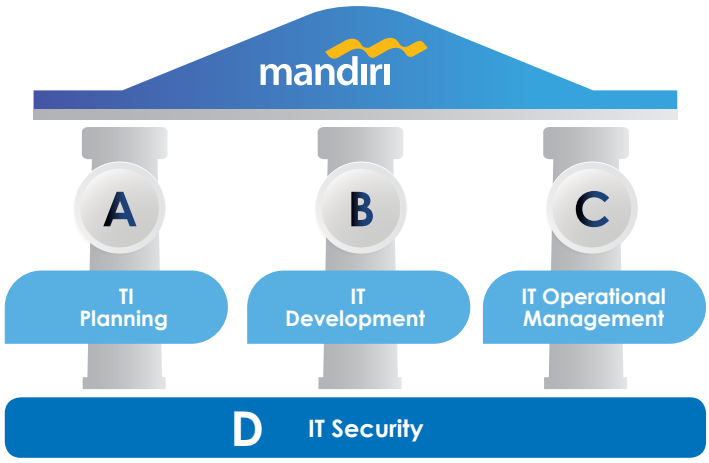
INFORMATION TECHNOLOGY **GOVERNANCE**

In general, Bank Mandiri's IT governance is divided into 4 (four) processes, namely Planning, Development, Operational Management and IT Security, as follows:

IT Governance Coverage



A. IT Planning

IT planning includes several IT strategic processes including the preparation and review of IT long-term strategic plans, the preparation of IT project portfolios aligned with the Bank's strategy, the management of IT standards as a reference for IT development and IT strategic research and studies for optimization of application utilization, IT infrastructure and adoption of new technology/business processes that have competitive value for the bank.

B. IT Development

IT development governance includes the end-to-end IT development process starting from the stages of defining needs, design, to testing and deployment. Bank Mandiri adopts a waterfall and agile System Development Life Cycle (SDLC) development methodology that is tailored to the readiness of resources and the character of project needs. Bank Mandiri also applies the DevSecOps method which is an intensive collaboration of each role (product, development, security, risk management, and operation) in the team supported by the use of tools.

C. Operational Management

IT Operational Management includes activities carried out to ensure the operation of Bank Mandiri's IT system is well maintained. This includes managing system operations, managing backup & restore, managing networks, maintaining systems, and managing IT infrastructure.

D. IT Security

IT security processes are attached to each process end-to-end, from planning, development, to managing IT operations. IT security governance focuses on a cybersecurity framework consisting of three execution pillars (Governance, Protection, and Operations). Each pillar has the following aspects:

- Governance: includes, among others, security awareness, security standards and organizational adequacy.
- Protection: includes, among others, defense mechanism, penetration testing dan user access management.
- Operation: includes, among others, Security Operation Center 24x7, threat intelligence, and vendor security assessment.