure their relevance to technological advancements, operational needs, and applicable regulations. Policies implemented at subsidiaries must align with those of Bank Mandiri as the parent entity.

MSMPG addresses various aspects, including aligning information technology security architecture to ensure corporate security and regulatory compliance; and data management that promotes the implementation of integrated management information systems and data governance in accordance with applicable regulations. Data governance at subsidiaries must also align with Bank Mandiri's data governance framework.

As the parent entity, Bank Mandiri has aligned and synergized with its subsidiaries in the areas of information resilience and security, as well as personal data protection within the Mandiri Group conglomerate, through the implementation of monitoring and assistance provided by each subsidiary. For information resilience and security, the CISO Office Group collaborates with subsidiaries by establishing Mandiri Group's information security standards, which include controls to anticipate cybersecurity attacks that are non-negotiable, considering the complexity of each subsidiary's systems. Compliance with these standards and controls is monitored and reported to the Board of Commissioners and the Board of Directors of Bank Mandiri and the subsidiaries on a regular basis. In 2024, the CISO Office Group will also organize a knowledge-sharing forum as part of the ongoing strengthening of cybersecurity resilience within the Mandiri Group.

Furthermore, regarding data protection, Bank Mandiri, through the Personal Data Protection Officer (PPDP) / Data Protection Officer (DPO), also coordinates the implementation of data protection across the Mandiri Group Financial Conglomerate through monitoring and assistance provided to the subsidiaries. In 2024, Bank Mandiri will organize a workshop for all subsidiaries to ensure that the implementation of Personal Data Protection has been comprehensively carried out and complies with the law. In this regard, all subsidiaries have implemented privacy policies that are listed on their respective corporate websites.

The information security policies at the subsidiaries are based on the information security policies in place at Bank Mandiri, while taking into account the operational conditions of each entity.

The information security and data protection policies at