Risk Management Framework

The Risk Management System is designed to support the Company in realizing sound business management and achieving sustainable growth, thus optimizing shareholder value. The Company adopts a comprehensive approach to managing risks comprehensively, by improving the performance in managing uncertainty, minimizing threats, and maximizing opportunities without neglecting the principles of Risk Management that at least include the following:

1. Active supervision by the Board of Commissioners and the Board of Directors;
2. Adequacy of policies, procedures, and limits set;
3. Adequacy of Risk Identification, Measurement, Monitoring, and Control Process, as well as the Risk Management Information System;
4. A comprehensive Internal Control System.

Risk Management System

Active Supervision of the Board of Commissioners and the Board of Directors

The Board of Commissioners has clear duties and responsibilities, including:

1. To endorse the Risk Management policy, including the Risk Management strategies and framework set forth in accordance with the Risk Appetite and Risk Tolerance.
2. The Board of Commissioners and/or through the Risk Management Committee conduct regular discussions and evaluations of risk profile reports (quarterly) and Bank Soundness Level Reports are submitted to the Commissioners and Risk Monitoring Committee on a semi-annual basis as material for evaluating the implementation of risk management policies and risk management strategies.
3. The Board of Commissioners approves the Recovery Plan Document for approval through the General Meeting of Shareholders (if required) and reports it to the Financial Services Authority.
4. The Board of Commissioners also approved the Company's Risk Appetite and Risk Tolerance.
5. Evaluating the accountability of the Board of Directors and provide direction for improvement on the implementation of Risk Management policies on a regular basis. Evaluation was carried out in order to ensure that the Board of Directors managed the Company's activities and risks effectively.
6. The risk profile was submitted to the Board of Commissioners and the Risk Monitoring Committee on a quarterly basis as material for evaluating the implementation of risk management policies and risk management strategies.

The Board of Directors is responsible for the effectiveness of the implementation of Risk Management in the Company. The implementation of active supervision by the Board of Directors includes but is not limited to the following:

1. The Board of Directors is responsible for ensuring the implementation of risk management is adequate in accordance with the characteristics, complexity and risk profile of the Company.
2. The Board of Directors understands well the types and levels of risk inherent in the Company's business activities.
3. The powers and responsibilities of the Board of Directors include:
   a. Formulating written and comprehensive risk management policies and strategies.
   b. Responsible for the implementation of risk management policies and risk exposure taken by the Company as a whole.
   c. Evaluate and decide on transactions that require the approval of the Board of Directors.
   d. Develop a risk management culture at all levels of the organization.
   e. Ensuring the improvement of human resource competencies related to risk management.
   f. Ensure that the risk management function operates independently.
   g. Carry out regular reviews to ensure the accuracy of risk assessment methodologies, adequacy, implementation of risk management information systems and the accuracy of risk management policies and procedures as well as determination of risk limits.

In order to carry out these powers and responsibilities, the Board of Directors must have an adequate understanding of the risks inherent in all functional activities of the Company and be able to take the necessary actions according to the Company's risk profile. To support the aforementioned functions, the Board of Directors is equipped with a Risk Management Committee.

Apart from the above powers and responsibilities, the supervision of the Board of Directors also includes:

1. Determining the risk management organization consisting of the Risk Management Committee and Divisions that supported the implementation of risk management, namely ERMD as the Risk Management Unit, the internal control function by IAD, the Credit Risk Division as an effort to improve the commercial credit business process through the implementation of four eyes principles, the establishment of the Retail Risk Division, the compliance function was carried out by CMGD as the Compliance Unit including

the authority and responsibility of each work unit. The Risk Management Committee (KMR) had the authority and responsibility to evaluate and provide recommendations to the President Director, and the Monitoring Committee Risk had the responsibility to provide recommendations to the Board of Commissioners regarding the Implementation of Risk Management.

2. Providing directions were on reports submitted by ERMD, namely:
   a. Bank Risk Profile submitted on a quarterly basis.
   b. The Liquidity Risk Position Monitoring Report was submitted daily
   c. Securities evaluation monitoring reports (MTM) were submitted daily
   d. Stress Testing for Liquidity Risk and Market Risk on a quarterly basis
   e. The Recovery Plan report was conducted once a month and is submitted at the ALCO meeting.
   f. Data loss reports due to operational risk (LED) were submitted quarterly
   g. Market Risk Monitoring Reports were submitted daily
   h. The Liquidity Risk Position Monitoring Report was submitted on a weekly basis.
   i. The Liquidity Risk Position Monitoring Report was submitted monthly.
   j. Data reports and measuring potential operational risks through the application (BTN-RCSA) were submitted semiannually.
   k. Monthly Monitoring Report on Risk Appetite, Risk Tolerance & Recovery Plan on a monthly basis
   l. The economic sector monitoring report for lending was submitted quarterly.
   m. Report on the Legal Lending Limit (BMPK) and the Provision of Large Funds was submitted monthly.
3. Ensuring that all material risks and impacts arising from these risks had been followed up and had submitted accountability reports to the Board of Commissioners periodically. The report included a progress report and problems related to material risks along with corrective measures that have been, are being, and will be carried out.
   a. Based on the Company's Risk Profile, the types of significant risks are Credit Risk, Liquidity Risk and Operational Risk. Through the Bank's Risk Profile report, Monitoring Position and Liquidity Risk reports and Monitoring Reports regarding the Credit Risk Exposure, the Board of Directors ensures that the related Work Units are to follow up on the recommendations in these reports so that Credit Risk, Operational Risk and Liquidity Risk will better managed.
   b. Significant risk profile developments have been submitted to the Board of Commissioners through the Company's Risk Profile Report Submission mechanism on a quarterly basis.
4. Ensuring the implementation of corrective measures for problems or irregularities in the Company's business activities discovered by SKAI.
   a. The Board of Directors ensured corrective steps for problems or irregularities in the Copmany business activities through:
      - Providing directions on monitoring reports of follow-up findings of external/internal examinations that IAD periodically submits to the Board of Directors.
      - Evaluating the results of the previous year's follow-up audit at the Audit exit meeting.
      - Audit Committee Meetings.
   b. As part of developing a risk management culture, the Board of Directors ensures, among other things:
      - Risk management certification and refreshment certification program for employees and officers of the Company.
      - Provision of risk management training for new employees.
5. Developing a Culture of Risk Management, which includes Risk Awareness across all organization levels, including adequate communication to all levels of the organization concerning the importance of effective Internal Control.
   a. Making an effort to internalize the Culture of Risk Management with all employees.
   b. Risk Culture dissemination through training on overview and application of risk management in Operation Academy, Loan Academy training, General Banking Staff training, ODP Training, Supporting Staff training, Asset management training, Coaching Branch Manager, and Consultative Selling
   c. Socialization of risk awareness through corporate culture outreach programs and regular socialization quizzes of the Company's internal policies.
   d. Management Support for the Change Agent Role where all levels of Management Divisions/Desks, Regional Offices and Branch Offices are required to support the role of Change Agent and actively participate in fostering a culture of risk awareness and applying the principle of prudence in achieving superior performance.
6. Ensuring adequate financial support and infrastructure to manage and control risks. The Board of Directors ensured financial/budget adequacy through approval in the 2020 RKAP.

a. The Bank had a risk appetite and risk tolerance which are aligned with the Bank's vision, mission and business strategy (as stated in the Bank's Business Plan 2020-2022 and RKAP 2020). Risk Appetite and Risk Tolerance Strategic risk had been formulated in the Bank's internal provisions concerning Risk Management Policy Guidelines.
b. Providing direction on the Revised RKAP for 2020 and Revision of the RBB for 2020-2022 in the preparation of the Revised Bank Business Plan (RBB) document for 2020-2022 and the Revision of the Corporate Budget Work Plan (RKAP) for 2020.
c. The performance targets listed in the Revised Bank Business Plan (RBB) 2020-2022 and the Revised Corporate Budget Work Plan (RKAP) for 2020 were supported by comprehensive and measurable work papers.
d. Business growth must be in the corridor of the Bank's prudential principles, implementation of good risk management, and Good Corporate Governance.
e. In providing the RKAP and RBB direction, the Board of Directors considered strategic plans for 2020.
f. In order to achieve the 2020 RKAP target, the Board of Directors provided direction for the 2020 performance focus on 4 (four) things, namely a more sustainable increase in low-cost DPK, a more massive improvement in credit quality, a faster reduction in LAT/DAT and savings in operating costs (efficiency). With regard to this performance focus, particularly the savings in operational costs (efficiency), the Board of Directors calls for increased coordination in programs involving Branch Offices and Regional Offices.
g. Compiling the Company's strategic plan, providing direction and approval of the 2021-2023 Bank Business Plan (RBB) and submitting it to the Board of Commissioners, Bank Indonesia and the Financial Services Authority (OJK).

7. Ensuring that the Risk Management function had been implemented independently, which was reflected in, among other things, the separation of functions between SKMR that performed risk identification, measurement, monitoring and control and the work unit that carried out and completes transactions.

Adequacy of Policies, Procedures and Limit Settings

The implementation of risk management is supported by a framework that includes risk management policies and procedures as well as risk limits which are set in line with the Company's vision, mission and business strategy. In determining the risk management framework including policies, procedures and limits, it was necessary to pay attention to the following matters:

1. Risk Management Strategy
   The Risk Management Strategy set was adjusted to the overall business strategy by taking into account the level of risk to be taken and the risk tolerance. The risk management strategy aimed to ensure that the Company's risk exposure was managed in a controlled manner in accordance with the Company's policies, internal procedures as well as the prevailing laws and regulations.
2. The level of risk to be taken (risk appetite) and risk tolerance
   The level of risk to be taken (risk appetite) was the level and type of risk that the Company was willing to take in order to achieve the Company's goals. The level of risk to be taken was reflected in the Company's business strategy and objectives. Risk tolerance was the maximum level and type of risk determined by the Company (per type of risk). In formulating risk management policies, the Board of Directors provided clear directions regarding the level of risk to be taken and the Company's risk tolerance. Risk appetite and risk tolerance were considered in the preparation of risk management policies, including in determining limits.
3. Limit
   The Company had a risk limit in accordance with the level of risk to be taken, the risk tolerance and the Company's overall strategy by taking into account the Company's capital ability to be able to absorb risk or loss exposure, past experience of losses, human resource capabilities and compliance with external regulations applicable.

   Procedures and determination of risk limits include at least:
   a. Accountability and clear levels of delegation of authority.
   b. Sufficient documentation of procedures and determination of limits to facilitate the implementation of reviews and audit trails.
   c. Conducting regular reviews of procedures and determination of limits at least once a year or more frequently, in accordance with the type of risk, the needs and developments of the Company.
   d. Limit determination was carried out comprehensively on all aspects related to risk, including the overall limit, limit per risk and limit per business activity of the Company that had risk exposure.

Adequacy of the Process of Identification, Measurement, Monitoring, and Risk Control and Risk Management Information System

The process of identification, measurement, monitoring and risk control was carried out by the Risk Management Unit, in this case ERMD had a Department that had an assessment work unit to identify and measure each risk.

Monitoring and risk control were carried out periodically to mitigate significant risks to the Company, in this case ERMD had a Department that had a Risk Development work unit where one of its functions was to control risk over policies to be issued by the Company in order to minimize the risks that would be faced by the Company.

Risk identification, measurement, monitoring and control became the main parts of the risk management implementation process. Matters of concern to the Company in the implementation of the identification, measurement, monitoring, control and risk management information system processes are as follows.

Risk Identification

Risk identification was the process of finding, recognizing and recording risks. The purpose of the risk identification process was to identify all types of risks that exist in any functional activity that could potentially harm the Company.

The risk identification process is done by analyzing all sources of Risks, Risk events and Risk impacts the least on the risk of the Company's products and activities and ensures that the Risks of new products and activities have gone through a proper Risk Management process before being introduced or executed. In addition, the Company identifies risks which are carried out periodically.

Risk Measurement

The risk measurement system was used to measure the risk exposure inherent in the Company's activities to be compared with the Company's risk appetite so that the Company could take risk mitigation measures and measure the capital adequacy of the Perserian to cover residual risk. Risk was carried out regularly for both products and portfolios as well as for the entire Company's business activities.

The risk measurement method was carried out quantitatively and/or qualitatively. The measurement method was in the form of standard methods stipulated by Bank Indonesia and FSA in the framework of risk assessment and capital calculation as well as internal methods developed by the Company itself. The choice of measurement method was adjusted to the characteristics and complexity of business activities.

The risk measurement system was evaluated and refined periodically or from time to time as necessary to ensure the suitability of assumptions, accuracy, fairness and integrity of data, as well as the procedures used to measure risk. Stress tests were carried out to complete the risk measurement system by estimating the Company's potential losses in abnormal market conditions by using certain scenarios in order to see the sensitivity of the Company's performance to changes in risk factors and to identify the effects that had a significant impact on the Company's portfolio.

Stress tests were carried out regularly and review the results of stress testing and take appropriate steps if it is estimated that conditions that would occur exceed an acceptable tolerance level. The results were used as input when setting or changing policies and limits.

Risk Monitoring

Monitoring systems and procedures included monitoring of the amount of risk exposure, risk tolerance, compliance with internal limits and results of stress testing as well as consistency in implementation with established policies and procedures. Monitoring results were presented in periodic reports submitted to management in order to mitigate risks and take necessary actions.

The Company prepared an effective back up system and procedures to prevent disruptions in the risk monitoring process and carries out regular checks and reassessments of the back up system.

Risk Control

The Company's risk control system referred to the predetermined policies and procedures. The implemented risk control process was adjusted to the risk exposure and the risk level to be taken from risk tolerance. Risk control could be carried out, among others by means of hedging mechanisms and other risk mitigation methods such as the issuance of guarantees, asset securitization, credit derivatives as well as additional Company capital to absorb potential losses.

Risk Management Information System

The initial risk management information system is focused on collecting and improving the quality of the risk database which is expected to be developed and applied to the risk management information system in stages so that the process of risk measurement and risk monitoring can be conducted in an integrated manner and can be presented in a timely manner.

Currently the Company was strengthening the utilization of Risk Management Tools, so as to ensure the adequacy of the risk management information system, several system developments had been carried out including:

1. Implementing a monitoring system for monitoring market risk/interest rate risk in the banking book (IRRBB).
2. Conducting Enhancement of Liquidity Risk monitoring application (Liquidity Coverage Ratio/LCR reporting module, stress testing, week report and liquidity risk profile).
3. Utilizing Bloomberg Terminal to support the effective risk management implementation in supporting the management of liquidity risk, credit risk and other risks.
4. Strengthening the risk management role with the Development of Sustainability Environment Risk Management.
5. Performing System Credit Scoring Model (CSM) Enhancement.
6. Conducting maintenance of ISO implementation in ERMD through ISO 9001:2015 Surveillance in Enterprise Risk Management Division to improve ERMD quality service standards to all stakeholders.

Internal Control System

Internal control system was implemented effectively to the implementation of business and operational activities at all levels of the organization, the implementation of an effective internal control system became the responsibility of all operational work units and supporting work units and IAD.

Internal control systems in the determination of risk management including:

1. Conformity of internal control system with the type and level of risk inherent in the Company's business activities.
2. Determination of authority and responsibility for monitoring compliance with risk management policies and procedures as well as setting risk limits.
3. Determination of reporting paths and clear separation of functions from operational work units to work units that carry out control functions.
4. An organizational structure that clearly described the Company's business activities.
5. Accurate and timely financial reporting and operational activities.
6. Adequacy of procedures to ensure the Company's compliance with the provisions and laws and regulations.
7. An effective, independent and objective review of the Company's operational activities assessment procedures.
8. Adequate testing and review of risk management information systems.
9. Complete and adequate documentation of operational procedures, scope and audit findings as well as the response of the Company's management to the audit results.
10. Verification as well as periodical and continuous review to address the Company's material weaknesses and the actions of the Company's management to correct irregularities that occurred.

Comprehensive Implementation of Integrated Governance, Risk & Compliance (GRC)

In order to build the Bank's strategic pillars for business growth, Bank BTN implemented the GRC function in an integrated and comprehensive manner. Integrated GRC could increase the potential for superior performance achievement supported by the implementation of GCG principles and good risk management.

The work program of Integrated Governance, Risk & Comprehensive Compliance was as follows:

1. Risk Management Work Unit conducted GRC Index Scoring Preparation
2. Compliance Work Unit
    a. Conducted periodic work unit compliance mapping.
    b. Implemented Joint Audit.
    c. Strengthened APU PPT program in line with APU PPT Compliance Mandatory Regulatory.
    d. Strengthened Anti-Corruption and Gratification Control Program.
    e. Implemented Profit Check Cooperation Program of KPK.
    f. Improved corporate governance capabilities based on:
        - Standard Corporate Governance according to the Regulator.
        - Standard Corporate Governance according to ACGS (ASEAN Corporate Governance Scorecard).
        - Standard Corporate Governance according to CGPI (Corporate Governance Perception Index).
3. Internal Audit Work Unit
    a. Audit Implementation (General, ICT and Investigation).
    b. Coordinated the implementation of the Anti-Fraud/ SAF Strategy (SAF Socialization, Email Blast and SMS Blast).
    c. Improved the effectiveness of Whistleblowing System.
4. Transformation Work Unit
    a. Coordinated the implementation and preparation of the GRC
    b. Increased the effectiveness of implementing GRC in a number of work units
5. Cultural Work Unit
    a. Implementation of Corporate Culture Program
    b. Monitoring and Observing Work Units related to the Implementation of The Corporate Culture Index

Basel Implementation

In implementing risk management and anticipating the application of Basel II in particular pillar 1, the Company has implemented:

1. To calculate RWA from Credit Risk, the Bank applies a standardized approach in accordance with FSA Circular Letter No. 42/SEOJK.03.2016 dated September 28, 2016 as amended by FSA Circular Letter No. 11/ SEOJK.03/2018 dated August 15, 2018 concerning Guidelines for Calculation of Risk Weighted Assets for Credit Risk using the Standard Approach.
2. To calculate RWA from Market Risk, the Bank applies the use of the Standard Method in accordance with FSA Circular Letter No. 38/SEOJK.03/2016 dated September 8, 2016 concerning Guidelines for Using the Standard Method in Calculating the Minimum Capital Requirement for Commercial Banks by Calculating Risks Market.
3. To calculate RWA from Operational Risk, the Bank applies the Basic Indicator Approach in accordance with FSA Circular Letter No. 24/SEOJK.03/2016 dated July 14, 2016 concerning Calculation of Risk Weighted Assets for Operational Risk using the Basic Indicator Approach.

For the implementation of Basel II, especially Pillar 2, the Company had submitted the results of the risk management implementation report for the Interest Rate in the Banking Book (IRRBB) and the IRRBB calculation report to regulators on a quarterly basis in accordance with FSA Circular No. 12/SEOJK.03/2018 dated August 21, 2018 on the Implementation of Risk Management and Risk Measurement Standard Approach for Interest Rate Risk in The Banking Book for Commercial Banks.

The implementation of Company's Basel III was:

1. Submitting the results of liquidity coverage ratio (LCR) report to regulators online every month through FSA Online Reporting Application (APOLO) and Bank website every quarter according to POJK No. 42/POJK.03/2015 dated December 23, 2015 on Liquidity Coverage Ratio for Commercial Banks.
2. Submitting the results of the Net Stable Funding Ratio (NSFR) report to regulators online every quarter through the OJK Online Reporting Application (APOLO) and the Bank's website according to POJK No. 50/POJK.03/2017 dated July 13, 2017 on Net Stable Funding Ratio for Commercial Banks.
3. Calculating and reporting leverage ratio (LR) calculation trials to regulators on a quarterly basis according to the LR Consultative Paper. And starting in March 2020 the Bank had submitted the results of the LR Report to regulators on a quarterly basis through a letter to the Regulator and through the FSA Online Reporting Application (APOLO) and the Bank's website in accordance with POJK No. 31/POJK.03/2019 on Obligation to Fulfill Leverage Ratio for Commercial Banks.
4. Taking into account buffers in the calculation of minimum capital adequacy, among others:
   a. Conservation Buffer in accordance with article 6 POJK No. 11/POJK.03/2016 dated January 29, 2016 on The Minimum Capital Provision Obligation of Commercial Banks
   b. Countercyclical Buffer in accordance with PBI No. 17/22/PBI/2015 dated December 23, 2015 on Countercyclical Buffer Establishment Obligation
   c. Capital Surcharge for Systemic Banks in accordance with POJK No. 2/POJK.03/2018 dated March 26, 2018 on Systemic Bank Determination and Capital Surcharge as well as the existence of Systemic Bank bucket determination letter submitted by the regulator.

In the first semester of 2020, the calculation of KPMM Bank had implemented the national economic stimulus policy as a countercyclical policy on the impact of the spread of 2019 Coronavirus Disease following POJK Regulation No. 11/POJK.03/2020 on National Economic Stimulus as amended through POJK No. 48 /POJK.03/2020 on Amendment to POJK No. 11/POJK.03/2020 on National Economic Stimulus as a Countercyclical Policy on the Impact of 2019 Coronavirus Disease Spread.

Risk Profile and its Management Efforts

Risk Profile

Credit Risk

Credit Risk is the risk of loss due to failure of other parties to meet their obligations. Included in Credit Risk are Credit Risk due to debtor failure, Credit Risk due to concentrated provision of funds (Credit Concentration Risk), Credit Risk due to counterparty credit risk, Credit Risk due to settlement failure, and Credit Risk due to country risk.

Credit Risk can be sourced from various the Company business activities. In most company, lending is the largest source of credit risk. In addition to credit, the Company faces Credit Risks from various financial systems such as securities, acceptances, interbank transactions, trade finance transactions, exchange rate transactions and transactions as well as commitment and contingent obligations.

Market Risk

Market Risk was the risk to the balance sheet position and administrative accounts including derivative transactions, as a result of the overall change in market conditions, including the risk of changes in option prices. Market risks included, among others, interest rate risk, exchange rate risk, equity risk, and commodity risk that might harm the Bank. Market risk could come from both trading book positions and banking book positions.

Liquidity Risk

Liquidity risk is the risk arising from the inability of the Bank to meet the maturing obligations from cash flow funding sources and/or from high-quality liquid assets that can be pledged, without disturbing the activities and financial condition of the Company.

The inability to obtain funding for cash flows resulting to liquidity risk can be contributed, among others, by:

- Inability to generate cash flows from productive assets as well as from the sale of assets, including liquid assets; and/or
- Inability to generate cash flows from funding, interbank transactions and fund borrowings.

Operational Risk

Operational Risk is the risk due to inadequate and/or malfunctioning of internal processes, human error, system failure, and/or the occurrence of external events that affect the Company's operations.

Operational risks can be sourced from among others HC, internal processes, systems and infrastructure, as well as external events.

These sources of risk may cause events that have an impact on the Bank's operations so that the emergence of these types of Operational Risk events is one measure of success or failure of Risk Management for Operational Risk. The types of operational risk events can be classified into several types of events such as internal fraud, external fraud, labor practices and work environment safety, customers, business products and practices, physical damage, business activity disruptions and system failures, and process and execution errors, including fraud arising from money laundering and terrorism financing activities.

Legal Risk

Legal Risk is the risk due to legal claims and/or weaknesses of juridical aspects. Legal risks can be sourced among others from weaknesses in juridical aspects caused by weak engagement made by the Bank, the absence and/or changes in legislation that causes a transaction that has been conducted by the Bank to be incompatible with the provisions, and a good litigation process arising from third party lawsuit against the Bank or the Bank against third parties.

Strategic Risk

Strategic Risk is the risk due to inaccuracy in making and/or implementing a strategic decision and failure to anticipate changes in the business environment. Strategic risk can be sourced from weaknesses in the process of strategy formulation and inaccuracies in the formulation of strategy, inadequate management information systems, inadequate internal and external environmental outcomes, setting strategic goals that are too aggressive, inaccurate implementation of strategies, and failure to anticipate changes in business environment.

Compliance Risk

Compliance Risk is the risk due to the Company not complying with and/or not implementing the laws and regulations, such as credit risk related to the Minimum Capital Adequacy Requirement (KPMM), Earning Asset Quality, Formation of CKPN, Legal Lending Limit (BMPK), market risk related to Net Open Position (NOP) provisions, strategic risk related to Work Plan provisions. Annual Budget (RKAT), and other risks associated with certain provisions. Compliance Risk may originate from, among other things, certain behaviors, namely the behavior or activities of the Company that deviate or violate the provisions and/or regulations and organizationl behavior, namely the behavior or activities of the Company that deviate or conflict with generally accepted standards.

Reputational Risk

Reputation Risk is a risk due to a decrease in the level of stakeholders' trust originating from negative perceptions of the Company. Reputation Risk can be sourced from the following various Bank activities:

- Events that have harmed the Company, such as the influence of the reputation of the owner of the Bank and related companies, the complexity of the Bank's products and business cooperation, negative news about the Company, violations of business ethics, and customer complaints.
- Other things that can cause Reputation Risk, for example weaknesses in governance, corporate culture, and business practices of the Company.

Efforts to Manage Risk

Bank BTN as a Company whose main focus is in the field of lending or housing finance, is that the asset system is dominated by Housing Loans (KPR) which are affected by changes in the external business climate such as inflation and the BI 7 Day Reverse Repo Rate. Efforts to minimize the impact of the system are conducted by risk management on a day-to-day risk management activities, based on the principles of Good Corporate Governance (GCG) to ensure all processes and mechanisms that occur in achieving the company's goals, prevent the company from irregularities and risks that may result in failure to achieve company goals, and based on the principle of prudence to ensure the growth of the Company's healthy and sustainable performance

PT Bank Tabungan Negara (Persero) Tbk is one of the Systemic Banks. As one of the efforts to prevent and deal with financial system crises, especially with regard to Systemic Bank problems, the Company must be able to determine a plan that will be conducted if it experiences financial stress that may jeopardize business sustainability. The plan was outlined in the form of a Action Plan (Recovery Plan) in accordance with POJK No. 14/POJK.03/2017 dated April 04, 2017 and internal regulations of Company SE No. 15/DIR/RMD/2018 dated March 22, 2018 concerning the Implementation of the Action Plan (Recovery Plan). The Company has prepared a Recovery Plan Document which contains Trigger Level (for the purpose of prevention, recovery and repair). For each system, the Recovery Options included in the Recovery Plan include: Capital Indicator, Liquidity, Profitability and Asset Quality.

Credit Risk Management

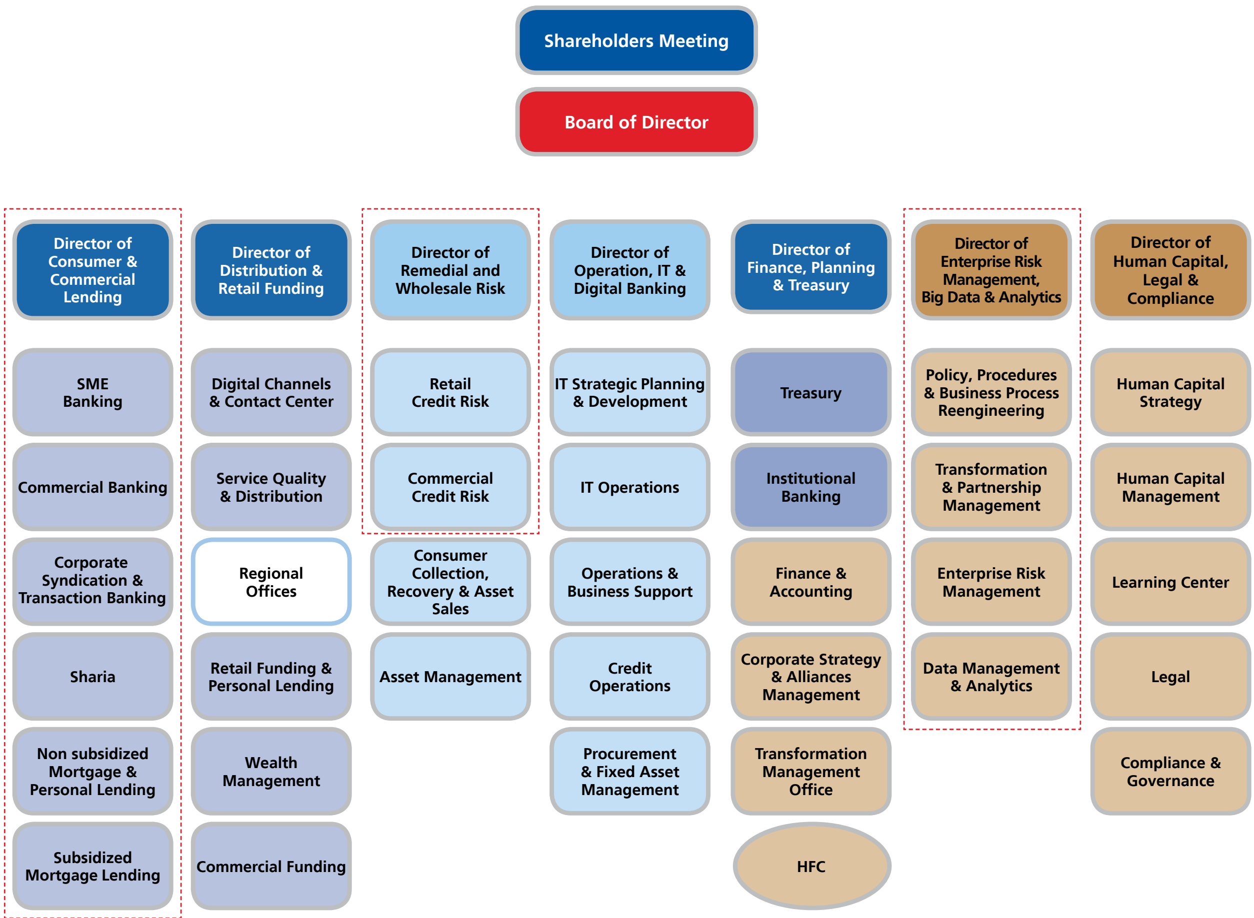
SAs part of credit risk management, the Company regularly reviews and updates Risk Management Policy Guidelines and Credit and Financing Policy Guidelines for the Company credit and financing as part of the risk assessment process. Credit risk exposures are monitored from the credit granting process to the credit maturity. Monitoring and controlling credit risk including evaluating credit risk exposure to credit risk limits (Risk Appetite & Risk Tolerance), the Company is conducting a pilot project on the implementation of the Internal Credit Rating (ICR) for commercial credit in analyzing in terms of credit risk in 3 (three) branch offices. In addition, a Monitoring Department in the Commercial Banking Division has been formed which specifically monitors the credit exposures of large debtors (50 core debtors) and has implemented Intelligence Credit Monitoring (iCremo), an application for commercial credit that functions to conduct commercial credit monitoring processes covering three pillars (Management, Business Prospects and Collateral). Whereas for consumer credit, the process of controlling credit risk is conducted through the Consumer iLoan system which is equipped with a Credit Scoring Model (CSM). The management of Kol-2 and NPL consumer credit debtors is conducted by the Consumer Collection and Remedial Work Unit while for commercial credit is conducted by the Commercial Asset Management Work Unit.

As a follow up to the application of Pillar 1 Basel II, the Bank has implemented credit risk measurement using the Standardized Approach in accordance with FSA Circular Letter No.42/SEOJK.03/2016 dated September 28, 2016 concerning Guidelines for Calculation of Risk Weighted Assets (ATMR) for Credit Risk using the Standard Approach.

In order to manage credit risk, the Company has implemented the Four Eyes Principle by separating credit risk functions from business units.

In commercial credit decisions consist of Commercial Risk and Business Units as the Risk Taking Unit and first line and consumer credit decisions consisting of the Retail Risk Division (Regional Loan Processing Center) and Branch Offices and Regional Offices.

This can also be illustrated by the Company's organization structure that has separated the credit risk and risk taking units and enterprise risk management functions:



Market Risk Management

As part of market risk management, the Company identifies, measures, monitors and controls market risk, which is conducted by the business unit and/or Enterprise Risk Management Division. One of the market risk identification is done for each product or activity that is included in the category of new products or activities. Related to market risk management, the Company has an Assets and Liabilities Committee (ALCO). In this regard, ALCO periodically discusses, among others, interest rates and market risk management at the Company, especially those originating from the banking book position.

In order to measure the interest rate risk in trading book and banking book positions, the Company conducted a sensitivity analysis aimed at measuring the impact of changes in market interest rates on the Company's profit (loss) and equity. Whereas in order to measure exchange rate risk, the Company conducted a sensitivity analysis aimed at measuring the impact of exchange rate changes on the Company's profit (loss). Specifically for the banking book position, the Bank measured interest rate risk in the banking book using the repricing gap method as stipulated in the Director's Circular Letter No.26/SE/DIR/RMD/2019 dated 19 June 2019 regarding Interest Rate Risk Management in the Banking Book. In accordance with Financial Services Authority Circular Letter Number 12/SEOJK.03/2018 dated August 21, 2018 concerning the Implementation of Risk Management and Risk Measurement of the Standard Approach to Interest Rate Risk in the Banking Book for Commercial Banks, the Bank submitted adjustments to policies related to IRRBB and IRRBB calculation reports in accordance with applicable regulations. In order to measure the interest rate risk in the banking book, the Bank developed an IRRBB policy and has developed an IRRBB measurement system/application. In order to complement market risk measurement with standard methods and sensitivity analysis, the Bank conducts stress testing to assess the Company's resilience in the face of extreme changes in interest rates and exchange rates, with the system referring to the regulatory provisions and the Company's internal system. For the Company's internal system, each year the Enterprise Risk Management Division coordinates with the Working Group Stress Test (related Division) to formulate the system and assumptions that will be used in the implementation of Market Risk Stress Tests for the next 1 (one) year.

Monitoring and controlling market risk includes evaluating market risk exposures to the Company's internal limits (Risk Appetite & Risk Tolerance) that have been set and reviewed periodically to be in line with the conditions of the Company. In addition, the Company has determined in order to control or limit exchange rate risk exposures, the Company has set limits that include treasury transaction limits, dealer limits, budget loss limits, stop loss/stop gain limits, and appropriate Net Open Position (NOP) limits with a maximum limit specified in PBI 17/5/PBI/2015 dated May 29, 2015 Bank Indonesia Regulation No.17/5/PBI/2015 dated May 29, 2015 concerning the Fourth Amendment to PBI Number 5/13/PBI/2003 concerning Foreign Exchange Position Net Commercial Bank.

As a follow up to the application of Pillar 2 Basel II, the Company has implemented market risk measurements using the Standardized Model in accordance with FSA Circular Letter No. 38/SEOJK.03/2016 dated September 15, 2016 concerning Guidelines for Using the Standard Method in Calculating the Minimum Capital Requirement for Commercial Banks by Calculating Market Risk. Portfolios taken into account in determining market risk capital CAR consist of a trading book portfolio for interest rate risk and a trading book and banking book portfolio for exchange rate risk.

Liquidity Risk Management

As a guideline in managing liquidity risk, the Company has a Liquidity Risk Management Policy Manual, which is part of the Company's Risk Management Policy Guidelines (PKMR). The Liquidity Risk Management Policy Manual regulates, among others, active supervision of the Board of Commissioners and Directors in the application of liquidity risk management, liquidity risk management processes, and policies, procedures and determination of liquidity risk limits. The Company has an Assets and Liabilities Committee (ALCO) that functions to manage liquidity and periodically discuss the management of liquidity risk at the Bank.

Referring to the Liquidity Risk Management Policy Guidelines, the Company identifies, measures, monitors and controls liquidity risk. Liquidity risk identification is basically intended to find out the amount and trend of liquidity needs as well as funding sources available to meet the needs.

The liquidity risk measurement in the Company is conducted by the Treasury Division (TRSD) and the Enterprise Risk Management Division (ERMD). Liquidity risk measurement uses 4 (four) methods, namely stockbased, maturity profile analysis, cash flow projections and stress testing. The stockbased method is used to measure liquidity risk at the Company using liquidity ratios, the maturity profile analysis method is used to measure liquidity gaps and cash flow projections are used to measure the amount and trend of liquidity requirements. The Company conducts stress testing using Bank Specific Crisis (BSC) scenarios and General Market Crisis (GMC) stress tests, which aim to measure the adequacy of available liquid assets and the Company's ability to meet liquidity needs in crisis conditions. The Enterprise Risk Management Division coordinates with the Stress Test Working Group (related

Division) to formulate the impact of risks on scenarios and assumptions that will be used in the implementation of Stress Tests for Liquidity Risk for the next 1 (one) year.

In order to maintain the availability and adequacy of liquid assets and control or limit exposures to avoid being affected by liquidity risk, the Company regularly monitors liquidity risk both daily, weekly, monthly and quarterly. ERMD liquidity risk monitoring submitted to the Board of Directors and strategy evaluation submitted to the relevant Division.

Monitoring and controlling liquidity risk includes evaluating liquidity risk exposures to the Company's internal limits (Risk Appetite & Risk Tolerance) and predetermined Recovery Plan levels. The limit is reviewed periodically to be in line with the conditions of the Company. In addition, the Company monitors the Early Warning Indicator (EWI) and is reported regularly to the Directors and related Work Units.

In accordance with FSA Regulation No. 14/POJK.03/2017 dated April 04, 2017 concerning the Action Plan (Recovery Plan) for Systemic Banks, the Company has been monitoring the liquidity system, one of which is seen from the LCR and NSFR ratios according to FSA Regulation No. 42/POJK.03/2015 dated December 23, 2015 concerning the Obligation to Meet the Liquidity Coverage Ratio (LCR) for Commercial Banks and FSA Regulation No. 50/POJK.03/2017 dated July 13, 2017 concerning the Obligation to Fulfill Net Stable Funding Ratio.

Operational Risk Management

In order to implement the risk management process, especially operational risk, the Company has an BTN Loss Event Database (BTN-LED) application that functions as an operational risk data collection for operational risk events at the branch office using the risk event criteria based on Basel II (7 risk event types). The BTN LED application is connected to the Branch Office so that in its reporting, the Branch Office can send data loss events online through web-based media every month. The output of this BTN LED is data accumulation of Company losses in one month in the form of actual loss, near miss and potential loss from each risk event, then the data will be converted into Top 10 risk. The results of the collected data will be processed and analyzed so that it can be known the operational risk exposure map of each Branch and Regional Office. This exposure map serves as a reference in preventing similar incidents by taking steps to improve existing business processes or by adding other forms of risk mitigation.

The Company also has a Risk and Control Self-Assessment (RCSA System) application that is used to conduct the process of identifying and measuring operational risks inherent in all work units of the Company. The approach used in the RCSA application is ISO 31000: 2009. Risk can be defined as the impact of uncertainty on achieving targets. Therefore, in filling out RCSA all work units are required to be able to identify and measure operational risks inherent in daily activities and have an impact on achieving the goals of the work unit.

To ensure the sustainability of the Company's operations in conducting business after being affected by operational risks originating from external factors such as natural disasters, social conflicts and IT system failures, the Company has implemented a Business Continuity Management (BCM) policy. The BCM policy contains systematic steps and guides employees in dealing with emergencies starting from pre-disaster preparedness, response to disasters, operational continuity plans, up to returning to normal conditions. In supporting the successful implementation of BCM, the Company conducts an internalization process for all employees by compiling video dissemination materials and conducting periodic trials or simulations. Reports on the results of trials or simulations will serve as benchmarks of success and serve as material for sustainable improvement.

Legal Risk Management

Legal Risk identification is conducted on the causes of risk, including legal claims and weaknesses in the legal aspects inherent in functional credit activities (provision of funds), treasury and investment, operations and services, information technology systems and MIS, and human capital management.

Legal Risk Measurement is conducted by the Enterprise Risk Management Division (ERMD), Legal Division (LGD) and Credit Operation Division (COD). From the measurements made by LGD, it was obtained an evaluation report on the analysis of individual legal cases for contingent liabilities arising from lawsuits that occurred, while from COD obtained the quality of credit document engagement (LAT).

Measurements are conducted based on reports on the results of analysis and evaluation of individual legal cases for contingent liabilities arising from lawsuits that occur as well as quality reports on loan document agreements. Indicators/parameters used in measuring Legal Risk include but are not limited to potential losses due to lawsuits, weaknesses in agreements due to non-fulfillment of conditions for legal agreements and changes in laws and regulations that cause the Company's products to be inconsistent with existing provisions.

Legal Risk Monitoring is conducted by ERMD by evaluating the effectiveness of the implementation of policies, procedures and compliance with specific policies, regulations and Bank limits. Monitoring is conducted regularly for all Legal Risk positions. In conducting legal risk control, LGD provides input and recommendations to each division and work unit and conducts periodic reviews of agreements and cooperation contracts with counterparties. In addition, the Company has a Legal Application System (LApS) that is designed in the form of a website and is used as a register and monitoring of cases that occur or are handled by the Company, both Criminal and Non-Criminal, so that every case that occurs both at the Branch and at the Head Office, the progress can be monitored.

The Company has placed employees in Regional Offices as Branch Legal Representative (BLR) with duties and responsibilities including:

1. Providing legal assistance to litigation issues submitted by each work unit in the context of implementing Bank operations and providing legal assistance in every legal case.
2. Representing the Bank in conducting court proceedings in the Court, Police, Attorney General's Office, other legal institutions, and outside the court in its working area.
3. Providing legal opinion on legal issues raised by Regional Offices, Branch Offices, and Sharia Branch Offices related to operations in their working area.
4. Providing legal consultation on legal issues raised by Sharia Branch Offices and Branch Offices.
5. Performing the legal watch function in accordance with Bank Indonesia regulations.
6. Managing and controlling legal risks that are within the scope of work.

Strategic Risk Management

Strategic Risk identification is based on Strategic Risk factors in certain functional activities, such as credit, treasury and investment activities as well as operations and services through a business plan prepared by the Corporate Strategy & Alliance Management Division (CSAD) as a translation of the General Policy of the Directors (KUD).

Strategic Risk Measurement was based on the bank's performance achievement by comparing actual results with the predetermined target. Strategic Risk Monitoring was carried out by the Corporate Strategy & Planning Division (CSPD) periodically by monitoring the achievement of Key Performance Indicator (KPI) and Enterprise Risk Management Division (ERMD) that monitored risk exposure compared to the Bank's risk appetite and monitoring of Risk Appetite and Strategic Risk Tolerance on a monthly basis. Furthermore, the Board of Commissioners, Board of Directors and Division reviewed the basic strategy with a focus on business transformation, infrastructure and human resources and conducted a review of risk appetite and risk tolerance periodically and at least once a year.

Furthermore, the Enterprise Risk Management Division monitors Strategic Risk by comparing targeted results with expected results, evaluating the performance of work units and ensuring the achievement of targets (target objectives).

In controlling Strategic Risk, the Corporate Strategy & Alliance Management Division (CSAD) functions to analyze gaps between system reports and business plan targets and convey the steps that must be taken to the Board of Directors periodically.

Compliance Risk Management

The Company has an internal application, namely the Compliance Regulatory & Monitoring System (CRMS) to facilitate all the Company employees in accessing all of the Company's internal requirements. In addition, to minimize the potential for compliance risk, the Company has a Compliance Work Unit called Compliance and Governance Division (CMGD) which monitors compliance risk by making a list of the Company's obligations to external parties and periodically reviewing internal regulations so that they remain relevant to external provisions in force.

The Company has placed a Regional Compliance Supervisory Officer (RCSO) at the Regioal Office Branch Compliance Supervisory Officer (BCSO) at the Branch Office to evaluate the level of compliance with the Company's transaction flows and nontransaction operations whether they are in accordance with applicable regulations, provisions or SOPs. CMGD monitors and reports compliance risks that occur to the Company's Board of Directors both at any time and periodically when Compliance Risk occurs.

Compliance Risk measurement is conducted on potential losses caused by non-compliance and the Company's inability to meet the applicable external provisions. Indicators/parameters used in measuring Compliance Risk include types, significance, and frequency of violations of applicable regulations or track records of bank compliance, behavior underlying violations, and violations of generally accepted standards.

In controlling Compliance Risk, ERMD and CMGD have the duty to evaluate the effectiveness of the implementation of Compliance Risk management by regularly monitoring all types of activities that have the potential to cause Compliance Risk.

Ruputation Risk Management

All employees, including business unit management and the Company supporting activities, are part of the Risk Management implementation structure for Reputation Risk, bearing in mind that reputation is the result of all of the Company's business activities. The role of the Business

Unit Management is to identify the Reputation Risk that occurs in the business or activity of the unit and as a front liner in developing and preventing Reputation Risk, specifically related to customer relationships. Reputation Risk identification is conducted on risk factors inherent in certain functional activities such as credit (provision of funds), fund raising, treasury and investment, operations and services, information technology systems and MIS, and HC.

In the process of identifying reputation risk, the Company has a SPN (Customer Complaints System) application and monitors all mass media (print and electronic, both local and national). The Company records every report about the Company both directly (straightnews) and indirectly (mention). The SPN application is integrated with Branch Offices and Contact Centers. Service Quality & Network Division (SQND) as the manager of SPN will follow up on customer complaints and resolve in accordance with the SLA that has been set.

The Reputation Risk Measurement is conducted based on the results of an assessment of the factors affecting the Company's reputation, including customer complaints and reporting about the Company. The Company 's Reputation Risk is managed by the Corporate Secretary Division (CSD) work unit that manages news about the Company which is published in the print and electronic mass media and the Operational & Business Support Division (OBSD) which manages customer complaints.

In order to monitor Reputation Risk and ensure customer satisfaction is maintained, the Company 's SPN (Customer Complaints System) functions to support the management of services and online customer complaint handling between parties related to problems in Branch Offices and Headquarters. In addition, Reputation Risk monitoring is also conducted by the Enterprise Risk Management Division (ERMD) by reminding and providing recommendations for improvement to the Reputation Risk Management Division of CSD and OBSD based on an assessment of reputation risk profile parameters.

In controlling Reputation Risk, the Corporate Secretary Division is responsible for implementing policies relating to handling and resolving negative news or avoiding counter-productive information. To control Reputation Risk related to customer complaints, OBSD follows up on customer complaints and resolves them in accordance with established SLAs.

Risk Management Refinement and Enhancement

As a Company that focuses primarily on lending and housing finance, the Company's asset portfolio is dominated by Housing Loans (KPR) plus the Company has dominantly assisted the government in Sejuta Rumah (Million Houses) Program, in the context of refining and improving the Risk Management, one of the ways that conducted is to improve the culture of risk management, the risk management work unit initiated a strategy to increase the risk awareness of all employees of the Company, among others by using the methods:

1. **Risk Management in Training**
   Training related to overview and application of risk management which includes mandatory material on risk culture, including GBS and ODP training by implementing Gamification, using Fun Risk Quiz Kahoot and Board Game Risk. The Enterprise Risk Management Division is also actively supporting the Learning Center for the Risk Management Competency Test (UKMR) of the Company employees in stages. ESDM employees who have UKM competence provide training to employees who will undergo the UKMR Certification Test facilitated by LSPP.

   For Millennials, ERMD also actively participates in the Kulgram (Telegram Lecture) to explain risk management, especially the Company's Soundness.

2. **Risk Awareness Blasting**
   Aiming to give messages to all employees to be aware of risks (email blasts and SMS blasts), in collaboration with CMPD, HMCD and IAD. During 2020 ERMD has spread Risk Awareness.

Risk Management Due to the Covid-19 Pandemic

The Covid-19 pandemic that had been occurring since early 2020 in Indonesia had greatly impacted the business sector and operational activities of the Company and could endanger the health of employees if infected with the virus. Therefore, there needed to be an anticipation in changing lifestyle and working patterns in every layer of society, especially the Company. The Company through the BCM (Business Continuity Management) Team had made a policy during this pandemic so that this new habit was carried out consistently and even became a work culture. In addition, policies were made as risk management, Covid impact management, and efforts to prevent the spread of the virus. Various actions taken by the Company including:

1. **Implementation of Health Protocols in the work**
In an effort to reduce the spread of the Covid-19 virus and provide security guarantees for employees in the work, all Company Work Units were obliged to implement Health protocols in the work area. 3M activities become minimal activities that should be employed as new lifestyle habits by all employees. Installation of health protocol support facilities had been done in each Work Unit, such as handwashing places, acrylic barriers, thermometer guns, etc. The use of room capacity was also reduced and meetings were directly restricted and replaced with meetings through online media as the application of social distancing.

2. **Covid Ranger Team Formation**
Covid Ranger was a mobilization team consisting of representatives from each Work Unit and responsible for monitoring, ensuring, and improving the effectiveness of the implementation of new habits in its Work Unit. Some of the responsibilities of Covid Ranger in handling Covid-19 including:
   a. Ensuring the implementation of Health Protocols in Work Units
   The Ministry of SOEs had established a standard Health Protocol that had to be implemented in all Work Units of State-Owned Enterprises including the Company. Therefore, Covid Ranger was responsible for ensuring that its work units had implemented health protocols in their work, so that it was expected to reduce the spread of the Covid-19 virus in the work area. Covid Ranger reported the implementation of this Health Protocol to COSMIC which was the official website of SOEs that monitored the implementation of Health Protocols in all state-owned companies centrally.
   b. Socialization of Health Protocols and Social Media Campaign
   Covid Ranger actively provided socialization on the importance of the application of Health Protocols to employees in its Work Unit so that the habit was carried out consistently and became a work culture.
   c. Monitoring of affected employees
   If there were employees in the Work Unit who were affected, Covid Ranger could coordinate with HMCD to handle positive cases of these employees. This was so that the positive case in the Company could be recorded properly and the affected employees got health treatment immediately.

3. **WFH Implementation Policy**
The Company maximized the implementation of WFH to reduce the risk of employees being exposed to Covid-19 by facilitating employees to work at home and maintain their productivity. The implementation of WFH was adjusted to the government's appeal and the level of criticality of the Work Unit, so as not to interfere with the operation of the relevant Work Unit.

4. **Provision of Health Facilities related to Covid-19**
   a. Rapid Antigen Test and PCR Swab Test
   In order to trace positive cases occurring in the work environment and as an effort to reduce the risk of the spread of Covid-19, Employees of the Work Unit who were in close contact with affected employees were given rapid antigen test and PCR swab test facilities. In addition, employees who fell into the category of exposure-prone, such as front liners and employees of public transportation users, were facilitated with regular tests.
   b. Provision of Safe House and cooperation with Hospitals
   The Company had cooperated with hospitals in handling affected employees who needed health care. In addition, the Company also had a Safe House facility that could be used as a place of self-isolation for affected employees if they did not get isolation rooms in the hospital. This was so that the handling of affected employees could be given quickly so that the employee's positive case could be handled properly.

Risk Assessment

Enterprise Risk Management Division as a Risk Management Task Force routinely conducted quarterly evaluation of the implementation of the effectiveness of risk management system by using risk profile tools including risk management for credit risk, market risk, liquidity risk, operational risk, compliance risk, legal risk, reputational risk and strategic risk. As stipulated in POJK No. 18/POJK.03/2016 on The Implementation of Risk Management for Commercial Banks and SEOJK No. 34/SEOJK.03/2016 on The Implementation of Risk Management for Commercial Banks, the risk profile report included an assessment of Inherent Risk and an assessment of the Quality of Company Risk Management Implementation.

Inherent Risk Assessment was an assessment of the risks inherent in the the Company's business activities, whether quantified or not, potentially affecting the the Company's financial position. Quality Assessment of Risk Management Implementation was an assessment of 4 (four) interconnected aspects including risk governance, risk management framework, risk management process, human resources adequacy, and management information system adequacy, as well risk control system adequacy.

Evaluation of Risk Management Implementation

The Board of Commissioners and Board of Directors had an obligation to supervise risk management activities carried out by the Company and conducted periodic assessments and evaluations of the risk management controls effectiveness and provided recommendations if deemed necessary. The implementation of a comprehensive risk management system enabled the Company to effectively manage risks so that it could take into account risk portfolios, minimized and took preventive measures and maximize profit achievement.

One form of evaluation on risk management policy was the annual evaluation of Risk Management Policy and Procedure Standards. The Board of Commissioners played an active role in the implementation of risk management system evaluation through the Risk Monitoring Committee by reviewing the evaluation results that had been conducted by the Board of Directors assisted by the Risk Management Committee as the organ responsible for the effectiveness of the implementation of the risk management system. The results of the annual evaluation showed that risk management at the Company during 2020 was adequate.

Internal Control System

The implementation of the internal control system was implemented in order to support the achievement of the Company's performance goals, increase value for stakeholders, minimize the risk of losses and maintain compliance with applicable laws and regulations. The Company implemented an internal control system as an important supervisory component in the management of the Company and became a reference for healthy and controlled operational activities. The Company referred to the COSO (Committee of the Sponsoring Organizations of the Treadway Commission) - Internal Control Integrated Framework in establishing an internal control framework to ensure adequacy of operational and financial controls, financial reporting, operational effectiveness and efficiency, as well as compliance with applicable laws and regulations

Basic Stipulation

For the Company, the Internal Control System is a monitoring mechanism established by management on an ongoing basis. The Company operates an internal control system with reference to the applicable regulations, including the following:

1. Financial Services Authority Regulation No. 18/POJK.03/2016 dated March 16, 2016 concerning the Implementation of Risk Management for Commercial Banks.
2. Financial Services Authority Circular No. 34/SEOJK.03/2016 dated September 01, 2016 concerning the Implementation of Risk Management for Commercial Banks.
3. Financial Services Authority Circular No. 35/SEOJK.03/2017 concerning Guidelines for Internal Control Standards for Commercial Banks.
4. Bank Indonesia Circular Letter No 5/22/DPNP dated September 29, 2003 concerning Guidelines for Internal Control System Standards for Commercial Banks.

Financial and Operational Control Activities

Control activities include several aspects which are not limited to the establishment of control policies and procedures as well as verification processes to ensure that the policies and procedures are consistently adhered to. Control activities especially related to operations and finance are applied at all functional levels whose responsibilities are adjusted based on the Company's organization structure including:

1. Management Review (Top Level Reviews)
   The Directors periodically conduct coordination meetings to obtain information on the Company's performance from officials and employees. So it is possible to conduct a study of the realization compared to the targets that have been set, such as financial reports or management reports that are compared with the specified budget plan. Based on the review, the Directors immediately detected problems such as control weaknesses, financial reporting errors or othe irregularities (fraud).
2. Operation Performance Review (Functional Review)
   This review is conducted by the Internal Audit Division on a monthly, quarterly, semester and annual basis, including:
   a. Reviewing the risk assessment (risk profile report) produced by the risk management work unit.
   b. Analyzing operational data, both data related to risk and financial data, namely verifying the details and transaction activities compared to the outputs (reports) produced by the risk management work unit.
   c. Reviewing the realization of the work plan and budget implementation, in order to.
      1) Identifying the cause of significant deviations.
      2) Establishing requirements for corrective action.
3. Control of Information Systems and Technology
   Control of information systems and technology is done by verifying the accuracy and completeness of the transaction and conducting authorization procedures, in accordance with internal regulations. Information system control activities can be classified into two criteria as follows:

   a. General control includes general control over data center operations, software procurement and maintenance systems, security of access, and development and maintenance of existing application systems. This general control is applied to mainframes, servers, and users workstations, as well as internal-external networks.
   b. Application controls are applied to the programs used by the Company in processing transactions and to ensure that all transactions are true, accurate and properly authorized. In addition, application control must be able to ensure the availability of an effective audit process and to check its accuracy.
4. Physical Control
   Control of physical assets is conducted to ensure the implementation of physical security of the Company's assets. These activities include safeguarding assets, records and limited access to computer programs and data files, as well as comparing the value of the Company's assets and liabilities with the values listed in the controlling records, in particular checking asset values periodically.
5. Documentation
   The Company at least formalizes and documents the policies, procedures, systems and accounting standards and audit processes adequately. The document must be updated regularly to describe the actual operational activities of the Company, and be informed to officials and employees. Upon request, documents must always be available for the benefit of internal auditors, public accountants and the Company's supervisory authority. The accuracy and availability of documents must be assessed by internal auditors when conducting routine and non-routine audits.
6. Segregation of Duties
   Segragation of Duties is a part of control activities intended to ensure that everyone in his position does not have the opportunity to make and hide errors or irregularities in conducting his duties at all levels of the organization and all steps of operational activities, as follows:
   a. Complying with the principle of this function segregation, known as "Dual Control";
   b. Establishing procedures (authority), including the determination of a list of officers who may access a transaction or business activity that is high risk;
   c. Avoiding giving authority and responsibility that may lead to various conflicts of interest. All aspects that may cause conflicting interests are identified, minimized and monitored carefully by other independent parties;
   d. The implementation of the Four-Eyes Principle and the Three Pillars Process namely Business, Operations and Risk are as follows:
      1) The Four-Eyes Principle is the main principle that underlies decision-making in granting credit where each loan is made by at least 2 (two) authorities, each from the Business unit and the Credit Risk unit, which are mutually independent of each other.
      2) Decision making for the type of credits that uses a scoring system or special criteria specified in the program/skim parameters is basically the implementation of the four-eyes principle, which is between the business unit and the socring system/criteria where the model design and scoring system parameters/criteria are arranged and maintained by the risk management unit.
      3) Segregation of sales/business functions, risk functions and operations functions (credit admin and legal) in the credit granting process.

Its Compatibility with the Committee of Sponsoring Organizations of the Treadway Commission (COSO)

The Company's Internal Control System is in accordance with the Integrated Internal Control Framework developed by the Committee of the Sponsoring Organization of the Treadway Commission (COSO). The objectives of Internal Control according to COSO include Operational objectives, Reporting objectives and Compliance objectives.

In COSO it is stated that Internal Control is a system or process performed by the Board of Commissioners, Board of Directors, Management and employees in a company, to provide adequate guarantees to achieve the Control objectives. COSO – the Internal Control Framework, consists of 5 (five) Control components, which are Environment Control, Risk Assessment, Activities Control, Information and Communication Control, and Monitoring Control.

The implementation of the Company's Internal Control System that refers to COSO has been adapted to the Company's Board of Commissioners and Board of Directors Joint Decree No. SKB-04 dated July 29, 2011 concerning the Guidelines for the Internal Control System and KD No. 01/DIR/KD/PPD/2018 dated January 23, 2018 concerning Guidelines for Corporate Governance Policy (PKTKP) Chapter 7 Internal Control Policies. Based on the decree, the Company's Internal Control component is in line with the COSO Internal Control Framework which includes the following:

1. Environment Control, which is a fundamental component in the Internal Control System. The component reflects the nuances and atmosphere of concern regarding all levels of officials and leaders

pertaining to the importance of effective Internal Controls. This Environment Control is strongly influenced by a Strong Tone from the Top.
2. Risk Assessment, which is a series of Risk Awareness initiatives for all employees towards the development of a Risk Culture and the activities of evaluating, rating and mitigating risks.
3. Activities Control, which includes the adequacy of policies, provisions, procedures and compliance in the implementation of Operational activities.
4. Information and Communication Control, which pertains to the condition of effective communication channels both internally and externally in accordance with their respective responsibilities.
5. Monitoring Control, which is an assessment process for monitoring the effectiveness of the design and operation of the Internal Control Structure and performance of the Management, whether it has been conducted properly and has made adjustments that are in accordance with the prevailing circumstances.

While elements of the Bank's Internal Control System as mentioned in the Joint Decree No. SKB-04 No. SKB04 dated July 29, 2011 and KD No. 01/DIR/KD/PPD/2018 dated January 23, 2018 concerning Guidelines for Corporate Governance Policy (PKTKP) Chapter 7 Internal Control Policies include the following matters:

1. Supervision by Management and the Culture of Control where the Board of Commissioners are responsible for ensuring that the Board of Directors have monitored the effectiveness of the Internal Control System, in order for the Board of Commissioners to ensure that improvements concerning the Company's problems will be enhanced due to the effectiveness of the Internal Control System. The Board of Directors is responsible for establishing Internal Control policies, strategies and procedures. The Board of Directors is also responsible for monitoring the adequacy and effectiveness of the Internal Control System. The Board of Commissioners and the Board of Directorsare responsible for improving and developing an Organizational Culture that promotes and emphasizes good Work Ethics and High Levels of Integrity, to all of the Bank's employees regarding the importance of Internal Controls that apply in the Company.
2. Risk Identification and Assessment is a series of actions performed by the Board of Directors in Identifying, Analyzing and Assessing the Risks confronted by the Company in order to achieve the business objectives.
3. Control and Segregration Activities regarding Operational Functions where Activities Control will assist the Company's Board of Directors and Board of Commissioners in managing and controlling risks that may cause harm on performance or result in losses to the Company. Activities Control includes policies, procedures and practices that provide confidence for the officials and employees of the Company that the direction of the Board of Commissioners and the Board of Directors of the Company have been implemented effectively. The separation of functions is intended that all personnel in their positions do not have the opportunity to perform and conceal errors or irregularities in performing their duties across all levels of the organization and at all phases of Operational activities.
4. Accounting/Financial, Information Technology and Communication Systems where the Accounting/ Financial System must include methods and records in identifying, grouping, analyzing, classifying, recording/ registering and reporting the Company's transactions. The Information Technology System must be able to produce reports regarding Business Activities, Financial conditions, the implementation of Risk Management and Compliance with the provisions that support the implementation of the duties of the Board of Commissioners and the Board of Directors. The Communication System must be able to provide information to all parties, both internal and external, including the the Company's Supervisory Authorities, External Auditors, Shareholders and Customers of the Company.
5. Monitoring Activities and Actions regarding the Correction of Deviations where the Company must continuously monitor the effectiveness of the overall implementation of Internal Control. Monitoring of the Company's main risks must be prioritized and function as an integral part of the Company's daily activities including periodic evaluations, both by the Operational Work Unit and by the Internal Audit Work Unit.

Internal Control System Implementation Evaluation

In 2020, the Company implemented Internal Controls in accordance with the principles of Control, and overall, a good quality Internal Control System. The Company, through the Internal Audit Division (IAD), conducted Internal Control Assessment (ICA) in evaluating the effectiveness of the Internal Control System. The assessment measured the Internal Control quality of the Auditee Work Unit for the 5 (five) Internal Control components of the COSO Framework using the rating criteria and methodology of the Internal Control Assessment (ICA) questionnaire and the Auditor's professional judgment through an in the field walkthrough.

Broadly speaking, the steps taken by the Company in ensuring the implementation of effective monitoring activities include the following:

1. To ensure that the Monitoring function is clearly defined and well-structured within the Company's organization.
2. To establish Work Units/employees who are assigned to monitor the effectiveness of the Internal Controls.
3. To establish the right frequency for monitoring activities based on Inherent Risks in the Company and the nature/ frequency of changes occurring in Operational activities.
4. To integrate Internal Control System into all Operational activities and provide routine reports including Book-keeping Journals, Management Reviews and Reports regarding the approvals for exceptions/deviations from established policies and procedures (justifications for irregularities) which are then reviewed.
5. To conduct reviews of the documentation and results of the evaluation of the Work Unit/ employee assigned to perform the monitoring function.
6. To establish information/feedback in the correct format and frequency level.

To assess the adequacy and effectiveness of the Internal Control System and Performance Quality being implemented is as follows:

1. Adequacy and Effectiveness of Internal Control employs the Internal Control Assessment (ICA) questionnaire to create a Risk Control Assessment and Audit Rating, which are retested during the implementation of a Field Audit (walkthrough).
2. Performance is assessed based on the achievement of real performance targets with the performance set forth in the Company's Work Budget Plan (RKAP).

Evaluation of the effectiveness of the Company's Internal Control System (Risk Control) was implemented on all Work Units based in the Headquarters (division/ desk/ Regional Office) as well as Branch Offices and Sharia Branch Offices. All that was related to the issue of the adequacy of Internal Control was reported directly to the Board Directors through the President Director and to the Board of Commissioners via the Audit Committee. Follow-up efforts were conducted in order to minimize risks and overcome problems that had arisen.

Internal Control Statement of Adequancy

The Board of Directors and the Board of Commissioners are committed to ensuring that Good Corporate Governance rests as the basis for achieving our goals, safeguarding, and enhancing the value of the Company. One of the implementations of Good Corporate Governance is ensuring that the Internal Control System has been implemented adequately.

The Board of Directors and the Board of Commissioners or the Audit Committee conducts an examination of the evaluation results concerning the effectiveness of the Company's Internal Control System, which includes five main components of Control, they are Environment Control including the Supervision by Management and Culture of Control (Oversight and Culture of Control Management), Risk Recognition and Assessment, Control and Separation of Activities (Activities Control and Segregation of Duties), Information Technology and Accounting and Communication Systems (Accountancy, Information and Communication), Monitoring Activities and any Deviations/ Weakness Correction Actions (Monitoring Activities and Correction of Deficiencies).

This Internal Control System Standard Guide is a guideline that contains the Internal Control System's minimum measure, which must be enforced by the Company in all aspects of Operations and implementation within the Company, to nurture a common understanding and foundation for the maintenance and commitment of all parties related to the Company.