## Risk Management Process

The Company's Risk Management process as stipulated in the Risk Management Policy is as follows:

1. Risk Management is carried out at all levels of the Bank up to the operational level both transactionally and at the portfolio level.
2. Risk Management is carried out individually and at consolidated/integrated level with the Subsidiaries, while taking into account the regulations and business characteristics of the Subsidiaries.
3. The Risk Management process is a dynamic process and is routinely compared to industry best practices and applicable regulations to be adjusted and updated when necessary.
4. The implementation of Risk Management is carried out in a series consisting of:

a. **Risk identification**
Risk identification aims to determine the types of risks inherent in each functional activity that have the potential to harm the Bank.

b. **Risk measurement**
Risk measurement aims to determine the risk exposure inherent in the Bank's activities to be compared with the Bank's risk appetite, hence the Bank can take risk mitigation measures and determine capital to cover residual risk.

c. **Risk monitoring**
Risk monitoring aims to compare the set risk limits with the risk exposure that is being managed.

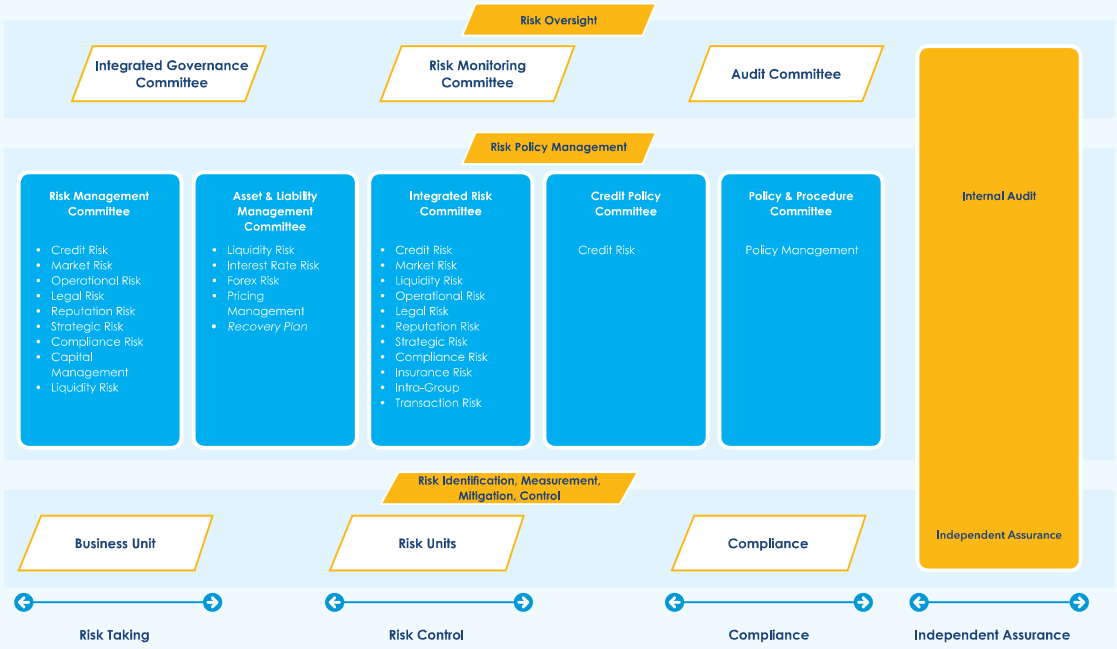
d. **Risk control**
Risk control is carried out on the potential for the occurrence of overreach of the risk limit that has been set and can be tolerated by the Bank.

# RISK MANAGEMENT FRAMEWORK

Bank Mandiri's Risk Management Framework is structured within the Bank's Risk Governance Structure, comprising three key components: Risk Oversight, Risk Policy and Management, and Risk Identification, Measurement, Mitigation, and Control. These elements are reinforced by the Audit Unit, as Independent Assurance to ensure the effectiveness of implementation.

In essence, the framework and governance of Bank Mandiri's risk management can be summarized as follows:

## BANK RISK MANAGEMENT POLICY




Bank Mandiri's Risk Governance Structure is developed based on four Risk Management Pillars as follows:

## Board of Commissioners and Board of Directors Active Supervision

The risk management framework and governance at Bank Mandiri are structured to ensure comprehensive oversight and execution. The Board of Commissioners oversees risks through the Audit Committee, Risk Monitoring Committee, and Integrated Governance Committee. The Board of Directors is responsible for risk policy and management, facilitated through risk-related Executive Committees, including Management Committee, Asset & Liability Management Committee, Integrated Risk Committee, Credit Policy Committee, dan Policy & Procedure Committee Capital & Subsidiaries Committee, and Integrated Risk Committee. Operationally, the Risk Management Unit, in collaboration with the Business Unit and Compliance Unit, carries out the functions of risk identification, measurement, mitigation, and control.

The duties, responsibilities, and authorities of the Board of Commissioners related to active supervision in Risk Management activities include, among others:

1. Evaluating and approval of Risk Management Policy;
2. Evaluating the prepared-and-determined strategies by the Board of Directors in managing risks according to the regulatory taxonomy and other risks such as country risk and cyber risk;
3. Evaluating the Board of Directors' responsibility for the implementation of the Risk Management Policy;
4. Evaluating and deciding the Board of Directors' application related to transactions that require the approval of the Board of Commissioners;

5. Requesting explanation and/or accountability of the Board of Directors on Financing to certain large borrowers;
6. Providing approval on the funding to related parties;
7. Conducting active oversight, including, among others, understanding the nature and level of risks faced by the Bank, assessing the adequacy of the quality of risk management and linking the risk level with capital adequacy of the Bank;
8. Conducting active supervision related to anti-Fraud which at least includes the following:
   a. Development of anti-Fraud awareness and culture in all levels of the organization, including anti-Fraud declarations and adequate communication on behavior categorized as Fraud;
   b. The signing of integrity pact by all organizational ranks of the Bank;
   c. Preparation and supervision of the implementation of a code of conduct related to fraud prevention for all levels of the organization;
   d. Preparation and supervision of the implementation of an anti-Fraud strategy as a whole;
   e. Development of the quality of human resources (HR), particularly those related to increasing awareness and control of Fraud;
   f. Monitoring and evaluation of Frauds and determination of follow-up; and
   g. Development of effective communication channels for the Bank's internal and external parties, hence all executives and employees of the Bank understand and comply with the applicable policies and procedures, including policies and procedures for fraud control.
9. Providing approval, oversight and evaluation on the implementation of the Action Plan (Recovery Plan).
10. For Resolution Plan, the Board of Commissioners shall:
    a. Approve the Resolution Plan;
    b. Supervise the Bank's fulfillment in compiling, updating, and/or improving the Resolution Plan to the Deposit Insurance Corporation;
    c. Evaluate the Resolution Plan that has been prepared by the Board of Directors;
    d. Supervise the implementation of plans to overcome potential obstacles to the implementation of resolution options.
11. Maintaining and monitoring the Bank's Soundness Rating and take the necessary measures to maintain and/or improve the Bank's Soundness Rating;

To implement risk management as mandated by the Ministry of SOEs, the Board of Commissioners is responsible for determining the Bank's Risk Classification based on the level of Risk Intensity. This assessment considers the Bank's size and complexity dimensions, as proposed by the Board of Directors, in compliance with applicable regulations.

To implement Integrated Risk Management, the Board of Commissioners is responsible to:
1. Direct, approve, and evaluate Integrated Risk Management policies;
2. Evaluate the implementation of Integrated Risk Management policies by the Board of Directors of the Main Entity.
3. Ensure the implementation of Integrated Risk Management is in accordance with the characteristics and complexity of the Financial Conglomeration business.

The duties, responsibilities, and authorities of the Board of Directors related to Risk Management activities include:
1. Developing and proposing Risk Management policies and strategies in writing and comprehensively;

## BANK RISK MANAGEMENT POLICY

2. Responsible for the implementation of the Risk Management Policy and risk exposure taken by the Bank as a whole;
3. Evaluating and deciding transactions that require the approval of the Board of Directors;
4. Developing a culture of Risk Management at all levels;
5. The active supervision of the Board of Directors related to anti-Fraud is the same as that of the Board of Commissioners as stated in the duties and responsibilities of the Board of Commissioners;
6. Ensuring the improvement of human resource competencies related to Risk Management;
7. Ensuring that the Risk Management function has operated independently;
8. Conducting periodic reviews to ensure;
   a. Accuracy of risk assessment methodology;
   b. Adequacy of Risk Management information system implementation;
   c. Accuracy of Risk Management policies and procedures, as well as setting risk limit and/ risk threshold.
9. Conducting active supervision includes, among others, understanding the nature and level of risks faced by the Bank, assessing the adequacy of the quality of risk management, and linking the risk level with capital adequacy of the Bank;
10. Developing and implementing the Bank's Recovery Plan, which includes:
    a. Developing a realistic and comprehensive Recovery Plan;
    b. Submitting the Recovery Plan to shareholders at the GMS for approval;
    c. Communicating the Recovery Plan to all ranks or levels of the Bank's organization;
    d. Evaluating and testing (Stress Testing) the Action Plan (Recovery Plan) periodically; and
    e. Implementing the Recovery Plan effectively and in a timely manner.
11. Developing and implementing a Resolution Plan which includes:
    a. Preparing, updating, and/or making improvements to the Resolution Plan;
    b. Ensuring the accuracy and completeness of data, information, and/or documents in compiling, updating, and/or improving the Resolution Plan, which is submitted to the Deposit Insurance Corporation;
    c. Submitting a Resolution Plan to the Board of Commissioners and Shareholders at the General Meeting of Shareholders for approval;
    d. Submitting a Resolution Plan, updating and/or improving the Resolution Plan to the Deposit Insurance Corporation in accordance with the predetermined time limit;
    e. Implementing plans to overcome potential obstacles to the implementation of resolution options.
12. Maintaining and monitoring the Bank's Soundness Rating and take the necessary measures to maintain and/or improve the Bank's Soundness Rating;
13. Implementing other Risk Management functions in accordance with laws and regulations, articles of association, and/or decisions of the General Meeting of Shareholders (RUPS)/ Minister of State-owned Enterprises (SOEs).

To comply with risk management regulations set by the Ministry of SOEs, the Board of Directors is responsible for classifying subsidiary company risks based on the level of risk intensity. This classification considers the dimensions of size and complexity in alignment with applicable regulations.

To implement Integrated Risk Management, the Board of Directors is responsible to:

1. Develop an Integrated Risk Management Policy in writing and comprehensively;
2. Implement the established Integrated Risk Management Policy;
3. Develop a risk culture as part of the implementation of Integrated Risk Management in Financial Conglomerates;
4. Ensure the effectiveness of human resource management which includes the competence, qualifications, and adequacy of human resources in the Main Entity to carry out the Integrated Risk Management function;
5. Ensure that the implementation of Integrated Risk Management has been carried out independently;
6. Periodically evaluate the results of the Integrated Risk Management Unit review of the Integrated Risk Management process;
7. Ensure the implementation of Integrated Risk Management in accordance with the characteristics and complexity of the Financial Conglomerates business.

To enhance the effectiveness of supervisory duties and responsibilities in implementing Risk Management, the Board of Commissioners and the Board of Directors may establish committees in accordance with applicable regulatory provisions.

Bank Mandiri's risk management organization consists of:

1. Board of Commissioners
2. Committee under the Board Commissioners
3. Board of Directors
4. Committee under the Board of Directors
5. Director in charge of Risk Management function;
6. Risk Management Unit (SKMR);
7. Operational Unit (risk-taking unit);
8. Internal Audit Unit (SKAI);
9. Compliance Unit.

The Risk Management Unit (SKMR), the Internal Audit Unit (SKAI) and the Compliance Unit concurrently serve as an Integrated Unit.

## Adequacy of Policies, Procedures, and Limits Setting

Bank Mandiri implements risk management guided by its Risk Management Policy, which serves as the primary framework for managing risks. For specific business areas such as credit, treasury, and operations, the Bank has detailed policies and procedures that define limits for activities at both the portfolio and transactional levels. These policies and procedures are integrated into every aspect of the Bank's operations, evaluated, and updated annually. In line with SEOJK 34/SEOJK.03/2016 on the Implementation of Risk Management for Commercial Banks, the Bank's policies and procedures are based on a Risk Management Strategy by taking into account the level of risk to be taken (Risk Appetite). Risk Appetite represents the type and level of risk the Bank is willing and able to take, within its risk capacity, to achieve or exceed its business objectives.

Bank Mandiri's Risk Appetite is manifested through the Risk Appetite Framework which is a strategic decision-making that describes Bank Mandiri's risk strategy. Risk Appetite is reflected in the Bank's business strategy and objectives.

Risk appetite is articulated through a Risk Appetite Statement (RAS), which is a formal guideline in the risk-taking process to achieve business targets. RAS is pivotal because it will provide clear and consistent direction to all levels of Bank Mandiri on the Bank's risk-taking ability.

### Adequacy of Risk Identification, Measurement, Monitoring, and Control Processes, as well as Risk Management Information Systems

Bank Mandiri conducts Risk Identification, Measurement, Monitoring, and Control processes, as well as operates its Risk Management Information System, through the Enterprise Risk Management (ERM) framework. The ERM implementation at Bank Mandiri employs a two-pronged approach to ensure that risks are not only well mitigated through daily business processes, but also in unexpected conditions (downturns) through capital reserves.

### Internal Control System

Bank Mandiri implements an Internal Control System for its Risk Management function through the Three Lines Model, where responsibilities are shared among the first, second, and third lines of defense.

The Internal Audit Unit, as the third line, conducts assurance and consulting activities to evaluate the adequacy of the Bank's internal control system, risk management, and governance processes, in compliance with applicable laws, regulations, and Bank policies.

# INTEGRATED RISK MANAGEMENT IMPLEMENTATION

Bank Mandiri has been implementing consolidated/integrated risk management since 2008, inline with the issuance of Bank Indonesia Regulation No. 8/6/PBI/2006 on the Implementation of Consolidated Risk Management for Banks that Control Subsidiaries. In its development, the regulation was replaced by Financial Services Authority Regulation No. 38/POJK.03/2017 on the Implementation of Consolidated Risk Management for Banks that Control Subsidiaries. In addition, Bank Mandiri has also been implementing integrated risk in accordance with Financial Services Authority Regulation No. 17/POJK.03/2014 on the Implementation of Integrated Risk Management for Financial Conglomerates. In the implementation of integrated risk management, Bank Mandiri is also guided by the Integrated Good Corporate Governance Guidelines, which comply with Financial Services Authority Regulation No. 18/POJK.03/2014 on the Implementation of Integrated Good Corporate Governance for Financial Conglomerates.