RISK MANAGEMENT FRAMEWORK
PT ASURANSI JIWA SINARMAS MSIG TBK

INTRODUCTION

All companies face risk, including PT Asuransi Jiwa Sinarmas MSIG Tbk (AJSM). Without risk, there is no reward. The flip side of this is that too much risk can lead to business failure arising from uncertainty and therefore impacting business objectives. Risk management allows a balance to be struck between taking risks and reducing them. As a result, the management of risk has evolved into an important driver for strategic decisions in support of business strategies, balancing the appropriate level of risk taken to the desired level of reward while maintaining a sound financial position and adequate capital. Furthermore, investors are more willing to invest in companies with good risk management practices.

Generally each of these standards and frameworks emphazise key elements of risk management such as:

- Risk is a reality for Share Holders and Company's Management regardless of the industry sector or size of the company.
- Well-run companies will have a comprehensive risk management framework in place to identify existing and potential risks and assess how to deal with them if they arise.
- Risk identification, measurement, mitigation, reporting and monitoring, and governance are the six key pieces of an effective framework.

The Framework is periodically reviewed and aligned to the business strategy and capital management objectives, in ensuring consistency in the management of risk within AJSM.

OBJECTIVE

The Risk Management Framework ("Framework") is intended to institutionalize vigilance and awareness of the management of risks across AJSM. It is not intended to be a substitute for common sense and sound judgment is to be exercised in the course of the assessment.

The primary objectives of the Framework are as follows:

- Provide a concise but holistic documentary standard as a single point of reference in providing direction for the management of all risks that AJSM is exposed to;
- Establish key risk principles that are fully integrated into the overall risk management structure, process and embedded in the day-to-day management of business;
- Facilitate effective RMC (Risk Management Committee) and ROC (Risk Oversight Committee) through a sound and clearly defined internal governance model, with clear structure of risk ownership and accountability;
- Enhance adequate risk awareness and culture across the governance structure and business processes.

REGULATORY COMPLIANCE

The Framework is subject to OJK Regulation Number 44/POJK.05/2020 is concerning Risk Management Implementation for Non-Bank Financial Institution and Number 4/POJK.05/2021 is concerning Risk Management Implementation within Information Technology.

OJK Regulation No. 44/POJK.05/2020	OJK Regulation No. 4/POJK.05/2021
Risk Management Implementation includes: a. Active supervision by the Board of Directors, Board of Commissioners, and Sharia Supervisory Board; b. Adequacy of Risk Management policies and procedures as well as stipulation of Risk limit; c. Adequacy of the process of Risk identification, measurement, control, and monitoring, as well as a Risk Management information system; and d. A comprehensive internal control system. Authorities and responsibilities of the Board of Directors at least consist of: a. Formulating Risk Management policies and strategies in writing and in a comprehensive manner; b. Responsible for the implementation of Risk Management policies and Risk exposure that are taken by LJKNB ("*Lembaga Jasa Keuangan Non-Bank*") in a comprehensive manner; c. Evaluating and deciding transactions and Risk limit that require the Board of Directors' approval; d. Developing Risk Management culture at every level of organization; e. Ensuring competency improvement for human resources that are related to Risk Management; f. Ensuring that the Risk Management function has operated independently; and g. Implementing a periodic review to ensure: (1) the accuracy of Risk assessment methodology; (2) the adequate implementation of the Risk Management information system; and (3) the accuracy of Risk Management policies and procedures as well as stipulation of Risk limit. Responsibilities of the Board of Directors for the implementation of Risk Management shall include: a. Evaluating and providing direction based on a report that is submitted by the Risk Management function; and b. Submission of accountability report to the Board of Commissioners and Sharia Supervisory Board at least 1 (one) time in 6 (six) months. Evaluation of the Board of Directors' accountability for the implementation of Risk Management shall at least be conducted 1 (one) time in 6 (six) months. In order to implement an effective Risk Management process and system LJKNB must establish: (a) a Risk Management committee; and (b) a Risk Management function. Authorities and responsibilities of the Risk Management committee shall provide a recommendation to the president director or equivalent, which at least contains: a. Formulation of policies, strategies, and guidelines for the application of Risk Management; b. Improvement or adjustment of the implementation of Risk Management based on the evaluation result of Risk Management application; and c. The stipulation of matters that are related to business decisions that deviate from the normal procedures.	Risk management implementation within Information Technology includes: a. Active supervision of the Board of Directors and the Board of Commissioners; b. The adequacy of policies and procedures for the use of Information Technology; c. The adequacy of the process of identification, measurement, control, and monitoring of risks of using Information Technology; and d. Internal control system for the use of Information Technology. The authorities and responsibilities of the Board of Directors within Information Technology at least include: a. Determine Information Technology development plans and NBFI (Non-Bank Financial Institution) policies related to the use of Information Technology; b. Establish policies and procedures related to the implementation of adequate Information Technology and communicate it effectively, both to the work unit of the organizer and to users of Information Technology; c. Ensure: (1) Information technology used by NBFIs can support the development of LKJNB business, the achievement of LKJNB business objectives and continuity of service to LKJNB consumers; (2) the adequacy and improvement of human resource competencies related to the implementation and use of Information Technology; (3) the availability of an information security management system that is effective and communicated to work unit of users and organizers of Information Technology; (4) the application of risk management processes in the use of Information Technology is carried out adequately and effectively; (5) Information Technology policies and procedures are applied effectively to the work units of Information Technology providers and users; (6) Performance measurement system for the implementation of Information Technology includes: a) support the monitoring process of the implementation of the development and procurement of Information Technology; b) support the completion of Information Technology development and procurement projects; c) optimizing the utilization of human resources and investment in Information Technology infrastructure; and d) improve the performance of the Information Technology implementation process and the quality of service delivery of the process results to Information Technology users. The authorities and responsibilities of the Board of Commissioners within Information Technology includes: a. Evaluate, direct, and monitor the Information Technology development plan and NBFI policies related to the use of Information Technology; and b. Evaluate the responsibility of the Board of Directors for the implementation of risk management in the use of Information Technology.

RISK MANAGEMENT BUILDING BLOCKS

The overall risk management processes are viewed in a structured and disciplined approach to align strategies, policies, processes, people and technology with the specific purpose of evaluating all risk types in line with enhancing shareholder value.

The Framework sets out seven key building blocks which serve as the foundations for risk management.

1. **Promote strong risk culture**
   - A corporate culture that is guided by strong risk management which supports and provides appropriate standards and incentives for professional and responsible behaviours must be established.
   - The risk culture is to be embedded in organization at all levels, reflected in the risk taking activities, roles and responsibilities, frameworks and policies. AJSM core values promote
   - The right risk culture as part of the overall corporate culture that is embraced at all levels.
   - In strengthening the risk culture, structured learning programmes should be established to maintain the desired direction towards risks and expected risk behaviour.

2. **Establish risk appetite & strategy**
   - The risk appetite articulates the nature, types and levels of risk within AJSM is willing to assume while taking a longer-term view that considers the institution's financial capacity, and continuing ability to meet obligations towards stakeholders (especially policyholders). It is to be established and approved by their respective Board.
   - The risk appetite should be reflective of the strategies and business objectives set, and reviewed on a continuous basis to ensure that it remains comprehensive, relevant and reflects any changes in the factors.
   - The risk appetite provides the basis for establishing risk tolerances / thresholds around specific risk areas, through qualitative and quantitative metrics.
   - Risk Tolerances should be effectively communicated and appropriately managed, monitored and escalated to the relevant stakeholders in the event of exceptions.

3. **Assign adequate capital**
   - Capital management is to be driven by strategic objectives and accounts for the relevant regulatory, economic and commercial environments.
   - To maintain a competitive edge and in support of business strategies, the capital management approach is to ensure adequate resources and efficient capital structure that commensurate with the level of risk of its business activities.

4. **Ensure proper governance and oversight function**
   - There should be a clear, effective and robust governance structure which includes the role of the Board with well defined, transparent and consistent.
   - The governance model should encapsulate the overall risk management structure.
   - Operational independence means that the Management cannot influence Independent Control Functions (Risk Management, Compliance or Internal Audit) when exercising their responsibilities. The Management is ultimately responsible to

decide how to react to the results, concerns and recommendations presented by the independent control functions. Each independent control function shall be able to communicate on its own initiative with any staff member and must have the necessary authority, resources, expertise and unrestricted access to all relevant information necessary to carry out its responsibilities.

5. **Establish adequate risk frameworks and policies**
   - Frameworks are to be developed to outline the guiding principles for the management of risks. This is supported by policies and procedures to ensure that risk management practices and processes are implemented effectively at all levels.
   - Policies and procedures are to be reviewed regularly to account for new businesses, regulatory guidelines, requirements and leading practices.
   - Policies and procedures should reflect the risk profile including material and potential risk exposures, operating environment and risk processes to guide businesses on day-to-day risk management.

6. **Establish risk management practices and processes**
   - Those should be reflective of the nature, size and complexity of the various business activities.
   - Robust processes should be in place to actively identify, measure, control, monitor and report risks inherent in all products and activities undertaken by the business.

7. **Ensure sufficient resources**
   - Resources and techniques should be available to appropriately support risk management practices and processes.

GOVERNANCE MODEL

The governance model aims to place accountability and ownership whilst facilitating an appropriate level of independence and segregation of duties between the three (3) lines of defence which include the risk taking units, risk control units and internal audit.

First Line of Defence – Risk Taking Unit

- Consist of business / front-line and support units with the ultimate responsibility to manage day-to-day risks inherent in its business, activities and risk exposures.
- Ensure that the business operates within the established strategies, risk tolerance, risk appetite, risk frameworks, policies and procedures.
- Business Units are responsible to ensure that AJSM does not suffer unpleasant surprises. They are responsible for managing any risk, as identified in the AJSM. They show exemplary behaviour in term of Risk Culture in their day-to –day activities.
- They are the first point and operationally responsible to ensure that AJSM does not suffer from unpleasant surprises. The Business Units are responsible for managing the full risk taxonomy that relates its execution of the business strategy and ranges from the Chief Executive Officer (CEO), Line Management and Business Managers to employees in the business lines. The first line of defence excels with robust risk culture and risk awareness all the way down into the deepest levels of organization.

Second Line of defence - Risk Control Units

- Consist of risk management and compliance functions providing an effective risk management and risk oversight and guidance over the effective operation of the internal control principles.
- Risk Management establishes risk frameworks, policies and procedures to identify, assess, control, mitigate, monitor and report all risk types which forms part of businesses day-to-day operations. Risk Management communicates risk strategies and creating risk awareness within the entire organization. Risk Management provides guidance in the implementation and execution of the established risk frameworks, policies and tools. This responsibility includes:
  - Coordinate the development and maintenance of internal risk policies.
  - Propose risk tolerances for each of the companies within AJSM for the respective Board for approval, and monitor the risk profile of the underlying company against the risk acceptance limits.
  - Organize reporting on risk-limits, risk-profile and any non-adherence, violations and / or breaches and inadequacies of current control procedures to those parties responsible and who need to know.
  - Monitor business units' utilization of and adherence to risk limits.
  - Support the development of specific tools and techniques to measure and manage the risks, and facilitate their implementation.
  - Promote risk management competence including facilitating development of technical risk management expertise and helping managers to align risk responses with the risk tolerances.
  - Facilitate and supports Risk Management and Risk Oversight Committees.
- Compliance ensures the financial institution's compliance to the applicable laws, regulations, internal policies and procedures. Its key responsibilities should include maintaining policies and procedures to detect and minimise risk of non-compliances and to assess the adequacy and effectiveness of such policies and procedures on an on-going basis. To this end, Compliance establishes compliance framework and

policies, provides advice and guidance on all areas of regulations, and surveillance over the effectiveness of the compliance controls embedded in the business.

Third Lines of Defence – Internal Audit

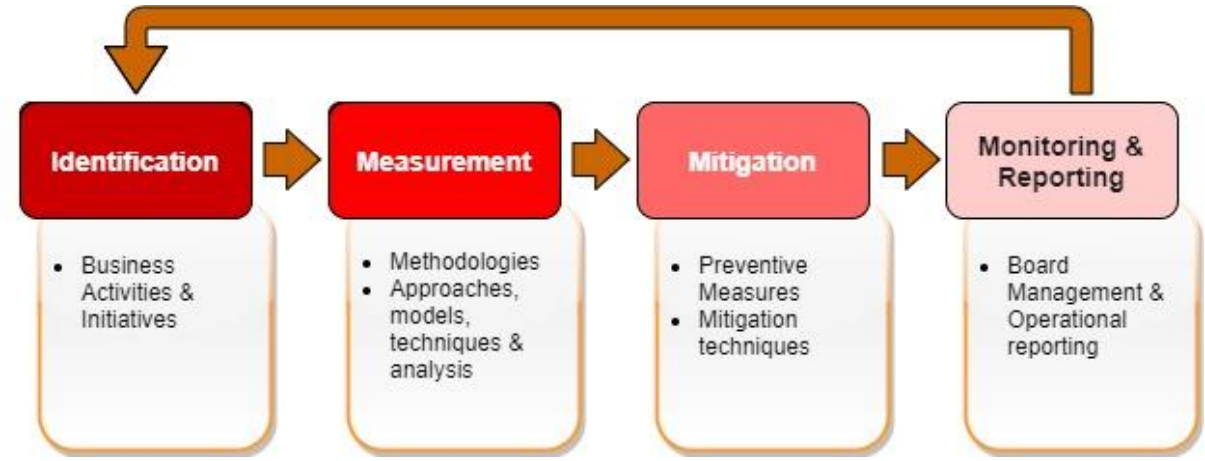
- Provide reasonable assurance via regular and independent assessment and validation that:
  - Risk management and compliance frameworks, policies and tools are sufficiently robust and consistent with regulatory standards.
  - Controls to mitigate risks are adequate and effectively executed by the Risk Taking Units.
  - Adequate oversight by the Risk Control Units over the Risk Taking Units.
- The internal auditors provide independent assurance of the effectiveness of the risk management approach and are the third line of defence.

RISK MANAGEMENT PRACTICE AND PROCESS

Risk management practices and processes are a fundamental component of the risk principles. It is essential in enabling systematic identification, measurement, controlling, monitoring and reporting of risk exposures.

To enable an effective execution of risk management practices and process, a common risk language is an imperative pre-requisite in facilitating a consistent and uniform approach in reference to risks across AJSM.

The four (4) main stages of the risk management process which form a continuous cycle are as follows:



1. Risk Identification
   Risk identification is the initial step in the risk management process. This firstly involves identifying and understanding the risks inherent in all products, businesses and operations.

   The definition of each cluster is provided below:
   a. Financial Risk

Risks of loss or adverse impact on earnings and/or capital that are related to the impact of investment concentration or movements in the financial markets

b. Operational Risk
   Loss that occurred from inadequate or failed internal process, people/system or external event.
c. Insurance Risk
   Risk of loss or of adverse change in the value of underwritten insurance liabilities, due to change in claims experience and the underlying assumptions on which pricing and reserving/claims estimations have been made.
d. Enterprise Risk
   Risks of loss or adverse impact arising from business/strategic, legal, compliance, and reputation risk.
   It covers external and internal factors that can impact the company ability to meet its current business plan for achieving ongoing growth and value creation.

With the objective of identification and understanding of risks, key risks and key risk indicators are identified to track the most important developments and actions. Where possible and necessary for aggregation and comparison, risk measures are made consistent across AJSM business activities.

2. Risk Measurement
   One of the main objectives of the risk management processes is to assess, measure, and manage risk in a consistent basis. In order to achieve this, risk measurement techniques should be developed across different dimensions of risk factors to ensure continual reassessment and identification of emerging risks.
   The use of models for identifying and measuring risk should be supported by robust processes for managing risk. Upon establishing the measurement methodology, AJSM has a primary responsibility to validate the relevant models used. The validation should encompass both quantitative and qualitative aspects of the risk models and is to be performed by a unit independent of the risk taking units.

3. Risk Mitigation
   With the identification and measurement of risk, there has to be proper control and mitigation of the identified risks. Consideration should be given to the impact of the chosen mitigation strategy on other risks (directly or indirectly), these should be explicitly considered and accounted for, to avoid giving rise to new unattended risks.

4. Risk Monitoring and Reporting
   Accurate, comprehensive, clear, informative and timely management information is fundamental for aggregating, monitoring and reporting of risk exposures and exceptions to Senior Management, Risk Management and Risk Oversight Committees on a regular basis.
   Data aggregation, monitoring and reporting process are essential in capturing existing exposures to facilitate early identification of emerging risks, prompt decision making and communication of mitigating strategies. As such, an effective data aggregation capabilities and forward looking reporting practices should be developed to provide

early warnings of any potential increases in risk exposures or breaches of risk limits that may exceed AJSM risk tolerance/appetite.

Communication should take place both horizontally and vertically to and from Senior Management with varying reporting frequency and granularity to facilitate effective decision making as highlighted below:

Reporting	Description
Board / Regulatory	• Summarises AJSM aggregate risk exposure. • Reporting for Financial Services Authority (OJK)
Management	• Reflects risk exposures.
Operational	• Detailed and granular reporting of risk exposure, compliance to policies, procedures, etc.