Policy and Governance of Information Technology

Bank Mandiri makes IT Governance a guideline in IT planning, development and operational processes. IT Governance is implemented by adopting the Regulations of Financial Services Authority and Bank of Indonesia while considering character and business strategy of Company. Bank Mandiri always guarantees that the IT governance continuously be improved in accordance to the developments through the implementation of periodic review.

IT Governance framework at Bank Mandiri is illustrated in the following chart:

Information Technology Planning includes IT strategic plan, IT development architecture, annual IT planning, as well as strategic research and study

Standardization of IT Strategic Initiative Project and IT Non-Strategic Initiative (Changer Request and Service Request) development by prioritizing quality of projects

Information Technology Security includes physical and environment security, communication security, access control security, and cryptography security

IT Operational Management includes operating system management, media back-up management, file report management, and system management.

The provisions related to IT Management at Bank Mandiri are set forth in the Standard Operating Procedures (SOP) and Technical Instructions (TI) which generally regulate the following:

1. **IT Standard Operating Procedures (IT SOP)**
   IT SOP is Information Technology Governance Guidelines starting from the planning, development, operational management to end-to-end IT safeguards that apply at Bank Mandiri including at Foreign Office as to be in line with the applicable regulations and best practices and is aligned with the business process improvement while paying attention to the principle of confidentiality, integrity, availability, reliability, continuity, and compliancy having regard to the principles of effectiveness and efficiency.

   IT SOP is a rule containing provisions and/ or procedures as a description of Bank Mandiri Operational Policy. The IT SOP refers to Regulator provisions as well as Internal Bank provisions.

The founding of Regulatory Provision is:
- Law of the Republic of Indonesia No. 10 of 1998 concerning Banking.
- Law of the Republic of Indonesia No. 19 of 2016 on Amendment to Law No. 11 Year 2008 concerning Information and Electronic Transactions.
- Government Regulation (PP) No. 82 of 2012 concerning the Implementation of the Electronic Transaction System.
- Financial Services Authority Regulation No. 38/POJK.03/2016 dated December 1, 2016 concerning Application of Risk Management in the Use of Information Technology by Commercial Banks.
- Circular Letter of the Financial Services Authority No. 21/SEOJK.03/2017 dated June 6, 2017 concerning Application of Risk Management in the Use of Information Technology by Commercial Banks.

Whereas in terms of Internal Bank, IT SOP is based on Bank Mandiri Operational Policy, Decree of Risk Capital Committee - Operational Risk Committee

(RCC - ORC) dated December 21, 2012 and Decree of the Procedure and Policy Committee (PPC) dated December 12, 2018.

2. **Technical Instructions (TI) related to IT**
   It is a provision regulating the stages of technical or process of implementation based on IT SOP. The IT SOP are as follows:

   a. **IT Planning**
      It is a work unit guideline in carrying out information technology planning that includes information technology strategic initiatives planning, annual information technology planning processes, information technology research processes and strategic studies, and information technology architecture planning processes.

   b. **IT Project Management**
      It is a guideline in the stage of developing the IT Strategic Initiative Project so each process of development phase execution is standardized while still prioritizing the quality of each project.

   c. **IT Operations Management**
      It is a guideline that regulates the management of IT Operations, including the management of system operations, management of backup and restore processes, management of infrastructure, and the process of monitoring and maintaining the system.

   d. **IT Security**
      It is a work unit guideline on aspects of IT security, including physical and environmental security, network security, application system security, and corporate security.

   e. **Use of IT Service Providers**
      It is a guideline that regulates the process for selecting Information Technology service providers and their evaluations.

   f. **Management of Source Code**
      It is a guideline that regulates the process of storing source code which includes the source code whether or not owned by the bank and is stored at the escrow agent.

In addition to periodic adjustments to policies and procedures, the implementation of good IT Governance requires a balance between aspects of People, Process and Technology. The performance frameworks adopted by Bank Mandiri are as follows following:

Control Objectives for Information and Related Technologies (COBIT)
Bank Mandiri IT adopted COBIT framework in order to provide a standard framework for IT Governance management practices and objective IT Related Enabler control instructions to connect business processes, controls and operational activities as a reference for business owners, auditors, and users. Bank Mandiri IT has exceeded the maturity level in accordance with the provisions of the Minister of BUMN No. PER-02/MBU/2013.

International Organization for Standardization 20000 (ISO 20000)
International Standard used in the management of IT Services that aims to improve the institution service quality by improving work process. Since 2014, Bank Mandiri has managed to get Certification for ISO 20000 and in 2017 Bank Mandiri managed to hold (recertification) ISO 20000 for the next three years within the scope of "The Service Management System of IT Applications Support Group and IT Infrasructure Group of PT Bank Mandiri (Persero), Tbk. That Supports Internal Customers at Jakarta Headquarter."

International Organization for Standardization 9001 (ISO 9001)
The implementation of a quality management system can help Bank Mandiri to improve its overall performance and provide a strong foundation for sustainable improvement initiatives. Bank Mandiri has held certification for ISO 9001 since 2003 within the scope of: "Operation and Development of Data Centers, DRC, IT Security and Infrastructure" that asissts Bank Mandiri to deliver reliable and secure banking services.

In 2017, Bank Mandiri IT has successfully upgraded ISO 9001: 2008 into ISO 9001: 2015. In ISO 9001: 2015, there is an additional new clause to ensure that the implementation of Bank Mandiri IT quality management increase, which in turn can be a guarantee of quality banking services. In 2018, Bank Mandiri maintained to hold ISO 9001 certification.

Improvement of Information Security Capability

The Information Security strategy is carried out through the development of capabilities as a continuous improvement effort for increasingly challenging business needs while considering the security, reliability and internal capabilities of IT. The strategy is implemented by focusing on 3 (three) areas, namely Governance, Protection and Operation with the following explanation:
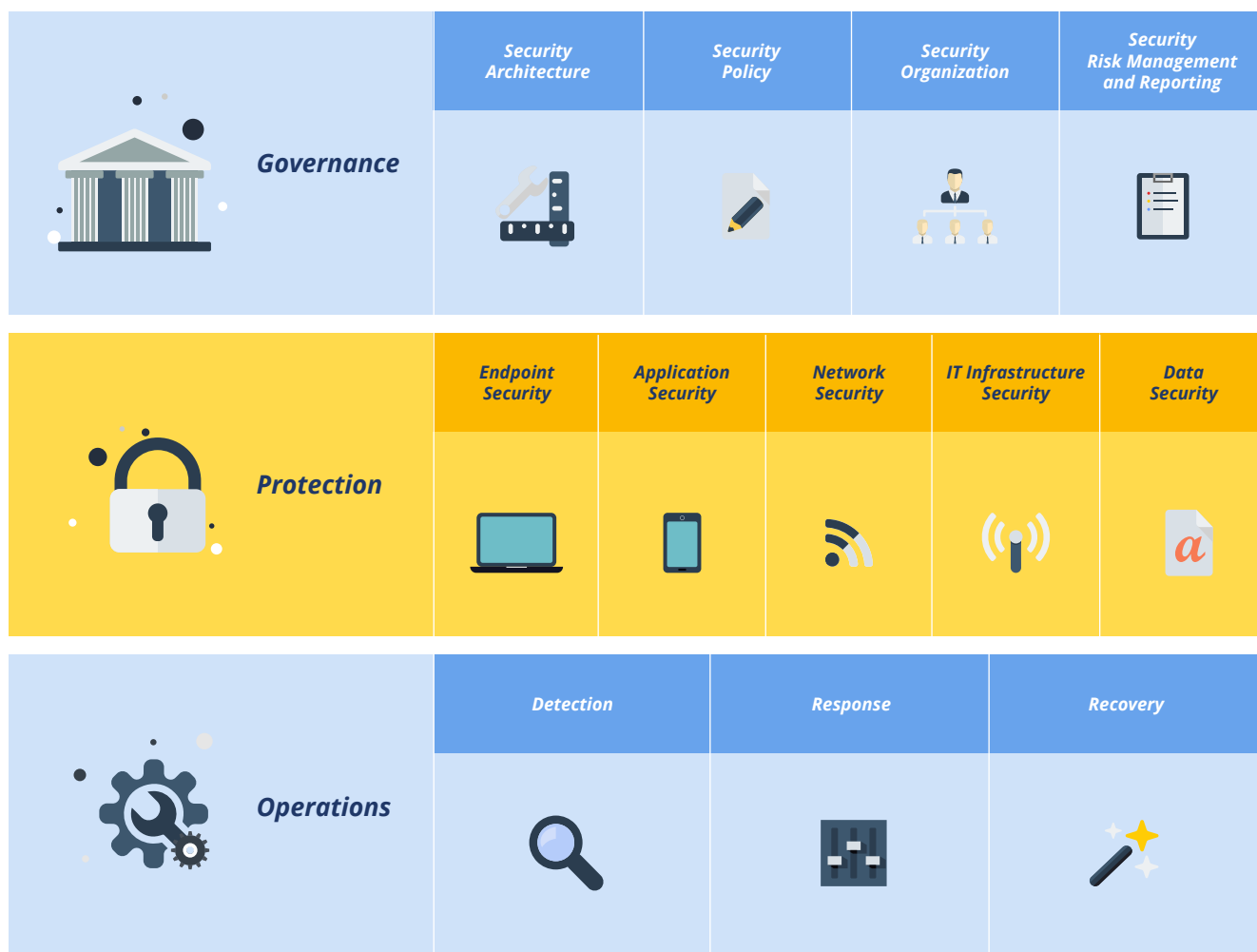
- **Governance**
  Ensuring that the implementation of Information Security runs well by paying attention to internal policies and applicable regulatory provisions on best practices. This area is developing in terms of security architecture, security policy, security organization and security risk management and reporting.

- **Protection**
  Implement Information Security at Infrastructure, Applications and Data layers to ascertain the principle of confidentiality, integrity and availability run well. The implementation of Information Security is carried out in terms of endpoint security, application security, network security, IT Infrastructure security and data security.

- **Operations**
  There are 2 (two) stages of operations, namely detection efforts through the implementation of security assessment and security operation center that runs 1x24 hours to monitor events and incidents at any time and increasing the ability to respond to cyber security threats through incident response and digital forensic.

Governance	Security Architecture	Security Policy	Security Organization	Security Risk Management and Reporting
Protection	Endpoint Security	Application Security	Network Security	IT Infrastructure Security	Data Security
Operations	Detection	Response	Recovery

Information
Technology | Corporate
Governance | Corporate Social
Responsibility | Cross
reference POJK | Cross
reference ACGS | Financial
Report

Audit to Guarantee Security and Reliability of Information Technology

In the process of evaluating IT policies and governance at Bank Mandiri, IT Audit work unit, which is one of the work units under the Internal Audit Work Unit (IAWU), is involved. Evaluation is carried out to ascertain that the management of the Company's IT is carried out in accordance with internal policies, applicable regulatory provisions on best practices. In addition, Audit IT has a role in ensuring the effectiveness of controls in planning, developing and implementing IT. The scope of the audit carried out by Audit IT includes IT Strategy and Governance, IT Operational, IT Infrastructure and Network and IT Security and Forensic. In carrying out its functions, Audit IT is supported by resources that have international certification namely Certified Internal Audit (CIA), Certified Internal Information System Auditors (CISA), Certified Information Security Manager (CISM), Certified in Governance of Enterprise IT (CGEIT), Certified Information Systems Security Professional (CISSP), Certified Data Center Professional (CDCP), Certified Ethical Hacker (CEH), Cisco Certified Network Professional (CCNP), and Microsoft Certified System Engineer (MCSE).

In 2018, there were several improvements made by Bank Mandiri through the IT Audit recommendations as follows:

* Updating policies, procedures and operational management to ensure compliance with the applicable regulations.
* Improving management and quality of data to improve the efficiency of project management and accurate reporting.
* Improving quality of security of application systems and its infrastructure to prevent the risk of fraud, misuse of customers data and other incidents.
* Improving control on applications to prevent problems in banking transactions.

Development Strategy Information Technology in 2018

In 2018, Bank Mandiri IT focused on developing IT capabilities based on the Re-Aligned IT Strategy and Execution Plan (ISP) 2017 - 2020 so as to support Bank Mandiri business services. The focus of the development was through channel development that enabled the provision of omni-channel and seamless experience for customers, developing data warehouse capabilities and big data to analyze information effectively and efficiently, optimize core banking to improve system stabilization, and develop system capabilities to support sales, marketing, and campaign management in offering banking products and services according to customer needs.

The IT Tranformation program that has been carried out during 2018 has been running well, covering 3 (three) stream is run the bank, change the bank, and transform IT. Each stream has resulted in an increase quality of IT management that is able to support Bank Mandiri's banking business processes significantly. Going forward, Bank Mandiri will continue to focus on continuing IT Transformation, specifically related to security, readiness, IT system reliability, IT strategic initiatives and improving IT capabilities to improve competitiveness Mandiri Bank.