GENERAL POLICY
REGARDING
RISK MANAGEMENT

PT BANK TABUNGAN NEGARA (Persero) Tbk
2022

GENERAL POLICY
REGARDING
RISK MANAGEMENT

2022

LIST OF CONTENTS

PT Bank Tabungan Negara (Persero) Tbk
Kantor Pusat
Menara Bank BTN
Jl. Gajah Mada No. 1, Jakarta Pusat 10130 Indonesia

T +62 21 633 6789, 633 2666
E csd@btn.co.id
www.btn.co.id
NPWP: 01.001.609.5-093.000

A. BACKGROUND

Banking is a financial institution that is regulated in a structured and comprehensive manner by the Regulator in carrying out its activities. This is aimed at protecting the national economy from systemic risks that can arise in connection with the role of banking intermediation. Risk Management is a series of methodologies and procedures for identifying, measuring, monitoring and controlling risks so that the business activities carried out do not cause losses that exceed capabilities or that can disrupt the continuity of the Bank's business.

The objectives of implementing effective Risk Management include:

1. Increase shareholder value.
2. Provide an overview to Bank management regarding the Bank's possible losses in the future.
3. Improve systematic decision-making methods and processes based on the availability of information.
4. Used as a basis for more accurate measurement of Bank performance and Health Level.
5. Assess the risks inherent in the Bank's relatively complex instruments or business activities and create a strong Risk Management infrastructure in order to increase the Bank's competitiveness.

The change in the Risk Management Policy Guidelines (*Pedoman Kebijakan Manajemen Risiko* - PKMR) to the General Policy of Risk Management Policy (*Kebijakan Umum Manajemen Risiko* - KUMR) was motivated by several things, namely alignment with the Bank's general policy structure, confirmation of the principles of implementing Risk Management based on company strategy which are implemented into the overall Risk Management implementation process, implementation which is based on the goal of creating a good Bank Health Level and in order to strengthen the implementation of Risk Management to realize the Bank's Vision "*To Become the Best Mortgage Bank in Southeast Asia by 2025*".

Therefore, the Bank has prepared a General Policy of Risk Management Policy as a guideline in applying Risk Management principles to business and operational activities for all levels of the organization. This General Policy of Risk Management Policy has been prepared referring to the Bank's new policy structure as well as provisions issued by the competent authority (Regulator) in the Banking sector which applies and explains the scope and process of Risk Management at the Bank.

B. AIMS AND OBJECTIVES

1. Aims
   1.1. Provide basic guidelines in implementing Risk Management in accordance with applicable regulations;
   1.2. Provide guidance to clarify the authority and responsibilities of all relevant parties in implementing Risk Management;
   1.3. Provide guidance in implementing Risk Management principles;
   1.4. Provide guidance in writing Special Policies and Technical Instructions for Risk Management in detail; and
   1.5. Become the basis for written guidelines for all levels of the organization in implementing risk management based on prudential principles and sound banking practices.
2. Objectives
   2.1. Maintaining the level of risk in accordance with the level of Risk to be taken (risk appetite) and risk tolerance that has been determined by the Board of Directors;
   2.2. Developing a Risk culture in every person at all levels of the organization;
   2.3. Maintain minimum capital adequacy adjusted to the characteristics, complexity and risk profile; and
   2.4. Ensure that the implementation of Risk Management is in accordance with the principles, values and directions set by the Bank and Regulators.

To achieve this goal, each work unit is required to implement Risk Management as regulated in this regulation.

C. SCOPE OF THE GUIDELINES

The scope of this policy includes:

1. Implementation of Risk Management including provisions for formulating Risk Management policies in the form of Special Policies and Technical Instructions;
2. Risk Management Organization in general includes the insight and implementation of the authority and responsibilities of the Board of Commissioners and the Board of Directors, determining work units responsible for implementing Risk Management, affirming the function of the three lines of defense, as well as implementing a Risk culture in every line of the Bank's organization;
3. Reporting on the implementation of Risk Management both internally and externally; and
4. General Policy of Risk Management Policy must be reviewed at least 1 (one) time every 1 (one) year. The results of the review must be reported to the Board of Directors and Board of Commissioners. The KUMR review process must be documented and administered in an orderly manner.

A. TYPES OF RISK

Risk Management is a series of methodologies and procedures that include the process of identifying, measuring, monitoring, controlling, and managing risks, originating from all Bank business activities, both from business activities and Bank products.

The Bank has two groups of Risk types which can be grouped according to the Bank's business with the following Risk types:

1. Types of Bank Risk as a Commercial Bank:

    1.1. Credit Risk

    Risks resulting from failure of other parties to fulfill obligations to the Bank, including Credit Risk due to debtor failure, credit concentration risk, counterparty credit risk, and settlement risk.

    Credit concentration risk is a risk that arises as a result of concentrated provision of funds to 1 (one) party or group of parties, industry, sector and/or certain geographic areas which has the potential to cause large losses that can threaten the continuity of the Bank's business.

    Counterparty credit risk is a risk that arises due to the failure of a counterparty to fulfill its obligations and arises from types of transactions that have certain characteristics, for example transactions that are influenced by movements in fair value or market value.

    Settlement risk is a risk arising from failure to deliver cash and/or financial instruments on the agreed settlement date of sales and/or purchase transactions of financial instruments.

    1.2. Market Risk

    Market Risk is the Risk on the balance sheet and administrative account positions including derivative transactions, due to overall changes in market conditions, including the Risk of changes in option prices.

    Market Risk includes, among others, interest rate risk, exchange rate risk, commodity risk and equity risk. “Interest rate risk” is the risk resulting from changes in the price of financial instruments from trading book positions or due to changes in the economic value of banking book positions, which are caused by changes in interest rates. The interest rate risk category also includes interest rate risk from banking book positions, which includes, among other things, repricing risk, yield curve risk, basis risk and optionality risk.

"Exchange rate risk" is the risk resulting from changes in the value of trading book and banking book positions caused by changes in foreign exchange rates or changes in gold prices.
"Commodity risk" is the risk resulting from changes in financial instrument prices from trading book and banking book positions caused by changes in commodity prices.
"Equity risk" is the risk resulting from changes in the price of financial instruments from trading book positions caused by changes in share prices.

1.3. Liquidity Risk

Liquidity Risk is the risk resulting from the Bank's inability to meet maturing obligations from cash flow funding sources and/or from high quality liquid assets that can be collateralized without disrupting the Bank's activities and financial condition.
In its implementation, liquidity risk management at the Bank includes but is not limited to the implementation of Liquidity Coverage Ratio (LCR), Net Stable Funding Ratio (NSFR) and other liquidity parameters in accordance with Regulatory provisions.

1.4. Operational Risk

Operational Risk is the risk resulting from inadequacy and/or non-functioning of internal processes, human error, system failure, and/or external events that can affect the Bank's operations.
In its implementation, operational Risk Management at the Bank includes but is not limited to the implementation of Operations Risk Controller, the implementation of Business Continuity Management and IT, Cyber and Digital Risk.

1.5. Legal Risk

Legal Risk is the risk resulting from lawsuits and/or weaknesses in juridical aspects.
Legal risks arise, among other things, due to the absence of supporting legislation or weaknesses in the agreement such as failure to fulfill the requirements for the validity of the contract or incomplete binding of collateral.

1.6. Strategic Risk

Strategic Risk is the risk resulting from inaccuracy in making and/or implementing a strategic decision as well as failure to anticipate changes in the business environment.
Strategic risks arise, among other things, because the Bank determines a strategy that is not in line with the Bank's vision and mission, carries out an analysis of the strategic environment that is not comprehensive, and/or there is a mismatch between strategic plans between strategic levels. Apart from that, Strategic Risk also arises from failure to anticipate changes in the business environment, including failure to anticipate changes in technology, changes in macroeconomic conditions, dynamics of competition in the market, and changes in relevant authority policies.

1.7. Compliance Risk

Compliance Risk is the risk resulting from the Bank not complying with and/or not implementing the applicable laws and regulations.

1.8. Reputational Risk

Reputation Risk is the risk resulting from a decline in the level of stakeholder trust originating from negative perceptions of the Bank.

2. Types of Sharia Risk

The Bank as a Conventional Commercial Bank which also carries out sharia business, monitors the types of Risk with an additional 2 (two) Risks as follows:

2.1. Rate of Return Risk

Risk due to changes in the rate of return paid by the Bank to customers, due to changes in the rate of return received by the Bank from disbursement of funds, which can affect the behavior of the Bank's third party fund customers.

2.2. Equity Investment Risk

Risk resulting from the Bank sharing in the customer's business losses financed in profit sharing based financing, whether using the net revenue sharing method or using the profit and loss sharing method.

PT Bank Tabungan Negara (Persero) Tbk
Kantor Pusat
Menara Bank BTN
Jl. Gajah Mada No. 1, Jakarta Pusat 10130 Indonesia

T +62 21 633 6789, 633 2666
E csd@btn.co.id
www.btn.co.id
NPWP: 01.001.609.5-093.000

B. SCOPE OF RISK MANAGEMENT

The Bank carries out Risk Management which covers all types of Risk that must be carried out and is ingrained in all levels of the organization through the implementation of a Risk culture. In addition, the Bank also implements comprehensive integrated monitoring, follow-up, and assessment of the Risk Management maturity index at every level of the Bank organization which is an inseparable part of Bank Risk management.

Risk Management is carried out individually and consolidated/integrated (if the Bank has a Subsidiary Company) while still paying attention to regulations and the Company's business characteristics. The implementation of the Bank's Integrated Risk Management is regulated in separate provisions in accordance with applicable Regulatory provisions.

The General Policy of Risk Management Policy is used as the main guideline in carrying out operational risk management and Bank capital management, which includes:

1. Principle of prudence in every aspect of the Bank's business processes and activities, including: Portfolio Management, Credit/Financing Policy, Provision of Capital Adequacy, Early Warning System, Limit Determination, and Risk Diversification.
2. Risk Management, including: Risk Profile, Risk Appetite, Risk Tolerance, Stress Testing, and Integrated Risk Management (if the Bank has a Subsidiary Company).
   In implementing Risk Management, the Bank applies 4 (four) pillars of Risk Management in accordance with Regulatory provisions, namely:
   2.1. Active supervision of the Board of Directors and Board of Commissioners;
   2.2. Adequacy of Risk Management policies & procedures and limit determination;
   2.3. Adequacy of Risk identification, measurement, monitoring and control processes as well as Risk management information systems; and
   2.4. Comprehensive internal control system.
3. Risk Management for each type of Risk, which includes: risk identification, measurement, monitoring, and control processes.
4. Risk Supervision, which includes: monitoring the implementation of Bank Risk management activities/ methodologies, and the Internal Control System.

A. AUTHORITY AND RESPONSIBILITIES

1. Board of Commissioners

   In implementing effective risk management, the authority and responsibilities of the Board of Commissioners are carried out in accordance with applicable Regulatory provisions regarding the Implementation of Risk Management for Commercial Banks.

2. Sharia Supervisory Board (*Dewan Pengawas Syariah* - DPS)

   In implementing effective risk management, the authority and responsibilities of the Sharia Supervisory Board are carried out in accordance with applicable Regulatory provisions regarding the Implementation of Risk Management for Sharia Commercial Banks and Sharia Business Units.

3. Board of Directors

   3.1. Authority and Responsibilities of the Board of Directors

   In implementing effective Risk Management, there are authorities and responsibilities that must be fulfilled, including:

   3.1.1. Develop written and comprehensive Risk Management policies, strategies and frameworks including overall Risk limits and per Risk type, taking into account Risk Appetite and Risk Tolerance according to the Bank's conditions and taking into account the impact of Risk on capital adequacy.

   3.1.2. Develop, determine and update procedures and tools to implement the Risk Management process.

   3.1.3. Evaluate and/or update Risk Management policies, strategies and frameworks at least 1 (one) time in 1 (one) year or more frequently if there are changes in factors that influence the Bank's business activities, risk exposure and/or profile Risk significantly.

   3.1.4. Determine the organizational structure, including clear authority and responsibility at each level of position related to the implementation of Risk Management.

   3.1.5. Responsible for implementing Risk Management policies, strategies and frameworks that have been approved by the Board of Commissioners as well as evaluating and providing direction based on reports submitted by the Risk Management Work Unit including reports regarding Risk profiles.

   3.1.6. Ensure that all material risks and impacts caused by these risks have been followed up and submit accountability reports to the Board of Commissioners on a regular basis.

3.1.7. Develop and determine transaction approval mechanisms, including those that exceed limits and authority for each level of position.
3.1.8. Ensure the implementation of corrective steps for problems or deviations in the Bank's business activities discovered by the Internal Audit Work Unit.
3.1.9. Developing a Risk Culture including Risk awareness at all levels of the organization.
3.1.10 Ensure adequate resource support to manage and control risks.
3.1.11 Ensure increased human resource competency related to Risk Management.
3.1.12 Carry out regular reviews to ensure the accuracy of the Risk assessment methodology, the adequacy of the implementation of the Risk Management information system and the accuracy of Risk Management policies and procedures and the determination of Risk limits.

3.2. Authority and Responsibilities of the Board of Directors regarding Human Resources (HR)

In order to carry out the responsibility for implementing Risk Management related to HR, the Board of Directors does the following:

3.2.1. Determine clear HR qualifications for each level of position related to the implementation of Risk Management.
3.2.2. Ensure adequate quantity and quality of human resources in the Bank and ensure that SOM understands their duties and responsibilities.
3.2.3. Develop an employee recruitment, development and training system including managerial succession plans and adequate remuneration to ensure the availability of competent employees in the field of Risk Management.
3.2.4. Ensuring increased competence and integrity of the leadership and personnel of the Operational Work Unit, Risk Management Work Unit and Internal Audit Work Unit, by paying attention to factors such as adequate knowledge, experience/track record and ability in the field of Risk Management through continuous education and training programs, to ensure the effectiveness of the Risk Management process.
3.2.5. Assign competent officials and statistics to each work unit in accordance with the nature, number and complexity of the Bank's business activities.
3.2.6. Ensure that officials and staff assigned to each work unit have:
3.2.6.1. understanding of the risks inherent in each Bank product/activity;
3.2.6.2. understanding of relevant risk factors and market conditions that influence the Bank's products/activities, as well as the ability to estimate the impact of changes in these factors on the Bank's business continuity;

3.2.6.3. ability to communicate the implications of Bank Risk exposure to the Board of Directors and Risk Management Committee in a timely manner.

3.2.6.4. ensure that all human resources understand the strategy, the level of risk to be taken, risk tolerance, and the risk management framework and implement it consistently in the activities handled; and

3.2.6.5. ensure that all SOMs are required to have Risk Management certification in accordance with the Regulator's provisions regarding Risk Management Certification for Bank administrators and officials.

4. Director/Official in charge of the Risk Management function

In order to carry out the responsibility for implementing the Risk Management function, the Director/Official in charge of the Risk Management function does the following:

4.1. Carry out Bank management in accordance with the field of Risk management in accordance with the provisions of laws and regulations, articles of association and/or other applicable provisions.

4.2. Carry out the determination of strategies and policies in the field of Risk management which are his responsibility by taking into account the Bank's vision, strategy and policies that have been determined.

4.3. Carry out the preparation and determination of work plans, development plans and human resources in the field of risk management which are their responsibilities for the benefit of SOE in achieving the Company's aims and objectives.

4.4. Carry out coordination and provide direction for the implementation of the principles of good corporate governance.

4.5. Carry out the necessary steps to ensure that SOE has complied with all applicable laws and regulations and ensure that the Bank's business activities do not deviate from applicable laws and regulations.

4.6. Carry out monitoring and maintain the Bank's compliance with all agreements and commitments made by the Bank to external parties.

4.7. Carrying out work organization development so that the Bank has reliable policies, procedures and methods in implementing risk management.

4.8. Carry out compliance monitoring and supervision attached to all work units of the Risk Management organization.

B. ORGANIZATION AND FUNCTIONS OF RISK MANAGEMENT

1. Risk Monitoring Committee

   The Risk Monitoring Committee is a Committee formed by and responsible to the Board of Commissioners whose task is to assist the Board of Commissioners in evaluating the suitability of the Risk Management Policy with the implementation of said policy and monitoring and evaluating the implementation of the duties of the Risk Management Committee and Risk Management Work Channels. Furthermore, it will be regulated and determined in the Risk Monitoring Committee Charter.

2. Risk Management Committee

   The Risk Management Committee is a committee formed to assist the implementation of the duties and authority of the Board of Directors related to the implementation of Risk Management.

   2.1. Membership of the Risk Management Committee

   The following are some of the characteristics of Risk Management Committee membership:

   2.1.1. The Risk Management Committee is generally permanent but can be supplemented with non-permanent members according to needs.

   2.1.2. The membership of the majority of the Board of Directors and related executive officers takes into account matters in accordance with applicable Regulatory provisions

   2.2. Authority and responsibility of the Risk Management Committee

   2.2.1. Carry out evaluations and provide recommendations to the President Director regarding Risk Management that at least comply with Regulatory provisions, including but not limited to:

   2.2.1.1. Preparation of policies, strategies and guidelines for implementing Risk Management;

   2.2.1.2. Improvement or refinement of the implementation of Risk Management based on the results of the evaluation of the implementation of Risk Management; and

   2.2.1.3. Determining matters related to business decisions that deviate from normal procedures.

   2.2.2. Monitor the implementation of monitoring of risks and activities of the Bank's Sharia business activities.

The composition of membership, detailed authority and responsibility details, as well as other procedures related to the Risk Management Committee are regulated in a separate internal regulation.

3. Risk Management Work Unit

The Risk Management Work Channel is a work unit that is directly responsible to the Director in charge of the Risk Management function and is independent of the Operational Work Unit which is a risk-faking unit, the Internal Audit Work Unit and the Compliance Work Channel.

3.1. Authority and Responsibilities of the Risk Management Work Unit

The authorities and responsibilities of the Risk Management Work Unit include at least:

3.1.1. provide input to the Board of Directors in the preparation of policies, strategies and Risk Management frameworks;

3.1.2. develop procedures and tools for risk identification, measurement, monitoring and control;

3.1.3. design and implement the tools needed to implement Risk Management;

3.1.4. monitor the implementation of Risk Management policies, strategies and frameworks recommended by the Risk Management Committee and approved by the Board of Directors;

3.1.5. monitor Risk positions/exposures as a whole, as well as per Risk, including monitoring compliance with Risk tolerances and established limits;

3.1.6. carry out stress testing to determine the impact of the implementation of Risk Management policies and strategies on the Bank's portfolio or overall performance;

3.1.7. reviewing proposed new activities and/or products developed by other units. The assessment focuses primarily on aspects of the Bank's ability to manage new activities and/or products including the completeness of the systems and procedures used and their impact on the Bank's overall risk exposure;

3.1.8. provide recommendations to business work units and/or to the Risk Management Committee regarding the implementation of Risk Management, including regarding the amount or maximum risk exposure that can be maintained and carry out escalations as needed;

3.1.9. evaluate the accuracy and validity of data used by the Bank to measure Risk for Banks that use models for internal purposes;

3.1.10 prepare and submit Risk profile reports to Regulators, Board of Commissioners, Board of Directors and Risk Management Committee periodically or at least quarterly. Report frequency is increased if market conditions change rapidly;

3.1.11 carry out regular reviews with a frequency adjusted to the Bank's needs, to ensure:

3.1.11.1. adequacy of the Risk Management framework;

3.1.11.2. accuracy of the Risk assessment methodology; and

3.1.11.3. adequacy of the Risk Management information system; as well as

3.1.12 The organizational structure, duties and responsibilities as well as other matters including the work procedures of the Risk Management work unit are regulated in a separate internal regulation.

3.2. In implementing its duties and responsibilities, the Risk Management Work Unit also identifies, measures and monitors risks and activities of the Bank's Sharia business activities.

3.2.1. The Risk Management Work Channel includes managing risks in a consolidated manner for all types of risks that have been defined. The implementation of integrated Risk Management in accordance with the Enterprise Risk Management concept is also implemented by the Risk Management Work Unit function in determining business strategy and planning, developing new products and businesses, determining pricing and/or measuring business performance.

3.2.2. The organizational structure, details of duties and responsibilities, as well as other matters including the work procedures of the Risk Management work unit are regulated in a separate internal regulation.

3.3. Apart from the organization and related Risk Management functions described above, there are also committees supporting the implementation of Risk Management which also apply Risk Management principles in their duties and responsibilities which will be regulated in separate internal regulations.

C. THREE LINES OF DEFENSE

The linkage of all levels of organization in the Bank in terms of risk management is carried out through the implementation of the Three Lines of Defense which divides the organizational function of Risk Management into three (3) layers of defense which are independent in each of these layers.

1. First (1st) line of defense

   1st line of defense includes all Operational Work Units in the Bank which act as risk owners/risk taking units (RTU) including RTU units that run Sharia business.

   1.1. Function and Position of the Risk Taking Unit (RTU)

   The function and position of the Risk Taking Unit in implementing Risk Management are as follows:

   1.1.1. The Risk Taking Unit carries out checks and balances, as well as dual control in the implementation of operational activities;

   1.1.2. The Risk Taking Unit is directly responsible to the Director in charge of the work unit concerned; and

   1.1.3. The Risk Taking Unit is a separate unit from the Risk Management Work Unit.

   1.2. Authority and Responsibility of the Risk Taking Unit in Implementing Risk Management

   The Risk Taking Unit has authority and responsibility in implementing Risk Management which includes:

   1.2.1. identify, measure, monitor and control risks regarding products and activities/ transactions and their impact on the Bank's risk exposure;

   1.2.2. submit proposals for new activities/ products;

   1.2.3. maintain good relations with all customers and counterparties and maintain the good name of the Bank; and

   1.2.4. Inform the risk exposure inherent in operational activities and in the development of new products in the relevant work unit to the Risk Management Work Unit on a regular basis.

   1.3. In order to implement effective risk control, the Bank also implements independent functions in several Operational Work Units that are not directly related to risk taking actions or recommendations for decisions. This function was formed as an additional control effort from the 1st line of defense whose task is to monitor and measure the level of risk that occurs in the Operational Work Unit, to then be reported to the head of the relevant work unit as a basis for the risk control strategy in the 1st line of defense.

2. Second (2nd) line of defense

Independent work units in implementing Risk Management and internal control are as follows:

2.1. Risk Management Work Unit

In implementing the three lines of defense, the Risk Management Work Unit acts as the 2nd line of defense unit with a general description of duties and responsibilities as outlined in Chapter III Sub-Chapter B Number 3.

2.2. Compliance Work Unit

2.2.1. The Compliance Work Unit is one of the functions/parties involved in internal control which is directly responsible to the Director in charge of the Compliance function.

2.2.2. The Compliance Work Unit is independent of the Business Work Unit, Risk Management Work Unit and Internal Audit Work Unit.

2.2.3. Authorities and responsibilities of the Compliance Work Unit

The authority and responsibilities of the Compliance Work Unit in the process of implementing Risk Management at a minimum include:

2.2.3.1. take steps to support the creation of a Compliance Culture in all Bank business activities at every level of the organization;

2.2.3.2. identify, measure, monitor and control Compliance Risk by referring to the provisions of the Financial Services Authority which regulate the implementation of Risk management for commercial banks and the provisions of the Financial Services Authority which regulate the implementation of Risk management for sharia commercial banks and sharia business units;

2.2.3.3. assess and evaluate the effectiveness, adequacy and conformity of the Bank's policies, provisions, systems and procedures with the provisions of laws and regulations;

2.2.3.4. review and/or recommend updating and improving policies, provisions, systems and procedures owned by the Bank so that they comply with the provisions of the Financial Services Authority and statutory regulations, including Sharia Principles for sharia commercial banks and sharia business units;

2.2.3.5. make efforts to ensure that the Bank's policies, provisions, systems and procedures, as well as business activities are in accordance with the provisions of the Financial Services Authority and statutory regulations; and

2.2.3.6. perform other tasks related to the Compliance Function.

3. Third (3rd) line of defense

3.1. The party included in the third line of implementing the three lines of defense is the Internal Audit Work Unit. The Internal Audit Work Unit is a function tasked with independently assessing the effectiveness of the implementation of Risk Management in internal control.

3.2. The Internal Audit Work Unit is directly responsible to the Director who oversees the Internal Audit function which is independent of the Business Work Unit, Risk Management Work Unit and Compliance Work Unit.

3.3. Authority and responsibility of the Internal Audit Work Unit

The authority and responsibility of the Internal Audit Work Channel in the process of implementing Risk Management includes carrying out reviews of at least:

3.3.1. reliability of the Risk Management framework, which includes policies, organizational structure, resource allocation, Risk Management process design, information systems and Bank Risk reporting; and

3.3.2. implementation of Risk Management by business units/supporting activities, including review of monitoring implementation by the Risk Management Work Channel.

D. RISK CULTURE

As one of the Bank's efforts to ensure that the implementation of Risk Management supports all business strategies and objectives, the Bank established a Risk Culture Pillar as part of the four Bank Culture Pillars.

The implementation of Risk culture is used as a basis for the formation of procedures, attitudes, behavior or understanding related to the implementation of Risk Management carried out at all levels of the Bank organization in carrying out all duties and responsibilities to achieve predetermined strategic goals.

1. General Provisions for Risk Culture

   In implementing Risk culture, the Bank pays attention to several aspects as follows:

   1.1. The Bank maintains its commitment to ensure that the Risk culture policy is understood and implemented by all Bank management and employees.

   1.2. The Risk culture implementation strategy is in line with the Bank's culture implementation strategy and the Bank's Risk Management implementation strategy.

   1.3. The Bank sets a roadmap for implementing Risk culture each year according to the maturity level it wishes to achieve.

   1.4. All levels of the Bank organization have duties and responsibilities in implementing Risk Culture.

   1.5. The implementation of Risk Culture is integrated with the process of preparing a competency development roadmap, performance measurement indicators, training and education, and is an integral part of the implementation of the overall corporate culture program, which is the responsibility of all functions and related parties which are specifically described in separate internal regulations.

   1.6. The level of maturity in the implementation of Risk culture and the implementation of Risk Management as a methodology for understanding the gap between implementation and the goals expected by the Bank were measured.

   1.7. In implementing Risk culture, it is carried out by:

      1.7.1. effective and open two-way communication;

      1.7.2. rewards and sanctions are applied consistently and transparently; and

      1.7.3. work assessment takes into account the implementation of Risk Management.

2. Risk Culture Objectives

2.1. Ensure that all levels of the organization have knowledge about Risk, both awareness of the dangers of Risk and the benefits if Risk can be controlled properly in every banking activity.
2.2. Confirmation that every level in the Bank organization is aware and understands that risk is something that cannot be avoided, but rather something that must be managed to support performance.
2.3. Making Risk culture an inseparable part of company culture.
2.4. Ensure decision making in terms of preparing strategic plans and performance is based on Risk Management strategies.

Detailed provisions related to Risk culture will be regulated in derivative regulations from this General Policy.

A. RISK MANAGEMENT STRATEGY

In determining the implementation of Risk Management, including the preparation of special policies and limits, the Bank pays attention to the Risk Management strategy which has been adapted to the overall business strategy by taking into account the level of risk to be taken (risk appetite) and risk tolerance (risk tolerance).

The Bank's Risk Management Strategy aims to ensure that Risk exposure is managed in a controlled manner in accordance with policies, internal procedures and applicable laws and regulations in order to achieve the goal of a good Bank Soundness Level.

1. General Principles

   The following are several general principles established by the Bank in developing a Risk Management Strategy:

   1.1. Risk Management strategy is an inseparable part of the company plan as stated in the Bank Business Plan (RBB) and Company Work Plan and Budget (*Rencana Kerja dan Anggatan Perusahaan* - RKAP);
   1.2. Risk Management strategies are used as a basis for determining the limits of the level of risk to be taken (risk appetite) and risk tolerance (risk tolerance);
   1.3. long-term oriented Risk Management strategy to ensure the continuity of the Bank's business by considering economic conditions/cycles as stated in the Recovery Plan and Resolution Plan;
   1.4. a comprehensive Risk Management strategy can control and manage Bank Risk and is reflected in the results of a good Bank Health Level; And
   1.5. achieving capital adequacy accompanied by adequate resource allocation.

2. Consideration Factors

   Factors considered by the Bank in developing a Risk Management strategy:

   2.1. economic and industrial developments and their impact on Bank Risk;
   2.2. Bank organization including the adequacy of human resources and supporting infrastructure;
   2.3. the Bank's financial condition, including the ability to generate profits, and the Bank's ability to manage risks arising as a result of changes in external and internal factors; and
   2.4. mix and diversification of the Bank's portfolio.

3. The Board of Directors must communicate the Risk Management strategy effectively to all Work Units and employees so that it is clearly understood.

4. The Board of Directors must periodically review the Risk Management strategy, including its impact on the Bank's financial performance, to determine the need for changes to the Bank's Risk Management strategy.

B. RISK MANAGEMENT POLICIES & PROCEDURES

1. General Policy of Risk Management Policy must be reviewed at least 1 (one) time in 1 (one) year. The results of the review must be reported to the Board of Directors and Board of Commissioners. The KUMR review process must be documented and administered in an orderly manner.
2. Provisions for preparing the Risk Management Policy

   Risk Management Policy is a provision that regulates the rules for implementing Risk Management in the Bank, both at the Special Policy and Technical Instructions levels.

   The Risk Management Policy is designed and implemented by taking into account the characteristics and complexity of business activities, the level of risk to be taken and risk tolerance, risk profile and regulations set by the authorities and/or sound banking practices.

   The Risk Management Policy includes but is not limited to:

   2.1. Determination of risks related to products and transactions based on the results of analysis of the risks inherent in each banking product and transaction that have been and will be carried out in accordance with the characteristics and complexity of the Bank's business activities;

   2.2. Determining methods for identifying, measuring, monitoring and controlling Risk as well as Risk Management information systems in order to accurately assess Risk exposure in each banking product and transaction as well as the Bank's business activities;

   2.3. The determination of reported data, report format, and type of information included in the Risk Management report reflects the risk exposure that is taken into consideration in the context of making business decisions while still paying attention to the precautionary principle;

   2.4. Determination of authority and limit amounts in stages, including transaction limits that require approval from the Board of Directors, as well as determination of Risk tolerance which is a limit of potential losses that can be absorbed by capital capacity, and a means of monitoring the development of Risk exposure;

   2.5. Determination of Risk profile ratings as a basis for determining steps to improve certain products, banking transactions and areas of bank business activities and evaluating the results of implementing Risk Management policies and strategies;

   2.6. An organizational structure that clearly defines the roles and responsibilities of related parties implementing Risk Management;

   2.7. Establishment of an internal control system in the implementation of Risk Management to ensure compliance with applicable external and internal regulations, effectiveness and efficiency of operational activities, effectiveness of Risk culture at every level of the organization, as well as the availability of management and financial information that is accurate, complete, appropriate and timely ;

2.8. Business continuity plan policies (business continuity plans or business continuity management) for the worst possible external and internal conditions, so that business continuity can be maintained, including disaster recovery plans and contingency plans. The preparation of business continuity plan policies meets the following provisions:

  2.8.1. involving various related work units;
  2.8.2. is flexible to be able to respond to various unexpected and specific disruption scenarios, namely a description of certain conditions and the actions required immediately;
  2.8.3. periodic testing and evaluation of business continuity plans; and
  2.8.4. The Board of Directors will test, review and update the business continuity plan periodically to ensure the effectiveness of the business continuity plan that has been prepared.

2.9. The Risk Management Policy is adequately documented and communicated to all employees.

C. DETERMINING RISK LIMITS

The Bank determines Risk limits in accordance with the level of Risk taken, Risk tolerance, and overall strategy by taking into account the capital's ability to absorb Risk exposure or losses that arise, past loss experience, human resource capabilities, and compliance with the applicable external regulations. The following are several things considered by the Bank in determining Risk limits:

1. Risk limits are determined by considering the level of risk to be taken (risk appetite) and risk tolerance (risk tolerance), which has taken into account the Bank's business strategy and objectives as well as the Bank's ability to take risks (risk bearing capacity)
2. Procedures for setting minimum limits include:
   2.1. clear accountability and levels of delegation of authority;
   2.2. adequate documentation of procedures and limit determination to facilitate the implementation of reviews and audit trails;
   2.3. carrying out reviews of procedures and setting limits periodically at least 1 (one) time in 1 (one) year or a more frequent frequency, in accordance with the type of risk, needs and developments of the Bank;
   2.4. Risk limit determination is carried out comprehensively for all aspects related to Risk, which includes overall limits, limits per Risk, and limits per bank business activity that has Risk exposure; and
   2.5. approval mechanism in case of exceeding the limit.
3. Risk limits are communicated well at all levels of the organization, including when changes occur.
4. The risk limit is used as a threshold to determine the level of risk mitigation intensity1 that will be implemented by management, including as a basis for preparing a follow-up plan (recovery plan) and resolution plan (resolution plan) for the Bank in the event that the threshold limit is exceeded.
5. The limit amount is proposed by the relevant Operational Work Unit, which is then recommended to the Risk Management Work Unit to obtain approval from the Committee in accordance with its authority as regulated in the Bank's internal regulations.
6. Determination of Risk limits is carried out in detail, through determining Risk limits per type of Bank Risk, determining Risk limits per Bank functional activity and determining Risk limits as a whole.
7. Risk limits are reviewed periodically by the Board of Directors and/or the Risk Management Work Unit to adapt to changes in conditions that occur.

Detailed provisions regarding limits per type of risk are regulated by derivative regulations from this General Policy.

D. RISK MANAGEMENT PROCESS

The Bank's Risk Management Process consists of the process of identifying, measuring, monitoring and controlling all risks managed by the Bank, which are formed with the aim of achieving a final score of good Bank Health Level. The following are several things that banks need to pay attention to for each Risk Management process:

1. Risk identification

   The aim of the Risk identification process is to identify all types of Risk inherent in each functional activity that has the potential to be detrimental and the implementation of new products and/or activities at the Bank.

   Things that need to be considered in implementing the Risk identification process:

   1.1. carried out periodically;

   1.2. supported by an adequate method or system; and

   1.3. includes analysis of all sources of risk, risk events and the impact of risk on the Bank's products and/or activities, as well as ensuring that risks from new products and activities have gone through an appropriate risk management process before being introduced or implemented.

2. Risk Measurement

   2.1. Risk Measurement System

   The Risk Measurement System is used to measure the amount of risk exposure which is used as a reference in carrying out risk control, and is carried out periodically for each existing product, new product implementation, portfolio and all Bank business activities.

   The Risk measurement system must be able to measure:

   2.1.1. Product/activity sensitivity to changes in factors that influence it, both under normal and abnormal conditions;

   2.1.2. The tendency for changes in the factors referred to is based on fluctuations that have occurred in the past and their correlation;

   2.1.3. Individual Risk Factors;

   2.1.4. Risk Exposure overall and per Risk, taking into account the relationship between Risks;

   2.1.5. All risks inherent in all transactions as well as Bank products and/or activities, including new products and activities, and can be integrated into the Bank's management information system; and

   2.1.6. Predict the potential possibility of a Risk event occurring.

The Risk measurement system will be evaluated and refined periodically or at any time if necessary to ensure the suitability of assumptions, accuracy, fairness and integrity of data, as well as procedures used to measure Risk.

2.2. Risk Measurement Methods

Risk measurement methods can be carried out quantitatively and/or qualitatively. This method can be a method determined by the Regulator or an internal Bank method that has been adapted to the characteristics and complexity of business activities.

In implementing internal methods for risk measurement, the Bank considers several aspects as follows:

2.2.1. Requirements for using the internal model, at a minimum include:

2.2.1.1. the content and quality of data created or maintained in accordance with generally applicable standards so as to enable reliable statistical results;

2.2.1.2. availability of a management information system that enables the system to retrieve appropriate and accurate data and information at the right time;

2.2.1.3. availability of a system that can produce Risk data for all Bank positions;

2.2.1.4. availability of documentation from data sources used for the purposes of the Risk measurement process; and

2.2.1.5. Databases and data storage processes are part of system design to prevent discontinuity in a series of statistical data.

2.2.2. Mandatory validation is carried out by an independent internal party or an appointed external party for the work unit that applies the model. Here are some further explanations related to validation:

2.2.2.1. Validation is a process:

a. evaluation of the internal logic of a particular model by verifying mathematical accuracy;
b. comparing model predictions with events after a certain position date (subsequent events); and/or
c. compare one model with other existing models.

2.2.2.2. In validating the internal model, the Bank uses historical data or a series of parameters and assumptions prepared internally and/or assumptions determined by the Regulator.

2.2.2.3. Validation is also carried out on new models, both those developed internally by the Bank and externally.

2.2.3. The model used is validated or backtesting periodically, especially in the event of significant changes in market conditions.

2.2.4. The risk measurement process must clearly include the validation process, validation frequency, data and information documentation requirements, evaluation requirements for the assumptions used, before the model is applied.

2.2.5. Risk measurement methods must be clearly understood by employees involved in risk control.

2.3. Stress testing

Stress testing is a type of test to complete the Risk measurement system by estimating potential losses in abnormal market conditions using certain scenarios to see the sensitivity of the Bank's overall performance to changes in Risk factors and identify influences that have a significant impact on the Bank's portfolio.

The Bank carries out stress testing periodically and reviews the results of the stress testing and takes appropriate steps if the predicted conditions that will occur exceed acceptable tolerance levels. The results of stress testing and reviews are used as input when determining or changing policies and limits.

3. Risk Monitoring

Risk monitoring systems and procedures include, among other things, risk monitoring of the magnitude of risk exposure, risk tolerance, internal limit compliance, and stress testing results as well as implementation consistency with established policies and procedures.

The things to pay attention to in implementing Risk monitoring are as follows:

3.1. monitoring is carried out both by the implementing unit and by the Risk Management Work Unit;

3.2. monitoring results are presented in periodic reports submitted to Management in the context of Risk mitigation and necessary actions; and

3.3. Risk monitoring is supported by effective back-up and procedures and carries out regular inspections and re-assessments of the back-up system.

4. Risk Control

The risk control process is adjusted to risk exposure and the level of risk to be taken (risk appetite) and risk tolerance. Risk control mechanisms implemented at the Bank include:

4.1. treating a risk: taking direct steps to reduce the impact or frequency of the risk;

4.2. terminating a risk: stopping activities that give rise to risk exposure;

4.3. transfer a risk: transferring risk to another party, for example through insurance or hedging (hedging activities); and

4.4. tolerate a risk: An acceptable risk.

5. Reporting

5.1. External Reporting (Regulator)

The Bank submits all Risk Management reports regulated by Regulators or related external parties who oversee the Bank's business, including the Ministry of SOE, in accordance with applicable needs and regulations.

5.2. Internal Reporting

The Bank prepares reports on the implementation of Risk Management to Bank Management on a regular basis with reports describing all exposures, positions and conditions of Risk Management in the Bank through various reports regulated by regulations as well as for internal Risk monitoring needs.

6. Risk Management Information System

The Risk Management Information System is part of the information system developed in accordance with the Bank's needs in order to implement effective Risk Management. The Bank's Risk Management Information System is used to implement risk identification, measurement, monitoring and control processes. In its implementation, the Bank pays attention to several things as follows:

6.1. Development of Risk Management Information Systems

Bank Management Information System development is carried out in order to ensure:

6.1.1. the availability of information that is accurate, complete, informative and timely, so that it can be used by the Board of Commissioners, Board of Directors and related work units in implementing Risk Management to assess, monitor and mitigate the risks faced, both overall/composite risks and each risk and/or in the framework of the decision making process by the Board of Directors;

6.1.2. effectiveness of implementing Risk Management which includes policies, procedures and setting Risk limits; and

6.1.3. availability of information about the results (realization) of the implementation of Risk Management compared to the targets set in accordance with the policies and strategies for implementing Risk Management.

6.2. Risk Management Information System Components

Things that the Bank should pay attention to when establishing a Risk Management Information System:

6.2.1. The Risk Management Information System and the information produced are adapted to the characteristics and complexity of business activities and are adaptive to change.

6.2.2. The adequacy of information coverage produced from the Risk Management information system is reviewed periodically to ensure that the coverage is adequate according to developments in the level of complexity of business activities.

6.2.3. The Risk Management information system supports reporting to Regulators.

6.2.4. In developing new information system technology and software, the Bank ensures that the implementation of new information systems and technology will not disrupt the continuity of the information system as a whole.

6.2.5. In the event that software development and system improvements are assigned to outsourced workers, the Bank ensures that the decision to appoint the third party is carried out objectively and independently. The related outsourcing agreement or contract includes clauses regarding maintenance, maintenance and anticipatory steps to prevent disruptions that may occur in its operations and ensure the fulfillment of data confidentiality agreements.

6.2.6. The new management information system that will be implemented has been tested first to ensure that the processes and outputs produced have gone through an effective and accurate development, testing and reassessment process, as well as ensuring that historical accounting and management data can be accessed by the system/device the new software works fine.

6.2.7. Administering and initiating system documentation containing hardware, software, databases, parameters, process stages, assumptions used, data sources and output produced, thereby facilitating inherent control and implementation of audit trails.

E. INTERNAL CONTROL SYSTEM

In carrying out the process of implementing effective Risk Management, the Bank completes an internal control system aimed at safeguarding the Bank's assets, ensuring the availability of reliable financial and managerial reporting, increasing compliance with statutory provisions and regulations, and reducing the risk of losses, deviations and violations. precautionary aspect.

With the existence of a reliable and effective internal control system, increasing organizational effectiveness and increasing cost efficiency is the responsibility of all Operational Work Channels and supporting work units as well as the Internal Audit Work Unit.

1. Implementation of the Internal Control System

   Matters that the Bank pays attention to in implementing the internal control system include the following:

   1.1. Effective implementation of the internal control system in implementing Bank Risk Management refers to the policies and procedures that have been established by the Bank. There is an application of the principle of separation of functions and duties (segregation of duties) which must be adequate and implemented consistently. The internal control system is also carried out by implementing a dual control system through the four eyes principle in decision making.

   1.2. The internal control system ensures, among other things:

      1.2.1. compliance with regulations and legislation as well as Bank internal policies or regulations;

      1.2.2. availability of complete, accurate, effective and timely financial and management information;

      1.2.3. effectiveness and efficiency in operational activities; and

      1.2.4. effectiveness of risk culture in the Bank organization as a whole.

   1.3. The Internal Control System in the Implementation of Risk Management includes at least:

      1.3.1. suitability of the internal control system to the type and level of risk inherent in the Bank's business activities;

      1.3.2. determining authority and responsibility for monitoring compliance with Risk Management policies and procedures, as well as determining Risk limits;

      1.3.3. establishing reporting lines and clear separation of functions from Operational Work Units to work units that carry out control functions;

1.3.4. an organizational structure that clearly describes the duties and responsibilities of each unit and individual;

1.3.5. accurate and timely reporting of financial and operational activities;

1.3.6. adequacy of procedures to ensure the Bank's compliance with regulations and legislation;

1.3.7. effective, independent and objective review of the Bank's operational policies, framework and procedures;

1.3.8. adequate testing and review of the Risk Management information system;

1.3.9. complete and adequate documentation of operational procedures, scope. and audit findings, as well as the Bank management's response based on the audit results; and

1.3.10. periodic and continuous verification and review of the Bank's handling of material weaknesses and the actions of the Bank's management to correct deviations that occur.

1.4. Implementation of a review of the implementation of Risk Management includes at least:

1.4.1. reviews and evaluations are carried out periodically, at least annually by the Risk Management Work Unit and the Internal Audit Work Unit; frequency/intensity of review and evaluation coverage can be increased based on developments in Bank Risk exposure, market changes, measurement methods and Risk management;

1.4.2. implementation of review and evaluation of Risk measurements by the Risk Management Work Unit, at least includes:

1.4.2.1. suitability of the Risk Management framework, which includes policies, organizational structure, resource allocation, Risk Management process design, information systems and Bank Risk reporting with the Bank's business needs, as well as the development of regulations and best practices related to Risk Management;

1.4.2.2. methods, assumptions and variables used to measure Risk and determine Risk exposure limits;

1.4.2.3. comparison between the results of Risk measurement methods that use simulations or future projections with actual results;

1.4.2.4. comparison between the assumptions used in the method in question and actual conditions;

1.4.2.5. comparison between the set limit and actual exposure; and

1.4.2.6. provisions for conformity between Risk exposure measurements and limits with past performance and the Bank's current capital position.

1.4.3. The implementation of reviews by independent parties or the Internal Audit Work Unit includes, among other things:

1.4.3.1. reliability of the Risk Management framework, which includes policies, organizational structure, resource allocation, Risk Management process design, information systems and Bank Risk reporting; and

1.4.3.2. implementation of Risk Management by business units/supporting activities, including review of monitoring implementation by the Risk Management Work Channel.

1.5. Submission of the results of the review assessment carried out by the Risk Management Work Channel to the Board of Commissioners, Internal Audit Work Unit, Director in charge of the compliance function, Audit Committee and other relevant Board of Directors as input in order to improve the Risk Management framework and process.

1.6. Monitoring by the Internal Audit Work Unit regarding improvements to internal and external audit findings. Audit findings that have not been followed up will be informed by the Internal Audit Work Channel to the Board of Directors so that necessary steps can be taken.

1.7. The Bank's level of responsiveness to weaknesses and/or deviations that occur against applicable internal and external regulations.

1.8. Banks must at least formalize and document adequate policies, procedures and systems.

1.9. This document must be updated periodically to describe the actual implementation of Bank Risk Management, and must be communicated to Bank officials and employees.

1.10 Upon request, documents must always be available for the benefit of internal and external auditors, the public, and bank supervision by regulators.

1.11 The accuracy and availability of documents must be assessed by internal auditors when conducting routine and non-routine audits.

In order to follow up on the implementation of Risk Management and increase the ability to absorb risks caused by both normal activities and crisis conditions, the Bank will ensure capital adequacy in accordance with applicable industry regulations and practices.

The following are the components monitored by the Bank in terms of maintaining capital adequacy:

A. MINIMUM CAPITAL PROVISION OBLIGATION (*Kewajiban Penyediaan Modal Minimum* - KPMM)

1. The capital components referred to consist of 2 (two) types, namely tier 1 capital which consists of main core capital (common equity tier 1) and additional core capital (additional tier 1), as well as complementary capital (tier 2).
2. As part of calculating the adequacy of the Bank's minimum capital as determined by the Regulator, the Bank uses the Risk Weighted Assets (RWA) calculation method from the following 3 (three) types of Risk:
   - 2.1. Credit Risk;
   - 2.2. Market Risk; and
   - 2.3. Operational Risk.

   All approaches in calculating the three RWAs mentioned above are carried out through several approaches that follow the applicable regulations.
3. The Bank provides minimum capital according to the risk profile, apart from being aimed at anticipating potential losses which, among other things, arise from Risk Weighted Assets (RWA) which have taken into account Credit Risk, Market Risk and Operational Risk, also to anticipate potential future losses from Risk that have not been fully taken into account in RWA include concentration risk, liquidity risk, interest rate risk in the banking book, legal risk, bankruptcy risk, reputation risk and strategic risk, as well as to anticipate the impact of implementation stress testing scenarios for Bank capital adequacy.
4. Apart from adjusting to the Bank's risk profile, the Bank considers the calculation of additional capital which functions as a buffer; aims to assist the Bank in situations of financial and economic crises that can disrupt the stability of the financial system. There are 3 (three) types of buffers that are considered by the Bank:
   - 4.1. Capital Conservation Buffer is additional capital that functions as a buffer in the event of a loss during a crisis period;
   - 4.2. Countercyclical Buffer is additional capital that functions as a buffer to anticipate losses in the event of excessive growth in banking credit which has the potential to disrupt the stability of the financial system; and
   - 4.3. Capital Surcharge for Systemic Banks is additional capital which functions to reduce the negative impact on the stability of the financial system and economy in the event of

a Bank failure which has a systemic impact by increasing the Bank's ability to absorb losses.

5. In addition, the Bank also takes into account the allocation of capital managed to support the Bank's business activities, including but not limited to business expansion plans such as opening office networks and other activities such as mergers and acquisitions.
6. Provisions for detailed procedures related to KPMM fulfillment are regulated in separate regulations while still referring to the applicable provisions.

B. INTERNAL CAPITAL ADEQUACY ASSESSMENT PROCESS (ICAAP)

The Bank implements the Internal Capital Adequacy Assessment Process to fulfill the minimum capital requirement according to the Risk profile which is adjusted to the size, characteristics and complexity of the Bank's business.

1. In implementing ICAAP, the Bank determines capital adequacy according to the Bank's Risk profile and develops a strategy to maintain capital levels periodically.
2. ICAAP components
   The components in implementing ICAAP in Banks are as follows:
   2.1. Active supervision of the Board of Directors and Board of Commissioners.
   2.2. Capital adequacy assessment includes at least:
      2.2.1. adequate policies and procedures to ensure that all risks have been identified, measured and reported periodically to the Board of Directors and Board of Commissioners;
      2.2.2. methods and processes for assessing capital adequacy by linking the level of risk with the level of capital required to absorb potential losses from the risk in question;
      2.2.3. adjustments to the methods and assumptions used in the event of changes to the business plan, risk profile and external factors; and
      2.2.4. documentation of Risk measurement results and calculation of required capital levels, including the methods and assumptions used.
   2.3. Monitoring and reporting, includes at least:
      2.3.1. Adequate information system to monitor and report Risk exposure and measure the impact of changes in Risk profile on the Bank's capital requirements; and
      2.3.2. Risk profile reports and capital levels submitted periodically to the Board of Directors and Board of Commissioners.
   2.4. Internal Control, includes an adequate internal control system to ensure the reliability of the implemented ICAAP.
3. The Bank documents the process of implementing and implementing ICAAP in accordance with applicable Regulatory provisions.
4. Procedural provisions related to the implementation of capital are regulated in derivative regulations from this General Policy while still referring to the applicable Regulatory provisions.

C. IMPLEMENTATION OF THE RECOVERY PLAN AND RESOLUTION PLAN

The Bank implements an action plan (recovery plan) and resolution plan (resolution plan) in order to ensure adequate capital and financial capacity to maintain the continuity of the Bank's business. One of the main objectives in preparing this action plan and resolution is to outline plan options in order to maintain the Bank's capital adequacy and liquidity if a crisis scenario occurs that could threaten the continuity of the Bank's business.

The following are several General Principles and Processes carried out by the Bank in preparing action plans and resolutions:

1. Principles for Recovery Plans and Resolution Plans in Banks
   1.1. Prepared by considering the company's overall strategy and risk strategy.
   1.2. As a form of follow-up mitigation action if there is an excess of the predetermined limits (risk appetite and risk tolerance).
   1.3. Involving all business aspects related to the Bank in the context of efforts to prevent, recover and improve crisis conditions which could impact the continuity of the Bank's business.
2. Components in preparing the Action Plan (Recovery Plan) and Resolution Plan (Resolution Plan) at the Bank
   2.1. Action plan
      2.1.1. Analyze and identify the Bank's main business.
      2.1.2. Determining responsible parties and communicating related plans to all levels and levels of the organization.
      2.1.3. Carrying out stress testing tests covering various crisis scenarios.
      2.1.4. Determine the trigger level indicator.
      2.1.5. Develop recovery plan options.

2.2. Resolution Plan
   2.2.1. Analyze strategic business which includes analysis of business group structure, financial information, material business lines, economic functions, and critical linkages of the Bank's business with external conditions.
   2.2.2. Preparation of resolution plan options.
   2.2.3. Preparation of a plan addresses potential obstacles to implementing resolution plan options.
   2.2.4. Analysis of business continuity when handling or resolution in a Bank scenario is declared failed, which includes identification of operational aspects and access to critical financial market infrastructure.

2.2.5. Preparation of communication strategies and management information systems.

This action plan and resolution document involves the Controlling Shareholders and is updated and evaluated periodically.

Detailed provisions and procedures related to the preparation of action plans (recovery plans) and resolution plans (resolution plans) are regulated in separate regulations while still referring to the applicable provisions.

1. This General Policy on Risk Management is effective from the date it is stipulated.
2. General Policy on Risk Management must be implemented and adhered to by all levels of the Bank's organization.
3. General Policy on Risk Management is reviewed at least 1 (one) time in 1 (one) year.
4. The attachments contained in this General Policy are an inseparable part of the General Policy on Risk Management.
5. With the enactment of the General Policy on Risk Management, Board of Directors Regulation Number 14/PO/DIR/PPD/2018 dated 28 October 2018 concerning Risk Management Policy Guidelines is revoked and declared no longer valid.
6. With the implementation of the General Policy on Risk Management, all implementing regulations from the Board of Directors Regulation Number 14/PD/DIR/PPD/2018 dated 28 December 2018 concerning Risk Management Policy Guidelines are declared to still be valid as long as they do not conflict with this General Policy.
7. Matters that have not been regulated in this General Policy will be determined later by the Board of Directors

GENERAL POLICY	**RISK MANAGEMENT**	Number	KU.8
		Edition	1
		Revision to	0
		Effective Date	23 December 2022
		Replaced Date	-

VALIDITY SHEET
GENERAL POLICY REGARDING RISK MANAGEMENT

Stipulated in Jakarta, on 23 December 2022

PT BANK TABUNGAN NEGARA (Persero) Tbk

[Signed]	[Signed]
Haru Koesmahargoyo	Setio Wibowo
President Director	Director of Risk Management

Published in the Bank Announcement Gazette
Number : 11/XII/2023
Announced in : Jakarta
Dated : 23 December 2023
The copy is in conformance with the original
PT BANK TABUNGAN NEGARA (Persero) Tbk
POLICY AND PROCEDURE DIVISION

[Signed]	[Signed]
K. Esti Dwi Retnosari	Wandira Kusuma W
Division Head	Department Head