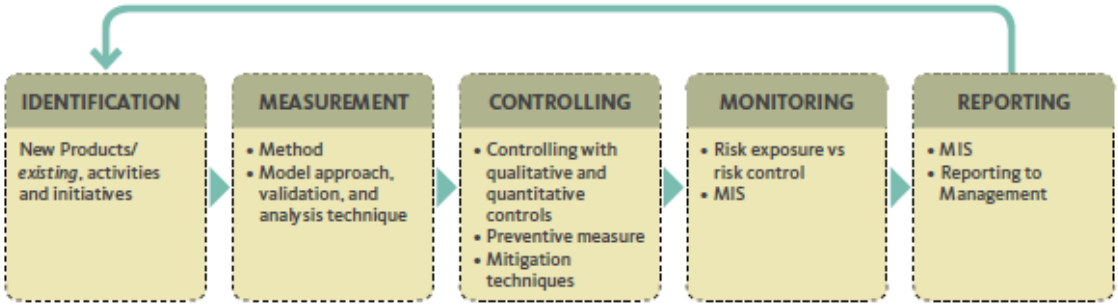
Risk Management

Maybank Indonesia continues to strive to conduct regular monitoring of the level of risk faced by the Bank, including the entire risk management process that is carried out based on the application of GCG principles. The Bank also continues to develop a robust risk infrastructure and culture with the aim of providing added value to all stakeholders, as well as carrying out comprehensive capital management and ensuring sustainable business growth.

The implementation of comprehensive risk management is one of the important and significant aspects for the Bank's success in effectively managing the various risks it faced. Therefore, the Bank pays great attention to the implementation of effective and efficient risk management in daily banking operational activities.

The implementation of risk management aims to protect the Bank from possible losses arising from its various activities and maintain the level of risk in accordance with the the Bank's business strategy and business growth. Therefore, the Bank maintains a balance between risk and benefits in order to produce sustainable long-term value growth for shareholders.

RISK MANAGEMENT SYSTEM IMPLEMENTED BY THE BANK



The Bank has implemented risk management consisting of 5 (five) main stages that constitute a sustainable cycle as follows:

The 5 main stages have been implemented by the Bank as described below:

- Sufficient organizational structure of Bank organization: Audit Committee, Risk Oversight Committee, Nomination and Remuneration Committee, Integrated Good Corporate Governance Committee, Risk Management Committee, Assets & Liabilities Management Committee, Internal Audit Committee, Information Technology Steering Committee, Integrated Risk Management Committee, Internal Audit Work Unit, Compliance Work Unit, Risk Management Work Unit and Integrated Risk Management Unit. In addition, the implementation of Integrated Good Corporate Governance is also sustained by the integrated work units' performance such as the Integrated Compliance Unit and the Internal Audit Work Unit. The Bank's own organizational structure is constantly updated to keep up with the needs of organizations and businesses.
- Implementation of the three lines of defense and four-eye principles as part of the Bank's commitment to systematically identify, control, monitor and mitigate risks sustainably.
- Risk Management infrastructure and governance in accordance with the complexity of business activities, risk profiles, risk levels to be taken, as well as regulations set by the Regulator.
- Develop a comprehensive Business Continuity Management (BCM) that serves as a guide for the Company to continue operating during an emergency.
- Raise awareness of Risk Management through risk awareness campaigns, posters and other internal publication media, as well as training conducted at head office, branch office and subsidiaries.

RISK MANAGEMENT DIVISION

The Bank also makes regular reviews and improvements in all of its policies and procedures that shape an effective risk management strategies in line with the increasingly complex business expansion. In managing risk management, a governance structure is needed to improve the four eyes principle and transparency in the risk management process. To ensure a sustainable implementation and supervision of risk management, the Bank has established a Risk Management Division.

RISK MANAGEMENT

In managing such risks as well as other potential risks, the Bank shall exercise appropriate control and mitigation of those risks identified and measured

Risk Control

Compliance and effective controls shall be established to regulate risk exposures and ensure alignment with a predetermined risk appetite. The risk appetite aligns the needs of all stakeholders as it serves as a risk manager and encourages business activities in current and future business environments. An effective risk appetite can be a powerful force that will drive the implementation of risk culture at the Bank.

Qualitative and quantitative risk controls include risk limits and triggers/thresholds set to monitor and manage identified risk exposures. Risk control also provides the means to manage risk identification, initiate discussions, take appropriate precautions and consider actions that need to be carried out in accordance with policies and procedures. Caution should be exercised to the conformity of approval, follow-up plan, and exposure review to ensure the effectiveness of risk management. The controls executed by the Bank will be reviewed periodically to ensure the effective control over the risk appetite and risk limits of the Bank.

Risk Mitigation

Risk mitigation techniques aim to minimize the impact of existing risks or avoid the occurrence of new risks (emerging risks). The techniques include the establishment of specific hedging, funding strategies, and insurance. In addition, the Bank has already in place and has implemented a Disaster Recovery Plan and Business Continuity Plan (BCP) as part of Business Continuity Management.

Both the Disaster Recovery Plan and the Business Continuity Plan have been devised and executed to help strengthen the Bank's resilience against risks that may cause serious impact to the Bank's operations, including plans to ensure the sustainability of critical business functions over a certain period of time during the recovery.

The Recovery Plan offers a systematic approach to handling potential disruptions on capital, liquidity, and funding that may have undesirable impacts on financial liquidity and solvency.

THE BANK RISK EXPOSURE

Currently, the Bank is exposed to certain risks that are classified based on the following grounds:

a. POJK No.18/POJK.03/2016 concerning Application of Risk Management for Commercial Banks:
   1. Credit Risk
   2. Market Risk
   3. Liquidity Risk
   4. Operational Risk
   5. Compliance Risk
   6. Legal Risk
   7. Reputation Risk
   8. Strategic Risk There are 2 (two) additional risks related to the Shariah Bank Business Unit according to POJK No.8/POJK.03/2014 namely:
   9. Profit Sharing Risk
   10. Investment Risk

b. POJK No.17/POJK.03/2014 on the Implementation of Integrated Risk Management for Financial Conglomerates There are 2 (two) types of additional risks related to the implementation of integrated risk management for a Bank's Finance Conglomerate under these provisions:
   1. Risk of Intra-Group Transactions
   2. Insurance Risk.

In addition to the risks mapped out under these regulations, due to the technological developments and various factors including business competition, market growth, and more expectations from regulators, the Bank also faces other risks such as data risk and information technology risks and non-financial risks such as money laundering and outsourcing.

Therefore, in order to identify and measure these risks, the Bank should always take into account a forward looking approach. This is to ensure adequate measures made by the Bank to mitigate all risks to which the Bank is naturally exposed.

Results of Review/Evaluation on the Effectiveness of Risk Management System in 2019

Elaborated below are results of the Bank's risk management system review in 2019:

1. The development of Environmental, Social and Governance policies as a form of Sustainable Finance application.
2. The development of the Retail SME Loan Origination System (LOS) segment to support the implementation of Retail SME policy, which has been updated to meet the Bank's new business model.
3. A further improvement in Credit Card Application Scorecard to improve the quality of risk measurement for potential credit card debtors.
4. A redefinition of business segmentation to align with the Bank's targets, supported by proper risk measurement.
5. The implementation of Enterprise Crisis Simulation Exercise (ECSE) to make the Bank ready for any event of disasters or cyber-attack.
6. The implementation of DNA (Document Navigator Application) to support documenting and tracking process during new products launching and/or activities at the Bank, and a Premises Sweep Application (PSA) to support clean desk policy movement to prevent any leakage of the Bank's confidential data/information.
7. The holding of Cyber Risk Assessment Challenge Sessions to help provide an independent view of the Cyber Risk Assessment made by the IT Department to ensure that minimum key risks, risk control and risk gaps have been identified and mitigation and actions have been established.
8. Updates on Recovery Plan to ensure the Bank is always ready for any crisis condition