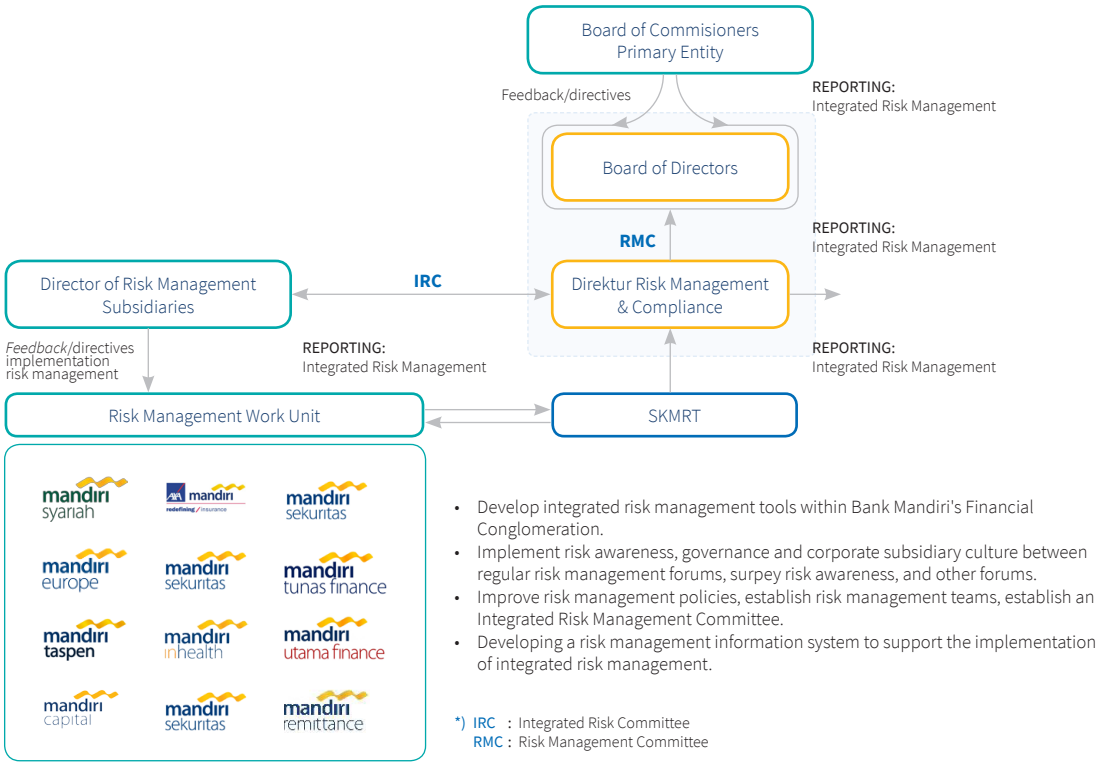


- Develop integrated risk management tools within Bank Mandiri's Financial Conglomeration.
- Implement risk awareness, governance and corporate subsidiary culture between regular risk management forums, surpey risk awareness, and other forums.
- Improve risk management policies, establish risk management teams, establish an Integrated Risk Management Committee.
- Developing a risk management information system to support the implementation of integrated risk management.

*) IRC : Integrated Risk Committee
RMC : Risk Management Committee

In order to improve the understanding of risk management implementation in Bank Mandiri and subsidiaries, several activities had been organized in 2017 as follows:

1. Integrated Risk Management Forum (IRMF) every quarter to discuss current issues related to risk management.
2. Assistance and dissemination related to risk management tools.
3. Credit Risk Workshop for investment activities.
4. Attachment of employees to subsidiaries.
5. Review the implementation of risk management in certain subsidiaries.

Internal Control System

Bank Mandiri's internal control system referred to Circular Letter of the Financial Services Authority No. 35/SEOJK.03/2017 on Guideline of Internal Control Standard for Commercial Banks. Internal Control is a supervisory mechanism established by the Bank's management on an on going basis.

The effective Internal Control System (SPI) is an important component of the Company's management and serves as a basis for the Company's sound and safe operational activities. The effective SPI can assist the Board of Directors and Board of Commissioners to safeguard the Company's assets, ensure reliable financial and managerial reporting, improve the Company's compliance with laws and regulations, and reduce the risk of loss, deviations and violations of prudential aspects.

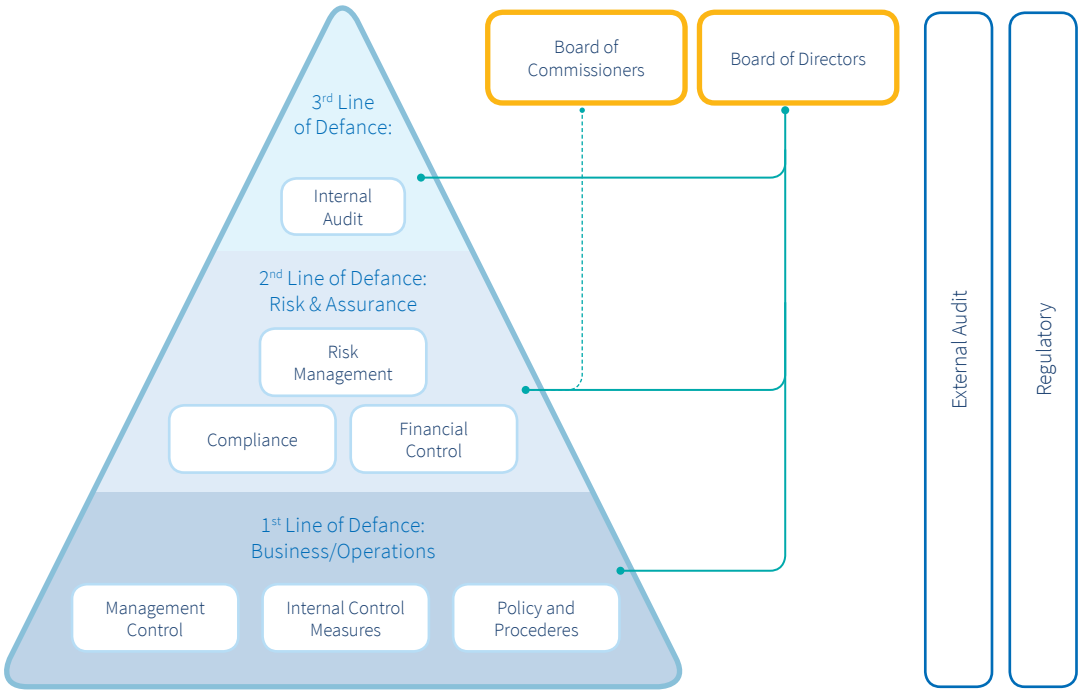
As a process carried out by the entire range of the Company, the Internal Control System was implemented in strategy establishment throughout the organization and was designed to identify the occurrence possibility of an event that might affect the company, and to manage risks to stay within the risk appetite, to provide sufficient confidence in the achievement of corporate goals.

Framework of Internal Control System

The Internal Control System Framework was implemented in all processes and decisions in the process of planning, execution and evaluation in the implementation of the Code of Conduct, the division of duties, authorities, procedures in which there were risk assessment, risk mitigation, limit setting, approval, and adequate reporting.

The framework of the internal control system adopted by Bank Mandiri was the Three Lines of Defense concept, which was a current implementation of the control strategy in accordance with the

COSO-Internal Control Framework monitoring system. This concept was a collaborative role of -on going monitoring dan separate monitoring by involving business units as managers of internal control aspects in the work unit and appointing units acting as Quality Assessment, comply unit, Inspection, Risk Management and Internal Audit role the series of defense of control.



Remarks:

1) Business Unit/Operation (first line of defense): As a risk owner played an important role in managing the internal control aspects of its work unit was to ensure a conducive control environment and consistent implementation of risk management policies and procedures.
2) Risk and Compliance Unit (second line of defense): Developing and monitoring the implementation of overall corporate risk management, supervision to enable business functions to implement risk management policies and standard operating procedures in accordance with established corridors as well as monitoring and reporting the company's overall risks to the highest accountable organ in the company.
3) Internal Audit Unit (first line of defense): As an Independent Assurance playing a review and evaluation of the design and implementation of overall risk management and ensuring that first and second layers of defense worked as expected.

With the implementation of three lines of defense, it was expected to strengthen the internal control system owned by Bank Mandiri as a result of the cooperation of all lines of Bank Mandiri starting from first, second or third lines of defense.

In addition, Bank Mandiri had established the Bank Mandiri Internal Control System Policy (KSPIBM) as the basis for the implementation of the Internal Control System, which was a control mechanism established by the Board of Directors with the approval of the Board of Commissioners on an on-going basis with the following goals:

1. Maintaining and securing the Company's assets.
2. Ensuring more accurate reporting.
3. Improving compliance with the applicable regulations.
4. Reducing financial/disadvantage impacts, irregularities including fraud, and violation of prudential principles.
5. Improving organizational effectiveness and cost efficiency.

Scope of Internal Control System

The scope of Bank Mandiri's internal control referred to the Appendix of the Circular Letter of the Financial Services Authority No. 35/SEOJK.03/2017 on Guideline of Internal Control Standard for Commercial Banks. The main components of the internal control system are as follows.

Monitoring by Control Management and Culture

The Board of Commissioners was responsible for ensuring that the Board of Directors had monitored the effectiveness of the implementation of the internal control system, so that the Board of Commissioners had an active role to ensure improvement on the Company's problems that could reduce the effectiveness of the internal control system. The Board of Directors was responsible for establishing internal control policies, strategies and procedures. The Board of Directors was also responsible for monitoring the adequacy and effectiveness of the internal control system. The Board of Commissioners and the Board of Directors were responsible for improving work ethics and high integrity as well as creating an organizational culture that emphasized on all employees regarding the importance of the internal control at Bank Mandiri.

Supervision by management was conducted through the formation of a control culture through the establishment of policies and practices of human capital, among others:

1. The Company had written policies and procedures on human capital, such as recruitment, career path, payroll and remuneration systems, as well as employee coaching and development.
2. The Company periodically evaluated the performance, competence and implementation of cultural values by employees, whose results formed the basis for assignment and placement of employees.
3. The Company had an adequate organizational structure and reflected the assignment of duties and responsibilities determined in accordance with the applicable regulations.
4. The Company had written policies on the provisions and procedures for changes to the organizational structure.
5. The management of the Bank was conducted in accordance with the principles of Good Corporate Governance.
6. The Company's decision-making was determined in the Board of Directors' meeting.
7. Decision-making process was conducted on a bottom-up and top-down basis.
8. The Company adopted policies aimed at preventing the occurrence of chances for deviations or violations of prudential principles.

Identification and Risk Assessment

Risk assessment is a series of actions undertaken by the Board of Directors in the context of identifying, analyzing and assessing the risks faced in achieving the defined business goals. Management identified events potentially affecting the Company's ability to implement strategies and achieve targets effectively. The identification was made toward events that were expected to have negative (risk) impacts requiring the Company's assessment and response. Identification was also conducted on events that were expected to have a positive impact which was an opportunity for Management in the preparation of strategies to achieve the Company's targets.

The management considered all aspects of the organization in identifying potential events. Risk assessment is a set of actions starting from the identification, analysis and measurement of risks to achieve the target set. Risk assessment was conducted on all risk types attached to any process/activity that could potentially harm the Company. Bank Mandiri had written risk management policies set by the Board of Directors and approved by the Board of Commissioners.

The conditions that might cause or alter the risk included:

1. Changes in the Company's operational activities;
2. Changes of personnel structure;
3. Changes in the information system;
4. Rapid growth in certain business activities;
5. Technological development;
6. Development of new services, products or activities;
7. The occurrence of merger, consolidation, acquisition and restructuring of the Company;
8. Changes in the accounting system;
9. Business expansion;
10. Changes in laws and regulations; and
11. Changes in behavior and customer expectations.

In order to implement an effective Internal Control System, Bank Mandiri continuously identified and assessed risks that might affect the achievement of targets. The Internal Audit periodically reviewed the risk assessment generated by the Risk Management Group so that the scope of the audit was broader and more comprehensive.

Risk assessment was performed by identifying encountered risks, setting limits and risk control techniques, assessment to measurable (quantitative) and non-measurable (qualitative) risk assessments as

well as to controllable and uncontrollable risks, taking into account the costs and benefits. The risk assessment methodology became the benchmark for creating risk profiles in the form of documentation of data that could be periodically updated. Furthermore, the Bank must decide to take the risk or not, by reducing certain business activities.

The assessment covered all the faced risks, both individual and total risk, including credit risk, market risk, liquidity risk, operational risk, legal risk, reputation risk, strategic risk, compliance risk, insurance risk and intra-group transaction risk.

Control Activity and Separation of Operational Function (Operational Control)

Control activities included policies, procedures and practices giving officials and employees confidence that the direction of the Board of Commissioners and Board of Directors had been effectively implemented. Control activities might assist the Board of Directors, including the Board of Commissioners in managing and controlling risks that might affect performance or result in loss of the Company. Separation of function was intended in order that everyone in his position did not have the opportunity to do and hide mistakes or irregularities in the implementation of his duties at all levels of the organization and all steps of operational activities.

The management established measures to respond to risks based on assessments of relevant risks and controls. Response actions might include risk avoidance, or risk reduction, and/or risk sharing, and/or risk acceptance as applied in the Company policy. In considering response actions, the Management considered cost and benefits, and selected response actions leading to the likelihood and impact in accordance with the risk tolerance and risk appetite of the Bank.

Control activities included the activities of segregation of duties.

1. Control Activities
   The control activities involved the whole range of Bank Mandiri. Control activities included planning, setting policies and procedures, implementing controls and an early verification process to ensure that policies and procedures were consistently adhered to, and were inseparable from every function or daily activity.

   Control activities were implemented at all levels of function within the Company's organizational structure, including:
   a. Review by the Board of Directors (Top Level Review)
      The Board of Directors periodically requested for information (explanation) and operational performance reports from the Head of Work Unit in order to review the realization outcomes compared to the established targets. Based on the review, the Board of Directors immediately detected problems, such as control weaknesses, financial report errors or other frauds.
   b. Review of Operational Performance (Functional Review)
      This review was carried out by the SKAI at the time of review or in the process of reporting to the regulator.
      - Reviewing the risk assessment (risk profile report) generated by the risk management unit.
      - Analyzing operational data, both data related to risk and financial data, i.e., verifying details and transaction activities compared to the output (report) generated by the risk management unit.
      - Reviewing the realization of the implementation of work plans and budgets made by each work unit (Group)/ Branch, in order to:

      (a). Identifying the cause of significant deviations.
      (b). Determining requirements for corrective actions.

      b. Control in the information system
      - The Company conducted verification on the accuracy and completeness of transactions and the implementation of authorization procedures in accordance with the applicable regulations.
      - The Company carried out information technology control measures to produce a system and data that its confidentiality and integrity were kept as well as supported the achievement of the Company's goals.
      - Control in the information system included:

      (a). Control of the operations of data centers (databases), procurement systems, development and maintenance of systems. Control was applied to mainframe, server and user workstation, and network.
      (b). Application control was implemented to programs used by the Company in processing transactions and to ensure the availability of an effective audit process and to check the accuracy of the audit process.

   c. Control of physical assets (physical controls)
      - Physical asset control was implemented to ensure the physical security of the Company's assets.
      - Control of physical assets included securing assets, records and documentation as well as limited access to application programs.
      - The Company conducted periodic checks on the value of assets (appraisal).

   d. • Documentation
      - The Company formalized and adequately documented all policies, procedures, systems and standards.

- All policies, procedures, operating systems and accounting standards were updated periodically to reflect actual operational activities.
- Upon request, documents were always available for the benefit of internal auditors, external auditors and the Banking Supervisory Authority.
- Internal Audit assessed the accuracy and availability of such documents when conducting routine and non-routine audits.

2. **Segregation of Duties**
   a. Separation of function was intended in order that everyone in his position did not have the opportunity to do and hide mistakes or irregularities in the implementation of his duties at all levels of the organization and all steps of operational activities.
   b. The organizational structure was made by separating the function 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 every activity and avoid conflict of interest.
   c. In the implementation of the separation of functions, the Company conducted the following measures, including:
      - Determining certain functions or tasks that were separated or allocated to several persons in order to reduce the risk of manipulation of data/information or misuse of assets of the Company;
      - Separation of functions was not limited to front and back office activities, but also in the context of controlling:
        (a). approval of expenditure and realization of expenditures;
        (b). accounts of customer and accounts of the Company's owners;
        (c). transactions in the books of the Company;
        (d). providing information to customers of the Company;
        (e). assessment of the adequacy of credit documentation and monitoring of debtors after credit disbursement;
        (f). other business activities that might create a conflict of interest;
        (g). Independence of risk management function in the Company.
      - Directors and Employees had adequate job description that contained functions, duties, authority and responsibility.
      - Directors and Employees were prohibited from concurrent positions in the internal environment which might create a conflict of interest.

Accounting System/Finance (Financial Control), Information and Communication

Bank Mandiri had an Information System that could generate reports or provide sufficient and comprehensive data/information on business activities, financial conditions, implementation of risk management, compliance with the applicable rules and regulations, market information or external conditions and conditions required for a right decision making.

1. The Company determined:
   a. Written policies and procedures governing the working relationships, duties and responsibilities of the Information System Technology Work Unit with other Work Units or users,
   b. Written standards governing procurement, design and development (enhancement), maintenance, operation, performance monitoring, documentation and changes in Information Systems Technology.
2. The internal control system shall at least include the provision of a reliable/adequate information system on all the Company's functional activities, particularly the significant functional activities and high potential risks. Such information systems, including electronic data storage and use systems, must be secured, monitored by independent parties (internal auditors) and supported by an adequate contingency program.
3. The Company had Business Continuity Management and conducted tests on it for all systems/applications and critical infrastructure as per Business Impact Analysis periodically.
4. The Company ensured that information security was effectively implemented to ensure that the maintained information had kept confidentiality, integrity and availability.
5. Information security was conducted on aspects of technology, human capital and the process of using Information Technology based on the assessment of the owned risk of information.
6. The Company maintained a system of user access authority (access right matrix system.
7. Particularly with regard to internal control over the administration of systems and information systems, the Company observed:
   a. the availability of sufficient evidence and documents to support the audit trail process. The audit trail process should be implemented effectively and documented. Internal Audit shall assess the effectiveness and accuracy of the audit trail process when evaluating the implementation of internal controls;

b. Implementation of control over the computer system and its security (general controls) as well as control over software applications and other manual procedures (application controls);
c. As part of the recording or bookkeeping process, the information system must be supported by a good accounting system including the establishment of transaction recording procedures and retention schedules.

8. One of the objectives of the Internal Control System was to ensure the availability of more accurate, complete, timely and relevant reports in order to make a decision by the Management.

The Company's Accounting System fulfilled the following matters:

1. The Company had written accounting policies complying with generally accepted accounting principles.
2. The Company's Accounting System included methods and records in order to identify, classify, analyze, categorize, record/book and report all transactions and activities of the Company.
3. The Accounting System must be applied consistently and persistently to all transactions of the Company.
4. The Company was required to reconcile the accounting data with the management information system every month. The results of reconciliation were documented in an orderly manner.
5. Each Work Unit that had responsibility for recording every transaction shall record transactions promptly, carefully and thoroughly, and conduct the process of control and monitoring to:

a. Ensure that every transaction had been booked in accordance with the proper ledger;
b. make sure that every ledger had been in line with the details; and
c. settle outstanding account (s) into the ledger (temporary account) immediately;
d. so as to give an idea of the actual condition and performance of the Company.

6. Each Work Unit that using forms or working papers must use standardized forms or papers and contain appropriate safeguard elements supported by adequate documentation.

Monitoring Activities and Deviation Correction Action

1. Management conducted on-going monitoring of the overall implementation effectiveness of the Internal Control System including but not limited to the effectiveness and safety of the use of information technology.
2. The Board of Commissioners ensured that the Management had monitored the implementation effectiveness of the Internal Control System and ensured that the Management had monitored the effectiveness and safety of the use of information technology.
3. Monitoring of the Company's key risks was prioritized and served as part of daily activities including regular evaluations, by the Work Unit, the Compliance Group, the Risk Management Group and the Internal Audit.
4. The relevant work units monitored the adequacy of the Internal Control System continuously in relation to changes in internal and external conditions and increased the capacity of the Internal Control System in order to improve its effectiveness.

Weaknesses in the Internal Control System, whether identified by the Risk taking Unit, Internal Audit or any other party, were immediately reported to the Management. Weaknesses of a material internal control system were also reported to the Board of Commissioners.

Conformity of Internal Control with The Framework of The Committee of Sponsoring Organizations of The Treadway Commission (COSO)

The internal control system of Bank Mandiri complied with the Internal Control Integrated Framework developed by The Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2013. Internal control objectives under COSO included operational objectives, reporting objectives and compliance objectives.

Operational objectives related to the effectiveness of operating efficiency. The reporting objective related to the interests of financial reporting meeting the reliable, timely, transparent criteria and other requirements stipulated by the regulator and the Company. While the compliance objective related to the Company's compliance with laws and regulations. Internal Control System consisted of 8 components that were mutually related to each other and determined the effectiveness of its application, namely:

Internal Environment

Internal environment became the basis for the Management in assessing risk and control as well as how to respond. It was the basis and the driving factor for the operation of the other seven components of the Internal Control System.

In its implementation, effective Internal Environment was reflected in the stipulation of written authorization/approval policies and procedures set forth in the policy architecture of Bank Mandiri, and standard of employee recruitment emphasizing on educational

background, work experience, prior achievement and integrity as well as good behavior in line with the policy of Bank Mandiri. In addition, the Internal Environment was also reflected in the determination of authority and responsibility of all employees according to their functions and written in the job description and code of conduct. Performance evaluation of all personnel reviewed periodically and imposing appropriate sanctions to any disciplinary action were also part of the Internal Environment component.

Objective Setting

Bank Mandiri set objective setting as a requirement for effective event identification, risk assessment and risk response process. Implementation of objective setting at Bank Mandiri was through the determination of key performance indicator (KPI) of work units in accordance with the corporate goals and in line with each other. In addition, the head of the work unit always communicated the mission/strategy and business targets (cascading) and believed the targets and goals of the company had been understood and implemented by all employees.

Event Identification

Management identified events potentially affecting the ability of Bank Mandiri to implement strategies and achieve targets effectively. The identification was made toward events that were expected to have negative (risk) impacts requiring the assessment and response.

Identification was also conducted on events that were expected to have a positive impact which was an opportunity for Management in the preparation of strategies to achieve the Company's targets. Management also considered all aspects of the organization in identifying potential events.

Work units needed to conduct Risk Control Self Assessment (RCSA), setting a risk profile that contained all events and significant risks to the achievement of goals that had been evaluated.

Risk Assessment

Risk assessment is a set of actions starting from the identification, analysis and measurement of the Company's risks to achieve the target set. Risk assessment was conducted on all risk types attached to any process/activity that could potentially harm the Company.

Each work unit had identified key processes and risks of each defined goal and documented on the risk profile of the work unit. Business planning of Bank Mandiri had considered the results of risk evaluation. The risk profile evaluation of the work unit was carried out periodically to adjust to the potential risks that arose at any time.

Risk Response

Management determined measures to respond to risks based on an assessment of risk and relevant controls. The risk profile of each work unit had included all significant risks and control had been established. Bank Mandiri had also implemented an early warning system in any risky business process to monitor changes in risk factors and to support the sustainability of risk management strategy assessments.

Control Activities

Control activities included the segregation of duties in all Bank Mandiri processes and activities such as the imposition of dual control on all business processes (branches, credit and Information and Technology), tiered supervision responsibilities attached to each business activity, four eyes principle in the segment credit process as well as the implementation of three lines of defense and combined assurance to ensure controlled layered activities.

Information And Communication

Bank Mandiri had had an Information System that could generate reports or provide sufficient and comprehensive data/information on business activities, financial conditions, implementation of risk management, compliance with the applicable rules and regulations, market information or external conditions and conditions required for a right decision making.

Bank Mandiri had an Information System that could generate reports or provide sufficient and comprehensive data/information on business activities, financial conditions, implementation of risk management, compliance with the applicable rules and regulations, market information or external conditions and conditions required for a right decision making.

Monitoring

Monitoring included monitoring activities as well as correction of weaknesses and corrective action of deviations. It was reflected in the establishment of relevant information monitoring facilities from the Management including mechanisms to review and monitor the effectiveness of controls through the effective implementation of three lines of defense.

Implementation Evaluation of Internal Control System

Management was responsible for the implementation of a reliable and effective Internal Control System and was obliged to promote an

effective risk culture and must ensure that it was inherent at every level of the organization.

Internal Audit was responsible for evaluating and taking an active role in improving the effectiveness of the Internal Control System on an ongoing basis in relation to operational implementation in achieving the targets set by the Company. Internal Audit conducted periodic review and examination of all activities in the Work Unit and subsidiaries.

Evaluation results were submitted to the management for follow-up and monitored for implementation to ensure that the Internal Control System run effectively. In order to strengthen the Internal Control System, specifically to control fraud, the Company adopted a comprehensive and integralistic anti-fraud strategy as part of its strategic policy. Based on the evaluation that had been conducted during 2017, it showed that the internal control system at Bank Mandiri had been adequate.

Quality Improvement of Internal Control System

Organizational developments and transactions in both volume and complexity as well as increased business competition were accompanied by the increased risk of the Company, thus requiring the Company to continuously improve the quality of its internal control system so that the Company's operations could run effectively and efficiently. An effective Internal control system provided assurance to all stakeholders that the Company's operations were carried out with sound governance and in accordance with the principles of prudence.

Efforts that had been made to improve the quality of the Bank Mandiri internal control system were, among others, by integrating the assurance function to create synergies in order that the implementation of assurance could run more effectively. In addition, Bank Mandiri also continuously improved risk and control awareness for all levels of Bank Mandiri to create an effective control and cultural control environment and support the achievement of the Company's goals.

Compliance Function

The increasingly tough competition and business scope of Bank Mandiri was a challenge to be aware of compliance risks. A precautionary measure was needed to minimize any violation of the applicable laws and regulations. Implementation of compliance function was not limited only to the prevention of law violations, but also to the underlying soul and spirit. It was important to maintain the reputation of Bank Mandiri as an institution engaging in financial services.

As part of good corporate governance process and in the framework of performing compliance function under the Regulation of Finance Service Authority No. 46/POJK.03/2017 on the Implementation of the Compliance Function of Commercial Banks, Bank Mandiri had a policy and standard of compliance procedures that define the task and responsibility of the Compliance Work Unit (SKK) in performing the compliance function.

Organization Structure of Compliance Function

The organization performing Compliance Function was set forth in the Bank Mandiri Compliance Policy (KKBM) that was further elaborated in detail in the Compliance Procedure Standard (SPKp). The organization consisted of:

1. Director in charge of the Compliance Function
2. Compliance Work Unit
3. Compliance Work Unit at Agency