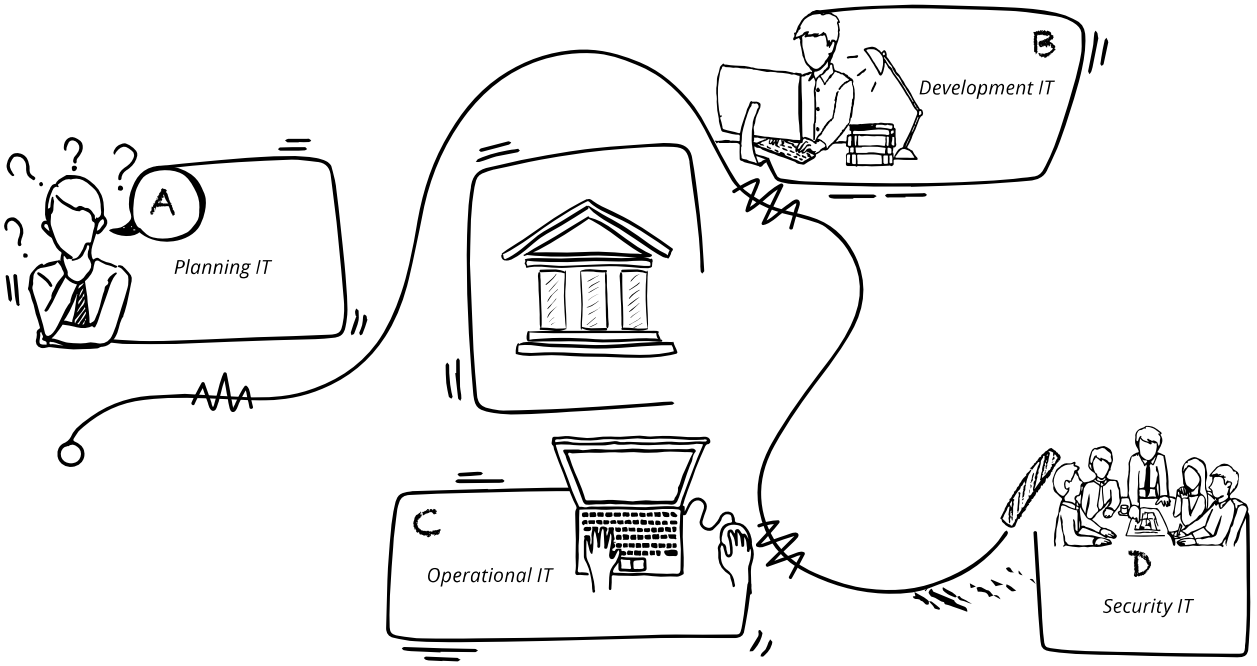
Information Technology Policy and Governance

To serve its business needs, improve services to customers, and streamline its operations, Bank Mandiri needs to implement an Information Technology (IT) system with good governance on an end-to-end basis to maintain confidentiality, integrity, availability, reliability, continuity, and compliance. Bank Mandiri IT Governance is carried out based on regulatory provisions, both the Financial Services Authority (OJK) and Bank Indonesia (BI) as well as other regulatory provisions, while still considering the character and business strategy of Bank Mandiri. Bank Mandiri always guarantees continuous improvements to its IT Governance in accordance with its business development by conducting a periodic review.

In general, Bank Mandiri's IT activities are divided into 4 processes: IT planning, development, operation, and security. The IT framework adopted by Bank Mandiri is illustrated in the following chart:



INFORMATION TECHNOLOGY PLAN

The Information Technology Planning Process consists of several sub-processes, including: Development of the IT Strategic Plan (ISP) as guidelines for IT initiative development that conforms to Bank Mandiri's Corporate Plan, Annual IT Initiative planning, IT Architecture planning, and IT Strategic Research and Studies.

DEVELOPMENT OF INFORMATION TECHNOLOGY

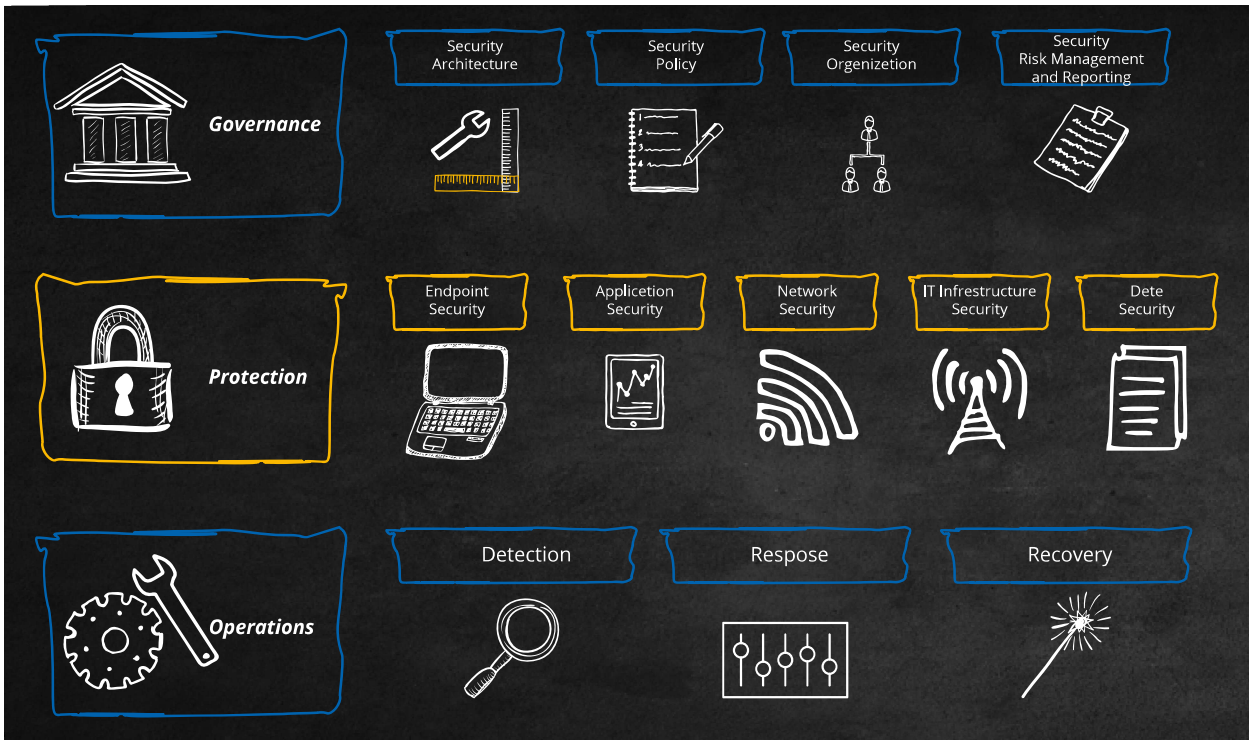
In general, the Information Technology Development process is comprised of IT initiative development, non-project IT initiative development, and End-User Computing (EUC) development, all of which are managed by the IT work unit. Bank Mandiri implements Waterfall and Agile development methods.

OPERATIONAL MANAGEMENT OF INFORMATION TECHNOLOGY

IT operational management consists of several processes. Operational management processes incude: System Operational Management, Backup and Restore Process Management, Network Management, IT Infrastructure and Asset Management, and IT Incident Management.

INFORMATION TECHNOLOGY SECURITY

Information Technology Security is undertaken in measurable and systematic manners through improvements in Enterprise Information Security Architecture (EISA)-based information security that focuses on 3 (three) areas, i.e. Governance, Protection, and Operations designed to prevent, indentify, respond, and recover the Bank in the event of cybersecurity. The EISA framework is illustrated in the following figure:



The following are focus areas of the EISA framework:

EISA FRAMEWORK		
Governance	**Protection**	**Operations**
CISO Office Group as the 1st line of defense is in charge of ensuring the Bank's information security and serves 3 main functions, they are: 1. *Design*, i.e. through security architecture and strategy designing 2. *Services*, i.e. through development, analysis, and disbursement of information about standard procedures, awareness program, risk management, and implementation of security control in the course of IT planning and development 3. *Operations*, i.e. efforts to address information security incidents, which include protection, detection, response, and recovery from cyber security. Operational Risk Group as the 2nd line of defense is in charge of managing cyber security risk at enterprise level. IT Audit as the 3rd line of defense is in charge of ensuring that all operational activities conform to internal regulations, external regulations, and best practices for the industry. The Bank improves its employee competencies through training and certification related to information technology, cyber security risk, and data protection. Bank's assets, in the forms of customer information and data are managed by implementing the principle of Confidentiality, Integrity, and Availability based on Work Culture, Good Corporate Governance, Code of Conduct, Business Ethics, and Prudential Banking. Bank has identified cyber risks in its relationships with third parties through 3rd party risk assessment periodically. Moreover, Bank instils security awareness into 3rd party and employees periodically through phishing drill, e-learning, and other media. Furthermore, Bank implements ORMT *(Operational Risk Management Tools)* to manage cyber security threats.	Bank Mandiri continuously applies security standards and improves capabilities through EISA roadmap development and implementation based on the latest technology, including initiatives on the 5 layers of information security architecture, i.e.: 1. ***Endpoint Security*** – through protection, encryption, and monitoring of end-users' IT devices. 2. ***Application Security*** – through the implementation of Secure System Development Life Cycle method at each stage of Bank system and application development. 3. ***Network Security*** – through updates on network security devices such as Next-Gen Firewall and Network Access Control. 4. ***Data Security*** – through technology such as Data Loss Prevention, Data Masking and Data Encryption to prevent leakage of Bank's information. 5. **IT *Infrastructure*** – through updates on security of the infrastructures used by Bank by means of patching, hardening, Identity and Access Management, and Privileged Access Management.	To maintain smooth operations 24/7, Bank through its Security Operation Center provides protection against insider and external cyber threats. Each information sec urity event or incident is managed in consistent, effective, and measurable manners. All information systems adopted by the Bank have undergone the security assessment process to manage any vulnerability well. Moreover, Bank provides online protection for its brand dan website against threats such as phishing, online scams, unauthorized, dan counterfeit sales that maight be detrimental to customers. Then, to maintain customer information and data security, Bank conducts internal monitoring and prevention of sensitive data transfer outside of Bank's network through email, web browser, and removable media. Furthermore, Bank already develops digital forensic capabilities that enables security incident investigation processes, ensures post-incident recovery, improve security postures, and prevents recurrence of such incidents.

Information Technology Development Plan 2020

The development of Bank Mandiri's Information Technology in 2020 has been planned and arranged based on the Corporate Plan and Re-Aligned IT Strategy and Execution Plan (ISP) 2017-2020, and focuses on improving IT Service Management and developing IT capabilities to support the Bank's business services, both from the front end, middle end, and back end.

The front-end development in 2020 focuses on channel development to enable omni-channel services and seamless experience as a touchpoint for both customers and employees. The middle-end development is undertaken through development of integration and workflow capabilities that enable seamless internal and external connectivity through the enterprise service bus. The back-end development is carried out through improvements to IT systems and applications supporting the management of banking services and products that enable Bank Mandiri to develop new and complex products. In addition, improvements are also made to core banking system stabilization, functionality of the core system, and infrastructure capabilities.