

# INTERNAL CONTROL SYSTEM

The Internal Control System (ICS) aims at supporting the achievement of the Company's performance objectives, improve value to the stakeholders and assure effectiveness and efficiency of operation, reliability of financial reports, sufficiency of financial and operational controls, and compliance with prevailing laws and regulations.

The ICS refers to a monitoring mechanism which is established by the Company's management on an on-going basis. An effective ICS is a key component in the Company's management and becomes the foundation of the Company's operational activities which are sound and secured. An effective ICS can help the Board of Commissioners and Directors in safeguarding the assets of the Company, ensuring the availability of credible financial and managerial reporting, increasing the Company's compliance with laws and regulations, and decreasing the risk of loss, deviation, and violations of prudential aspects. The application of ICS in the Company refers to the Internal Control Policy (ICP).

As a process executed by all levels of the Company's organization, ICS is applied in the strategy setting in all operating units, and it is designed to capably identify the plausible occurrence of an event that can impact the company, to manage risk in order to still remain within the risk appetite, and to provide adequate confidence in order to achieve the company goals.

## The Objectives of Controls

The objectives to implement an effective ICS are classified into 4 (four) main objectives as follows:

1. **The Compliance Objective**  
To ensure that all of the Company's business activities have been undertaken resting upon the applicable laws and regulations, both the provisions issued by the Government, the Banking Supervision Authority, the Capital Market Authority and the Company's internal policies, stipulations, as well as procedures.
2. **The Information Objective**  
To provide accurate, complete, on-time, and relevant information required in an effort to make appropriate and accountable decisions, including financial and non-financial reports needed by both internal and external parties of the company.
3. **The Operational Objective**  
To enhance the effectiveness and efficiency in using assets and other resources as well as to protect the Bank from the risk of losses including those on account of fraud event.
4. **The Objective of Risk Awareness Culture**  
To identify weaknesses and to assess deviations early and re-assess the fairness of the internally prevailing policies alongside the procedures at the Bank on an ongoing basis.

## Management Oversight and Control Culture

The control environment indicates the entire commitment, behaviour, care, and measures of the Board of Directors and Commissioners of Bank Mandiri in executing the operational activities. The Board of Commissioners is responsible for ensuring whether the Directors have monitored the effectiveness of the ICS implementation. The Board of Commissioners has an active role in ascertaining the improvements to the Company's issues that can potentially reduce the effectiveness of ICS.

The Board of Directors are responsible for setting the policies and strategies as well as internal control procedures. Also, responsible to monitoring the sufficiency and effectiveness of ICS. In addition, the Board of Commissioners and Directors are responsible to enhancing the work ethics and high integrity as well as to creating an organizational culture subjected to all employees appertaining to the importance of internal controls prevailing in Bank Mandiri.

Monitoring by management is undertaken through building up the control culture by means of the establishment of human resource policies and practices, including the following points:

1. The Company has the written policies and procedures in regard to human resources encompassing the recruitment, career paths, payroll and remuneration systems, and employee coaching and development.



## INTERNAL CONTROL SYSTEM

2. The Company evaluates the performance, competency, and application of cultural values by employees periodically, wherein the results become the basis for assigning and placing the employees.
3. The Company has an organizational structure which is adequate and reflects the task specification and responsibilities determined resting upon the applicable regulations.
4. The Company has a written policy in association with the provisions and procedures for changing organizational structures.
5. The Company management is executed in referential to the principles of Governance.
6. The Company decision making is determined at the meeting held by the Board of Directors.
7. The process of making decision is undertaken in bottom-up and top-down manner.
8. The Company makes policies which are aimed at preventing any occurrence opportunity of deviation or violations of the prudential principles.
9. The Company applies the principle of transparency hence employees can communicate any problems in the Bank's activities to the relevant management.
10. The entire process of recruitment, development and career path is carried out by considering employee competence.
11. Management assigns and places employees based on job exposures, level of

knowledge, ability, mastery of technical competence and application of behaviour as well as results of employee performance appraisals.

12. The Board of Directors establishes a corporate culture that reflects the values that underlie the behaviour of all levels of the Bank.
13. All levels of the Bank are required to have integrity and uphold ethical values.
14. Management is 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 embedded at every level of the organization.

On the oversight by the Board of Directors and a culture of control, the Company sets objectives (objective setting) as a requirement for an effective event identification, risk assessment and risk response process, consisting of:

- a. Strategic Objectives are targets that are high level and in line with the Bank's vision and mission.
- b. Operational Objectives, are targets and strategic objectives at the operational level (activities, operating units and others).

The Company has standard procedures to set targets in accordance with the vision, mission and risk appetite.

### Risk Identification and Assessment

The Board of Directors identifies events that have the potential to affect the Bank's ability to perform its strategies and achieve the targets effectively. The identification is carried out on events estimated to have a negative impact (risk) that require the Bank's assessment and response. Identification is also carried out on events that are expected to have a positive impact which is an opportunity for the Board of Directors in formulating strategies to achieve the Bank's goals.

The Board of Directors considers all aspects of the organization when identifying potential events.

Risk assessment is a series of actions starting from the identification, analysis and measurement of the Company's risk to achieve the targets. Risk assessment covers all types of risks inherent in every process/activity that is potentially harmful to the Company.

The Company has a written risk management policy determined by the Board of Directors and approved by the Board of Commissioners.

In order to implement an effective ICS, the Company continuously identifies and assesses risks that may affect the achievement of targets. The Internal Audit Unit (SKAI) periodically reviews the risk assessments produced by the Risk Management Unit (SKMR) hence the scope of audits is broader and comprehensive. The assessment

## INTERNAL CONTROL SYSTEM

covers all inherent risks, both individual and overall risks, which include credit risk, market risk, liquidity risk, operational risk, legal risk, reputation risk, strategic risk, compliance risk, insurance risk and intra-group transaction risk.

The Board of Directors determines the actions to respond based on an assessment of the relevant risks and controls. Response actions taken may include risk avoidance, or risk reduction, and/or risk sharing, and/or risk acceptance as implemented in Bank policy. In considering response actions, the Board of Directors considers costs and benefits, and chooses response actions that lead to likelihood and impact in accordance with the Bank's risk tolerance and risk appetite thresholds.

### Control Activities and Segregation of Duties

Control activities include the controlling and segregation of duties, with the following descriptions:

#### 1. Control Activities

Control activities involve all levels of the Company which include planning, establishing policies and procedures, implementing controls and early verification processes to ensure that policies and procedures are consistently adhered to. Control function cannot be separated from every

function or daily activities of the Company. Control activities are implemented at all levels of functions according to the Company's organizational structure, which include:

- **Review by the Board of Directors (Top Level Review)**

The Board of Directors periodically requests for explanations (information) and operational performance reports from the Head of the Unit to review the results compared to the set targets. Based on the review, the Board of Directors can quickly detect issues, such as control weaknesses, financial statement errors or other irregularities (fraud).

- **Operational Performance Review (Functional Review)**

This review is carried out by SKAI at the time of inspection or in the process of reporting to the regulator, which includes:

- a) Reviewing the risk assessment (risk profile report) produced by the Risk Management Unit.
- b) Analysing operational data, whether risk related or financial data, namely verifying transaction detail and activities

compared to the output (report) produced by the Risk Management Unit.

- c) Reviewing the realization of work and budget plans made by each work unit to:
  - 1) Identify the dominant causes of deviations.
  - 2) Establish requirements for corrective actions.

- **Information system control**

- a) The Company carries out verification of the accuracy and completeness of transactions as well as the implementation of authorization procedures in accordance with applicable regulations.
- b) The Company carries out IT control measures to produce systems and data that are kept confidential and with integrity and can support the achievement of the Company's objectives.
- c) Control of information systems includes:
  - 1) Control over data centre operations (data base), procurement system, system/application development and maintenance. This control is applied to mainframes, servers,



## INTERNAL CONTROL SYSTEM

and user work stations, as well as networks.

- 2) Application control on programs used by the Company in processing transactions and to ensure the availability of an effective audit process and to check the correctness of the audit process in question.

- **Physical asset controls**

- a) Physical asset control is implemented to ensure the implementation of physical security of the Company's assets.
- b) Physical asset control includes safeguarding assets, records and documentation as well as limited access to application programs.
- c) The Company must check the asset value (appraisal) periodically.

- **Documentation**

- a) The Company documents all policies, procedures and work standards in an orderly and neat manner
- b) All policies, procedures, operational systems and accounting standards are updated regularly to reflect actual operational activities.

- c) Upon request, documents are always available for the benefit of the internal auditors, external auditors and the Banking Supervision Authority.
- d) The Internal Audit Unit assesses the accuracy and availability of these documents when conducting routine and non-routine audits.

### 2. Segregation of Duties

- The separation of functions is intended so that everyone in their position does not have the opportunity to commit and hide mistakes or irregularities in the execution of their duties.
- The organizational structure is made by separating the functions of recording, inspection, operational and non-operational (segregation of duties), so as to create a dual control system, dual custody and avoid duplication of work in each activity and avoid conflicts of interest (conflict of interest).
- In implementing the separation of functions, the Company takes the following steps:
  - a) Assign certain functions or tasks in the Company which are separated or allocated to several people in order to reduce

the risk of manipulation of Company data/information or misuse of Company assets.

- b) The separation of functions is not limited to front and back-office activities, but also in the context of controlling:
  - 1) The approval of the disbursement of funds and the realization of the expenditure.
  - 2) customer accounts and bank owner accounts.
  - 3) The transactions in the Bank's books.
  - 4) information to Bank customers.
  - 5) assessment of the adequacy of credit documentation and monitoring of debtors after credit disbursement.
  - 6) other business activities that may cause a conflict of interest
  - 7) the independence of the risk management function at the Bank.
- Directors and employees have adequate job descriptions that contain functions, duties, authorities and responsibilities.
- Directors and employees are prohibited from holding concurrent positions within the Bank's internal environment which may cause a conflict of interest.

## INTERNAL CONTROL SYSTEM

### Accounting, Information and Communication Systems

#### a. Accounting System

- The Bank has a written accounting policy that complies with generally accepted accounting principles.
- The Bank's Accounting System includes methods and recording system to identify, classify, analyse, classify, record/book and report all transactions and activities of the Bank.
- Accounting system must be applied consistently and persistently for all Bank transactions.
- The Company is required to reconcile the accounting data with the management information system every month. The results of the reconciliation are documented in an orderly manner.

#### b. Information

The Company has an Information System that can produce reports or provide sufficient and comprehensive data/information regarding business activities, financial condition, implementation of risk management, compliance with applicable rules and regulations, market information or external conditions and conditions required for making appropriate decisions. appropriate.

#### c. Communication

The Company has a communication system that is able to provide information to all stakeholders, both internal

and external, such as the Banking Supervision Authority, external auditors, shareholders and customers of the Company.

ICS ensures that there is an effective communication channel so that Management and Employees understand and comply with applicable policies and procedures in carrying out their duties and responsibilities.

The Board of Directors has an effective communication channel so that the required information is reached by interested parties. This requirement applies to any information, both regarding established policies and procedures, risk exposures and actual transactions as well as regarding the Company's operational performance.

### Monitoring and Irregularity Correction Activities

The Board of Directors conducts continuous monitoring of the overall effectiveness of the ICS implementation, including but not limited to the effectiveness and security of the use of IT, in which the Board of Commissioners ensures that the Board of Directors has properly monitored.

Monitoring of the Company's main risks is part of the Company's daily activities including periodic evaluations, whether by the Work Unit, Compliance Unit, Risk Management Unit, and Internal Audit Unit.

The relevant operating units monitor the adequacy of the SPI continuously in relation to changes

in internal and external conditions and increase the capacity of the SPI so that its effectiveness can be increased. Meanwhile, if there are weaknesses in the SPI, whether identified by the Work Unit (risk taking unit), Internal Audit Unit or other parties, it is immediately reported to the Board of Commissioners and Board of Directors of the Company.

### Conformity with SEOJK No. 35/SEOJK.03/2017 concerning Guidelines for Internal Control Standards for Commercial Banks

The ICS consists of 5 (five) interrelated components to be implemented effectively by all organizational levels to achieve the Company's goals. The ICS component implemented by the Company refers to the regulator stipulations and takes into account the principles/practices of internal control that apply internationally (international best practices).

The 5 Internal Control System interrelated components that can affect the effectiveness of each of their implementation are:

1. Supervision by Management and a Culture of Control
2. Risk Identification and Assessment
3. Control Activities and Segregation of Functions
4. Accounting, Information and Communication System
5. Deviation Monitoring and Correction Activities

### Evaluation of Internal Control System

The Board of Directors is responsible for the implementation of a reliable and effective SPI and has the obligation to promote an



## INTERNAL CONTROL SYSTEM

effective risk awareness culture and must ensure that it is embedded at every level of the organization.

Internal Audit is responsible for evaluating and playing an active role in improving the effectiveness of SPI on an ongoing basis in relation to the operations in achieving the targets set by the Company. Internal Audit conducts periodic reviews and examinations of all activities in the Work Unit and Subsidiaries.

The evaluation results are submitted to the Board of Directors to be followed up and its implementation monitored to ensure the SPI has been running effectively. The Board of Commissioners, especially through the role of the Audit

Committee, has an active role in the evaluation of SPI by reviewing the assessment by the Internal Audit. The evaluation that has been carried out during 2021 shows that the SPI system at Bank Mandiri is adequate.

### Effectiveness of Internal Control System

As mentioned above, the 5 Internal Control System that are interrelated components can affect the effectiveness of ICS implementation in the Company.

The Management is responsible for the implementation of reliable and effective Internal Control System and is obliged to improve effective risk culture and shall ensure Internal Control System has been

embedded on every organization level.

Internal Audit is responsible to evaluate and play an active role in improving Internal Control System effectiveness on an ongoing basis with regard to the implementation of the Company's operation to achieve goals set by the Company. The evaluation results are submitted to management for follow up and monitor their implementation to ensure the Internal Control System is effective.

The Management views that the internal control system implemented has been performing effectively, however remain to be improved in line with the growing and complex business.