THE EVALUATION OF RISK MANAGEMENT SYSTEMS

Bank Mandiri constantly evaluates the effectiveness of the risk management systems. The evaluation entails adjusting the strategy and the framework of risks as the constituent of risk management policies, considering the adequacy of risk management information systems and the adequacy of risk identification, measurement, monitoring and control processes.

An example of evaluation on the risk management policy is the annual evaluation on the Risk Management Policy and Standard Procedure. The Board of Commissioners plays an active role in the evaluation of the risk management system by reviewing findings of the evaluation undertaken by the Board of Directors as the organ in charge of effective implementation of the risk management system. The annual evaluation results show that during 2019 Bank Mandiri has implemented fairly good risk management.

INTERNAL CONTROL SYSTEM

The Internal Control System (ICS) refers to a monitoring mechanism which is established by the company's management on an on-going basis. An effective ICS is an important component in the company management and becomes the foundation of the company operational activities which are proper 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 work 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 of implementing an effective ICS are classified into 4 (four) main objectives as follows:

1. **The Compliance Objective**
   It is 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, provisions, as well as procedures.
2. **The Information Objective**
   It is 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**
   It is 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**
   It is 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.

CONTROL ENVIRONMENT

The control environment indicates the entire commitment, behavior, care, and steps 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 plays an active role in ascertaining that there are improvements to the company's problems that can potentially reduce the effectiveness of ICS.

The directors are responsible for setting the policies and strategies as well as internal control procedures. They are also responsible for monitoring the sufficiency and effectiveness of ICS. In addition, the Board of Commissioners and Directors are responsible for enhancing the work ethics and high integrity as well as for 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 culture control 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.
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 Good Corporate 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.

RISK ASSESSMENT

Risk assessment is a set of actions which start out from the identification, analysis, and measurement of the company's risks for the sake of attaining the targets set. The risk assessment is done to all kinds of risks inherent in each process or activity that is conceivably potential to harm the company.

Bank Mandiri has the written risk management policies set by the Board of Directors and approved by the Board of Commissioners.

In an effort to implement an effective ICS, the company continuously identifies and assesses risks that can have an impact on the attainment of targets. The Internal Audit Work Unit (IAWU) periodically reviews the risk assessment produced by the Risk Management Work Unit (RMWU) so that the coverage of the audit is more extensive and comprehensive.

The assessment as such incorporates all risks faced, either individual or overall risks, which entail loanrisk, market risk, liquidity risk, operational risk, legal risk, reputation risk, strategic risk, compliance risk, insurance risk, and intra-group transaction risk.

CONTROL ACTIVITIES

Control activities entail the control and segregation of duties, with the descriptions presented as follows:

1. Control Activities
   Control activities involve all levels of the company that include planning, policy and procedure determination, implementing controls and early verification processes to ensure that those policies and procedures are consistently obeyed. The control activities are those that cannot be separated from each function or daily activity of the company.

   These activities are applied in all levels of function based on the structure of company organization as follows:
   a. Review by The Board of Directors (Top Level Review)
      The Board of Directors periodically requests explanation (information) and operational performance reports from the Head of Division in order to review the results of the realization compared to the set targets. Based on the review, soon the Board of Directors detects some problems that may occur, for instance control weaknesses, financial statement errors or other irregularities (fraud).
   b. Review of Operational Performance (Functional Review)
      This review is conducted by SKAI at the time of inspection or in the reporting process to the regulator, which includes:
      - Conducting a review of the risk assessment (risk profile report) made by the Risk Management Unit
      - Analyzing operational data, both related to the risk and financial data, by verifying details and transaction activities compared to outputs (reports) produced by the Risk Management Unit
      - Carrying out a review of the implementation of work plans and budgets made by each division in order to:
        1) Identify the significant cause of deviation
        2) Determine requirements for corrective action
   c. Managing the information system
      - The company carries out verification of the accuracy and completeness of transactions and the implementation of authorization procedures in accordance with applicable regulations.

- The company accomplishes controlling steps of information technology (TI) to deliver system and data that are maintained confidentially with a good integrity and support the company's goal.
- Controlling information technology includes:
  1) Controlling operational database, procurement system, development and maintenance of system/application. This controlling act is implemented for mainframe, server, user work station, and connectivity.
  2) Controlling of application is carried out for a program used by the company to process transactions in order to ensure the availability of effective auditing process and go over the validity of that auditing process.

d. Physical controls
- Physical controls are carried out to guarantee the implementation of physical safeguards towards the company's assets.
- These controls include securing assets, records and documentation and limited access to application programs.
- The company has to check appraisal continuously.

e. Documentation
- The company documents all policies, procedures, and working standard neatly and in a good order.
- All policies, procedures, operational system and accounting standard are updated regularly in order to figure out the actual operational activities.
- By request, documents are always available for the sake of internal auditor, external auditor, and Banking Monitoring Authority.
- The Internal Audit Unit assesses the accuracy and availability of these documents when conducting routine and non-routine audits.

2. (Segregation of Duties)
   a. The aim of this segregation of duties is that everyone in the company does not have any opportunity to do and cover up mistakes or irrelevancies while doing their jobs.
   b. The structure of organization is made by separating the functions of recording, inspecting, operational and operational items (segregation of duties), in which it is expected that it will create a system of dual control, dual custody and there will be no double jobs and conflict of interest in any activities.
   c. In the implementation of this segregation policy, the company carries out several moves for instance:
      – Determine the function or certain job only for several employees in which these are separated from the others to decrease the risk of information/data manipulation or misuse of company's assets.
      – This separation is not limited only for front and back office activities but it is intended to manage several things as follows:
        1) Approval of spending and the realization of it.
        2) The customer account and bank account owner.
        3) Transactions in bank bookkeeping.
        4) Giving information to the bank customer.
        5) Assessing the adequacy of loan documentation and debtor monitoring after loan disbursement.
        6) Other business activities that may cause conflict of interest.
        7) The independence of the bank risk management function.
   d. Both Directors and employees have a comprehensive job description including their functions, duties, authorities and responsibilities.
   e. Both Directors and employees are not allowed to have a double job in their internal institution that can cause a conflict of interest.

Based on the explanation above, the internal control system can be grouped into 2 (two) control activities namely operational control and financial control. It can be explained as follows:

OPERATIONAL CONTROLS

Operational controls conducted by Bank Mandiri include:

1. Review by the Board of Directors by requesting explanation (information) and reports of operational performance of the company so that the board of Directors can detect in case of control weakness, misconduct of financial statements or other irregularities (fraud).
2. Review by Internal Audit, by reviewing the risk assessment (risk profile report) produced by the Risk Management Work Unit, analyzing operational data,
3. Reviewing the realization of the work plan and budget implementation.

4. Controlling the information technology that includes control of data center operations and control of applications.
5. Documentation for all of the policies, procedures and working standards.

FINANCIAL CONTROL

Financial controls that have been carried out by Bank Mandiri include:

1. Applying the intended separation of functions so that everyone in his office does not have the opportunity to make and hide mistakes or irregularities in the implementation of their duties.
2. All policies, procedures, operating systems and accounting standards are updated periodically to describe actual operational activities.
3. Approval of funds withdrawal and expense realization.
4. Control over customer's account and Bank's owner's account.
5. Control over transactions in the Bank's bookkeeping.
6. Control of physical assets includes asset safeguarding, notes and documentation as well as limited access to application programs.

INFORMATION AND COMMUNICATION

a. Information

The company has system information that provides comprehensive and sufficient data/information related to business activities, financial condition, the implementation of risk management, the obedience towards rules and regulations, market information or external condition needed while making proper decisions.

b. Communication

The company has such a communication system which is able to deliver information to all stakeholders including internal and external parties such as Banking Monitoring Authority, external auditors, shareholders and customers of the company.

SPI's duty is to make sure the availability of effective means of communication so both managerial people and employees understand and obey the applicable policies and procedures while doing their jobs and responsibilities.

Managerial people have an effective communication channel so all information needed can be reached by interested parties. This requirement is for all information including policies and procedures that have been assigned, risk exposures, real transactions, and operational performance of the Bank.

MONITORING ACTIVITIES

Directors conduct periodic monitoring activities to find out the effectiveness of overall SPI implementation although it is not limited only about the effectiveness and the safety of TI use in which The Board of Commissioners also ensure that The Directors have conducted the monitoring well.

Monitoring towards the main risks of the company is a part of daily activities including periodic evaluation carried out by Work Unit, Compliance Unit, Risk Management Work Unit, and Internal Audit Work Unit.

Related work units monitor the adequacy of SPI continuously in regard with the internal and external changing conditions and increase the capacity of this SPI so its effectiveness can be improved. If there are some SPI'S weaknesses identified by risk taking unit, intern audit of taking unit or the others, they should be reported to the Board of Commissioners and Board of Directors.

ITS COMPATIBILITY WITH THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO)

SPI consists of 8 components which are related to each other and applied effectively by all levels in the company in order to achieve its goal. It is the development of 5 principal elements of SPI regulated by Regulator.

This development referred to the COSO Model developed by Committee of Sponsoring Organizations of the Tread way Commission (COSO) in 2008 which consists of:

1. Internal Environment
2. Objective Setting
3. Event Identification
4. Risk Assessment
5. Risk Response
6. Control Activities
7. Information & Communication
8. Monitoring

THE EVALUATION OF INTERNAL MONITORING SYSTEM IMPLEMENTATION

The Board of Directors are responsible for the implementation of reliable and effective SPI in which they also have to increase the culture of risk awareness effectively and ensure that those values have embedded in every level of organization.

Internal audit is responsible for evaluating and actively improving the use of SPI continuously in regard with the operational implementation in achieving the company's goals. It also conducts reviews and verifies all activities in risk taking unit and subsidiaries periodically.

Evaluation results were submitted to the Board of Directors for follow-ups and monitoring to ensure effective implementation of the Internal Control System (SPI). To strengthen the Internal Control System, especially to control frauds, the Company implemented comprehensive and integrated anti-fraud strategies as part of the strategic policy. Based on evaluation throughout 2019, it is revealed that Bank Mandiri has a fairly good Internal Control System.

COMPLIANCE FUNCTION

Recently transactions are done using technology and it requires banking industries to move forward and collaborate with others to improve its system and strategy in order to meet the needs of community. The rapid progress of technology and business development of Bank Mandiri indeed will increase the risk exposure encountered by the company including compliance risk. To overcome this exposure, the compliance function is needed to minimize offenses that may cause loses for the company.

Related with the compliance function, Bank Mandiri refers to the OJK Regulation No. 46/POJK.03/2017 about The Implementation of Bank Compliance Function. Now, Bank Mandiri has got policies and a standard of compliance procedures explaining the duties and responsibilities of Compliance Work Unit.

THE ORGANISATION STRUCTURE OF COMPLIANCE FUNCTION

Organizations running the compliance functions have been regulated in Compliance Policies of Bank Mandiri and it can be seen in detail in Standard of Compliance Procedure. This organizations consist of :

1. Directors in charge of the compliance function
2. Compliance Unit
3. Compliance Work Unit in the Work Unit

DIRECTORS IN CHARGE OF COMPLIANCE FUNCTION

The directors in charge the Company's compliance function during 2019 were Mr. Agus Dwi Handaya as Director of Compliance & HRM

COMPLIANCE UNIT

Compliance Group is a unit having a role as Compliance Work Unit in Bank Mandiri and is directly responsible for The Board of Directors in charge for the compliance functions. As its role as Compliance Work Unit, Compliance Group has fulfilled the following requirements:

a. Independence.
b. Mastering the applicable rules and regulations.
c. Do not carry out other tasks outside the Compliance Function.
d. Have a high commitment to implement and develop a compliance culture.

Additionally, in order to implement Bank Indonesia Regulation No. 18 / POJK.03 / 2014 concerning the Implementation of Integrated Governance for Financial Conglomerates, Compliance Group also acts as an Integrated Compliance Unit to assist and evaluate the implementation of the compliance function in all members of the Financial Services Institution that is a member of the Mandiri Group financial conglomerate.

To carry out the compliance function, Compliance Group has 5 Departments and 1 functional unit Compliance Officer with the following structure: