



INTERNAL CONTROL SYSTEM

The Internal Control System ensures that every process within Bank Mandiri operates securely, systematically, and in alignment with governance principles, enabling effective risk management and reliable achievement of the Bank's strategic objectives.

Bank Mandiri's Internal Control System (ICS) is established by the Board of Directors and approved by the Board of Commissioners as a continuous mechanism to protect assets, enhance compliance, reduce potential losses and irregularities, and strengthen the overall effectiveness of the organisation. The ICS is embedded across all levels of the Bank as part of its risk management process to identify events that may affect operations, manage risks within the defined risk appetite, and provide reasonable assurance in achieving the Bank's strategic objectives. The implementation of the ICS refers to Bank Mandiri's Internal Control Policy (KICN).

Control Objectives

The objectives of effective ICS implementation are grouped into 4 (four) main objectives as follows:

1. Compliance Objectives

To ensure that all business activities of the Bank have been carried out in accordance with the prevailing laws and regulations, both the provisions issued by the Government, the Banking Supervisory Authority, the Capital Market Authority as well as the Bank's internal policies, provisions, and procedures.

2. Purpose of Information

To provide accurate, complete, timely and relevant information needed in making appropriate and accountable decisions, including financial and non-financial reporting needed by internal and external parties of the Bank.

3. Operational Objectives

To increase effectiveness and efficiency in using assets and other resources and protect the Bank from the risk of losses including those caused by fraud events.

4. Risk Culture Objectives

To identify weaknesses and assess deviations early and reassess the reasonableness of existing policies and procedures within the Bank on an ongoing basis.

Management Oversight and Control Culture

The control environment reflects the commitment, conduct, and oversight of Bank Mandiri's Board of Directors and Board of Commissioners in ensuring that operations align with governance principles. The Board of Commissioners oversees the effectiveness of the Internal Control System and encourages improvements where needed, while the Board of Directors establishes internal control policies, strategies, and procedures and monitors their adequacy. Both governing bodies foster strong ethics, integrity, and an organisational culture that emphasises the importance of internal controls across the Bank.

Supervision by management is carried out through the establishment of a control culture through the stipulation of policies and practices of human resources, as follows:

1. Bank has written policies and procedures regarding human resources, including recruitment, career path, payroll and remuneration system, as well as employee coaching and development.
2. The Bank evaluates the performance, competence and application of cultural values by employees on a regular basis, the results of which become the basis for employee assignment and placement.
3. The Bank has an adequate organizational structure and reflects the field of duties and responsibilities established in accordance with applicable regulations.
4. The Bank has a written policy regarding the provisions and procedures for changing the organizational structure.
5. The management of the Bank is carried out by referring to the principles of Good Corporate Governance.
6. The Bank's decision-making is determined in the Board of Directors meeting.
7. The decision-making process is carried out in a bottom-up and top-down manner.
8. The Bank establishes policies aimed at preventing opportunities to commit irregularities or violations of the precautionary principle.
9. The Bank applies the principle of transparency hence employees can communicate to the relevant management about any issues that occur in the Bank's operational activities.

10. The entire process of recruitment, development and career path is carried out taking into account the competence of employees.
11. Management assigns and places employees based on job exposure, level of knowledge, ability, mastery of technical competence and application of behavior and results of employee performance assessment.
12. The Board of Directors establishes a corporate culture that reflects the values underlying the conduct of the entire Bank's levels.
13. All levels of the Bank are required to have integrity and uphold ethical values.
14. Management becomes a role model, always increases the engagement level of all employees and has a high personal commitment to the development of a sound Bank.
15. Management is obliged to improve an effective risk culture and ensure that it is inherent at every level of the organization.

For the oversight of the Board of Directors and control culture, the Bank sets strategies & objectives as requirements for an effective event identification, risk assessment and risk response process, consisting of:

1. Strategic Objectives, the high-level targets and in line with the Bank's vision and mission.
2. Operational Objectives, the derivative goals and strategic objectives at the operational level (activities, work units and others).

The Bank has standard procedures for targets setting in accordance with the vision, mission and risk appetite.

Risk Recognition and Assessment

The Board of Directors identifies events that may influence Bank Mandiri's ability to execute its strategies and achieve its objectives. This includes recognising events that may create risks requiring assessment and response, as well as opportunities that may support strategic development. In doing so, the Board considers all aspects of the organisation to ensure a comprehensive view of potential events.

Risk assessment is carried out through several activities, from identifying and analysing to measuring risks, across all processes that may pose potential losses to the Bank. Bank Mandiri has a written risk management policy established by the Board of Directors and approved by the Board of Commissioners as the foundation for effective risk management. The assessment covers both quantitative and qualitative risks, as well as risks that can be controlled and those that cannot.

The risk assessment methodology forms the basis for developing a risk profile that is periodically updated. Based on the results, the Bank determines whether a particular risk should be accepted, mitigated, or avoided by adjusting business activities. When new risks arise or existing risks remain uncontrolled, the internal control system must be reviewed through continuous evaluation of changes in conditions and the effectiveness of existing controls.

Following the assessment, the Board of Directors determines the appropriate risk response, including mitigation measures and enhancements to internal controls, to ensure that Bank operations remain secure and aligned with strategic objectives.

Control and Separation of Functions Activities

Control activities include control activities and segregation of duties, with the following description:

1. Control Activities

Control activities engage all levels of the Company, which includes planning, setting policies and procedures, implementing controls and early verification processes to ensure that policies and procedures have been consistently adhered to, and are activities that cannot be separated from every function or activity of the Bank on a daily basis. Control activities are implemented at all levels of functions according to the Bank's organizational structure, which includes:

- a. Top Level Review
The Board of Directors regularly requests reports and explanations from Unit Heads to review performance against targets. This review enables the Board to promptly identify issues, including control weaknesses, financial reporting errors, or potential fraud.
- b. Functional Review
The review is carried out by Internal Audit during examinations or regulatory reporting by assessing the risk evaluations prepared by the Risk Management Unit, analysing operational and financial data by verifying transactions against risk reports, and reviewing each unit's work plan and budget to identify significant deviations and determine necessary corrective actions.

- c. Control of information systems
The Bank ensures transaction accuracy and compliance with authorization procedures, implements IT controls to maintain system and data confidentiality and integrity, and applies information system controls covering data center operations, system procurement and maintenance, servers, workstations, networks, and application controls to ensure reliable transaction processing and effective audit procedures.
- d. Physical controls
Physical asset controls are implemented to ensure the security of the Bank's assets, including safeguarding records and documentation, restricting access to applications, and conducting periodic asset appraisals.
- e. Documentation
The Bank properly documents all policies, procedures, systems, and work standards, updates them regularly to reflect current operations, and ensures their availability to internal auditors, external auditors, and supervisory authorities. The Internal Audit Unit evaluates the accuracy and completeness of these documents during routine and non-routine audits.

2. Segregation of Duties

- a. The separation of functions is intended for everyone in his/her position to not have the opportunity to commit and hide errors or deviations in the performance of his/her duties at all levels of the organization and all steps of operational activities.
- b. The organizational structure is made by separating the functions of recording, audit, operational and non-operational (segregation of duties), hence to create a system of dual control, dual custody and avoid duplication of work in every activity and avoid conflicts of interest.
- c. In implementing segregation of duties, the Bank allocates key tasks to multiple individuals to reduce the risk of data manipulation or asset misuse. This separation applies not only to front and back-office activities but also to fund approval and disbursement, management of customer and owner accounts, transaction

recording, customer information delivery, credit documentation review and monitoring, activities that may create conflicts of interest, and maintaining the independence of the risk management function.

- d. Directors and Employees have an adequate job description that contains functions, duties, authorities and responsibilities.
- e. The Board of Directors and Employees are prohibited from concurrently holding positions in the Bank's internal environment that can cause conflicts of interest.

Accountancy, Information and Communication Systems

1. Accounting System

The Bank applies an accounting system based on written policies that comply with generally accepted accounting principles, covering the methods and recording processes used to identify, classify, analyse, book, and report all transactions. This system must be implemented consistently, including monthly reconciliations between accounting data and the management information system, with proper documentation. Each unit is required to record transactions promptly and accurately, ensure alignment with the general ledger, clear suspense accounts, and use standard forms or working papers equipped with appropriate security features and adequate documentation.

2. Information

The Bank implements an information system capable of generating reports on business activities, financial condition, risk management, and compliance to support the Board of Directors and Board of Commissioners. Internal controls ensure reliable information across all functional activities, particularly high-risk areas, with secured data, monitoring by internal auditors, and adequate contingency programs. The Bank also ensures effective information security to maintain the confidentiality, integrity, and availability of all managed data.

3. Communication

The Bank maintains a communication system that delivers information to all stakeholders, both internal and external, including regulators, external auditors, shareholders, and customers. The Internal Control System ensures effective communication

channels so that management and employees understand and comply with applicable policies and procedures. Management also ensures that information on policies, risk exposures, transactions, and operational performance is accessible to relevant stakeholders as needed.

Monitoring Activities and Correcting Deficiencies

The Board of Directors continuously monitors the effectiveness of Internal Control System, including IT security and usage, with the Board of Commissioners ensuring proper oversight. Key risks are regularly evaluated by Business Units, Compliance, Risk Management, and Internal Audit to assess the adequacy of the ICS amid internal or external changes. Any weaknesses identified by relevant units or other parties are promptly reported to Management, and material issues are escalated to the Board of Commissioners for corrective action.

Compliance with SEOJK No. 35/SEOJK.03/2017 on Internal Control Standard Guidelines for Commercial Banks

Bank Mandiri's Internal Control System comprises five interconnected components applied across the organisation to support the Bank's objectives, following regulatory requirements and international internal control practices, namely:

1. Oversight by Management and a Control Culture
2. Risk Identification and Assessment
3. Control Activities and Separation of Functions
4. Accounting, Information, and Communication Systems
5. Monitoring Activities and Deviation Correction Actions

Evaluation of Internal Control System Implementation

The Board of Directors ensures the implementation of a reliable and effective Internal Control System and fosters a strong risk-aware culture across the organisation, while Internal Audit periodically evaluates and enhances the system through reviews of business units and subsidiaries. Evaluation results are reported to the Board of Directors for follow-up and monitoring, with the Board of Commissioners, through the Audit Committee, reviewing these outcomes. Based on the 2025 assessment, Bank Mandiri's ICS is considered adequate.

Effectiveness of Internal Control System

The effectiveness of Bank Mandiri's Internal Control System relies on the integration of its five interrelated components, which must be consistently applied across the organisation. Management is responsible for ensuring that the ICS operates reliably and effectively while fostering a strong risk-aware culture at all organisational levels.

Internal Audit continuously evaluates and enhances the effectiveness of the ICS by reviewing operational processes to support the achievement of corporate objectives. Evaluation results are submitted to Management for follow-up and monitoring. Overall, Management considers the ICS to be effective, while recognising the need for ongoing improvements in line with the Bank's growing scale and business complexity.