

Risk Management Framework 2026

Thaire Group Holdings Public Company Limited

Table of Contents

	Page
Risk Management Objectives	3
Risk Management Framework	4
Risk Management Infrastructure	5
Vision and Mission	5
Risk Appetite Framework	5
Enterprise Risk Management	7
Information Systems	8
Risk Governance Structure and Risk Management Culture	9
Risk Governance Structure	9
Management Support	14
Integration of Risk Management	15
Risk Awareness and Understanding Development	15
Scope of Risk Management	16
Types of Risk	16
Core Activity	17
Risk Management Process	18
Risk Identification	18
Risk Assessment	18
Risk Response	19
Risk Control and Monitoring	19
Risk Management Reporting	19

Risk Management Objectives

Thaire Group Holdings Public Company Limited (the “Company”) was established as an investment-focused entity in the non-life reinsurance business. This business plays a vital role in enhancing the country's capacity to retain risks domestically and in supporting the operations of non-life insurance companies as a strategic business partner.

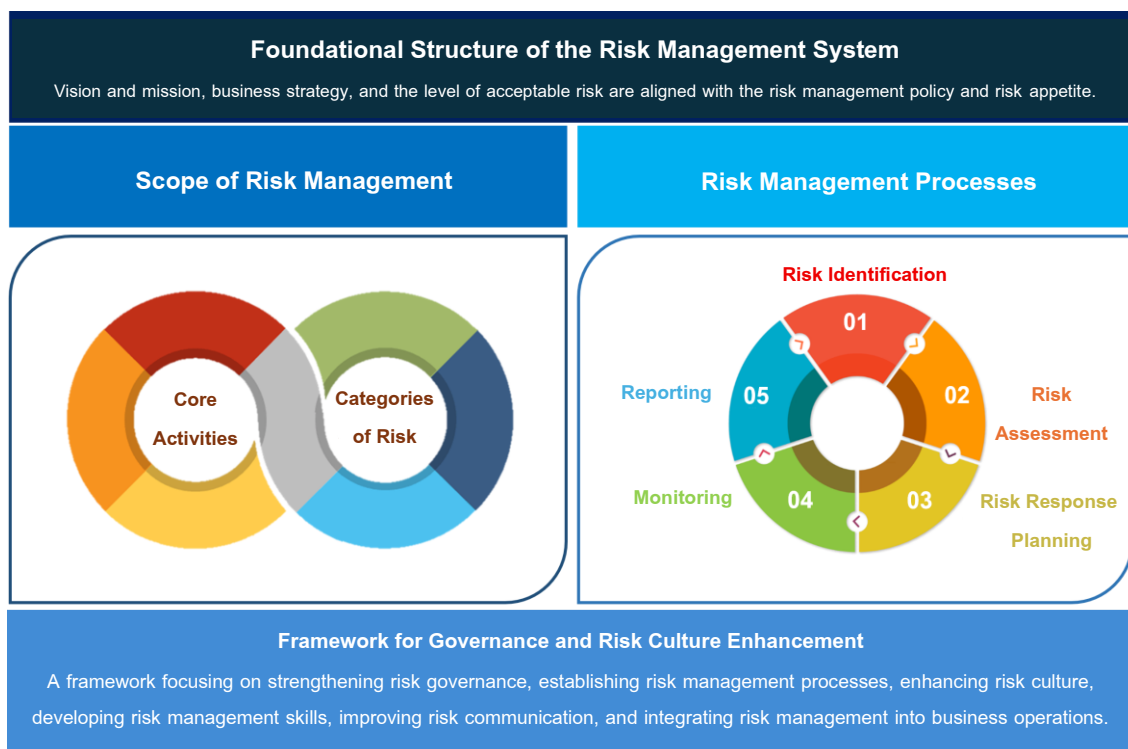
In pursuing the aforementioned objectives, the Company is confronted with both internal and external challenges arising from changes in social, political, economic, environmental, and technological factors, as well as the emergence of new and evolving risks. These developments have resulted in a business environment that differs significantly from the past and has introduced increased complexity, making it more difficult to predict future outcomes.

Accordingly, the Company must implement effective and efficient risk management practices to ensure the achievement of its vision and mission. Such practices also support the Company in meeting its operational targets, maintaining financial stability, safeguarding its reputation and corporate image, sustaining its competitive advantage, and appropriately responding to the expectations of its key stakeholders.

Risk Management Framework

The Company has established a Risk Management Framework as a guideline for integrated risk management across the organization. The Company's Risk Management Framework has been developed based on internationally recognized risk management standards, such as those issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), as well as rating agencies including Standard & Poor's, A.M. Best, and Fitch Ratings. In addition, it also takes into account relevant laws and regulatory requirements related to enterprise-wide risk management issued by supervisory authorities.

The Company's Risk Management Framework consists of four key components 1) Risk Management Infrastructure 2) Risk Governance Structure and Risk Management Culture 3) Scope of Risk Management 4) Risk Management Process



Part 1 – Risk Management Infrastructure

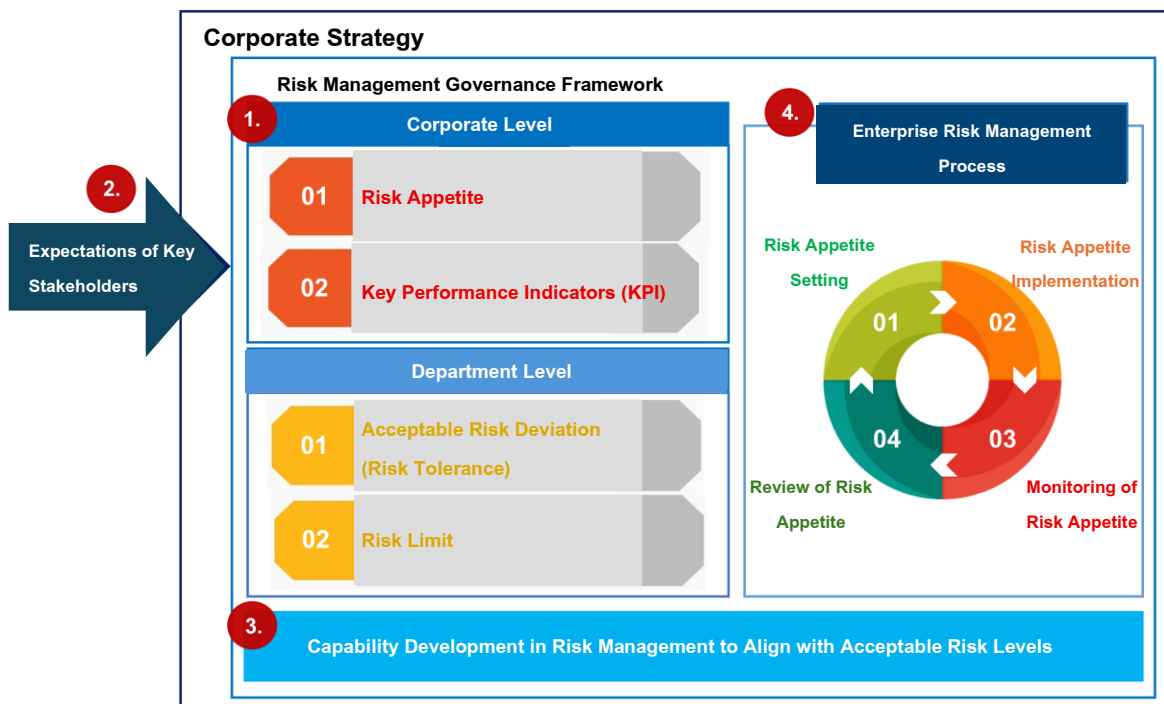
Risk management infrastructure relates to the fundamental factors that support the success of risk management. It consists of the following components:

Vision and Mission

Vision and mission define the direction and objectives, as well as the scope of operations and what the Company aims to achieve in the future. The Company establishes its strategies, objectives, and operational plans to ensure the achievement of its vision and mission. It also conducts analysis and assessment of both internal and external environments to identify key risks, defines risk indicators, establishes risk management measures, and continuously monitors risk management performance. This enables the Company to effectively manage its key organizational risks within an acceptable level.

Risk Appetite Framework

The Company has established a Risk Appetite Framework, with the Board of Directors and management responsible for defining the direction for its development. This framework serves as a guideline for internal operations within the organization. The Company's Risk Appetite Framework integrates corporate strategy, capital adequacy, and risk management to enable a comprehensive view of the organization's overall risk profile. It incorporates the concepts of risk management and capital management into operational practices, continuously analyzes changes in risk exposures, and manages risks to remain within acceptable levels.



In developing the Risk Appetite Framework, the Company considers the following factors:

1. Stakeholder Interests – The Company takes into account the diverse needs of its key stakeholders and consolidates them to determine an appropriate level of risk appetite. This ensures a balanced alignment among strategy, capital, and associated risks.
2. Risk Appetite and Risk Tolerance – The needs of key stakeholders, together with the Company's strategy and business plans, are used to define corporate-level and departmental performance indicators. These, in turn, guide the establishment of appropriate and aligned risk appetite levels and acceptable deviation ranges for each key risk.
3. Required Capabilities – To manage risks within acceptable levels, the Company must establish risk management policies and relevant operational guidelines. It must define risk appetite levels, risk tolerance ranges, key risk indicators, and risk limits, as well as continuously monitor and measure these metrics. The Company also communicates the risk appetite to relevant parties to ensure a common understanding and establishes escalation mechanisms in cases where risk appetite levels or tolerance thresholds are breached.
4. Risk Appetite Management Process – The risk appetite management process consists of: 1) defining the Company's risk appetite 2) using the risk appetite as a framework for business operations 3) monitoring compliance with or breaches of the risk appetite; and 4) reviewing the risk appetite periodically.

Risk Appetite refers to the overall level of risk that the Company is willing to accept in order to achieve its mission, vision, objectives, and business goals. The Company defines its overall risk appetite with Board approval. Senior management, the Risk Management Committee, risk owners, and relevant departments then use this risk appetite as a framework for operations and for managing key risks.

The risk appetite serves as a benchmark for determining which activities and operations are acceptable to the organization. It also supports decision-making regarding capital allocation and other available resources, enabling the Company to achieve its objectives while managing risks within acceptable boundaries.

The Company also defines Risk Tolerance, which represents a more granular level of risk derived from the overall risk appetite for each key risk. Risk tolerance is used as an operational boundary to achieve desired outcomes. In addition, the Company uses Key Risk Indicators (KRIs) to monitor the status, trends, and changes in key risks. Furthermore, the Company establishes Risk Limits, which are thresholds set for KRIs to help ensure that risks remain within the defined tolerance ranges and overall risk appetite.

If any activity or operation involves risks that exceed the Company's risk appetite, the Company shall present the potential breach to the Board of Directors for consideration and approval of any necessary additional actions. This also includes evaluating the need to review and adjust the Company's risk appetite to ensure it remains appropriate in response to the evolving risk landscape.

Enterprise Risk Management

The Company must establish a Risk Management Policy approved by the Board of Directors to serve as a guideline for implementing risk management in a manner that is appropriate and aligned with the Company's strategy and risk appetite, thereby ensuring effective risk management across all departments within the organization. In addition, the Company must develop a Risk Appetite Framework to serve as a basis for business operations and organizational decision-making.

The Company's risk management must integrate risk management, capital management, and business planning to achieve defined objectives and to ensure that organizational risks are maintained within acceptable levels. The Company shall analyze its strategies and business plans to identify and assess key risks that the Company currently faces and may face in the future, and concurrently establish appropriate risk management measures for such key risks. The process of risk analysis, assessment, and the establishment of mitigation measures shall be conducted in accordance with the risk management process defined in the Company's Risk Management Framework.

The Company must establish Risk Management Policies covering its key business activities and all significant risk types inherent in its operations and processes. These include: 1) Strategic Risk 2) Operational Risk 3) Market Risk 4) Credit Risk 5) Liquidity Risk 6) Reputational Risk 7) Information Technology Risk 8) Emerging Risk 9) Group Business Risk

The Company shall maintain a risk register to monitor and report on the status of key risks and compliance with the Risk Management Policy. The risk register must include information on risks, risk causes, risk categories, risk owners, key risk indicators, risk limits, current risk mitigation measures, and potential future risk management actions.

In addition, the Company must conduct business continuity analysis, including stress testing at intervals consistent with its business plans and risk appetite. This is to ensure the Company's financial stability and the effectiveness and efficiency of its risk management measures. Stress testing shall be conducted at least annually, or when events occur that may significantly impact the Company's financial stability or overall risk profile. If the results of such stress tests indicate a breach of risk appetite, the Company must present action plans and report the findings to the Risk Management Committee for acknowledgment.

The Company must establish a risk governance structure and clearly define the roles and responsibilities of relevant parties. All executives and employees are required to comply with the policies, frameworks, and guidelines set forth in this policy, and to participate in risk management in accordance with their assigned roles and responsibilities. Furthermore, they are expected to contribute

to fostering a risk management culture, ensuring that risk management becomes an integral part of the daily operations of all executives and employees across the organization.

Information System

The collection of high-quality data and statistics is a fundamental component of effective risk management, as such data and statistics form a valuable database for analysis and decision-making. The Company's information systems must be developed efficiently to ensure that the data collected for analysis and decision-making—used to support business operations and risk management across each unit is complete, accurate, up to date, readily available, secure, and suitable for an evolving environment.

The Company's information systems must support enterprise risk management and be reliable, appropriate, and aligned with the size, nature, and complexity of the business operations, as well as future business plans. The systems must also include data backup and recovery mechanisms in the event of emergencies. Furthermore, the Company must establish measures to manage risks related to data and information systems, including defining access rights for relevant personnel and enforcing such measures strictly.

The Company must take into account risks arising from the use of information technology in business operations, including compliance with personal data protection laws and cybersecurity requirements, as these may affect systems, operational processes, and the Company's reputation. The Company must strictly implement the established risk management measures to ensure that such risks are managed within acceptable levels.

Part 2 – Risk Governance Structure and Risk Management Culture

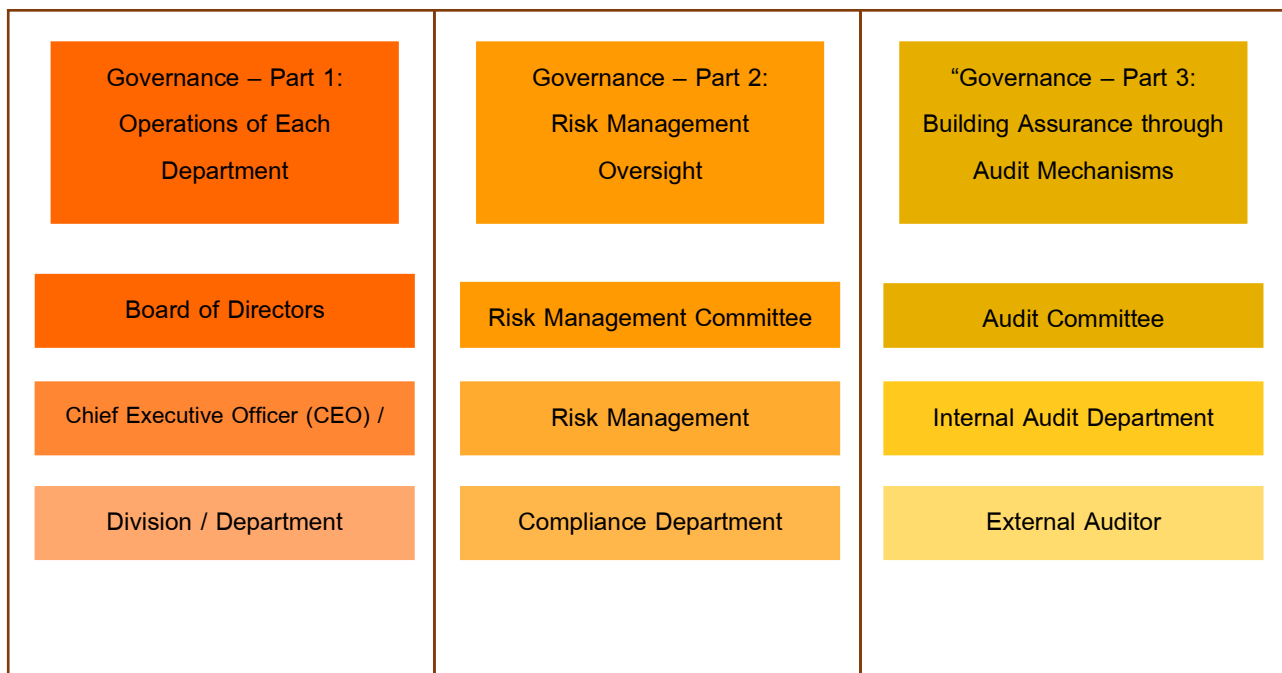
The Company must establish an appropriate governance structure to ensure a system of checks and balances within the organization, and to guarantee that the Company's risk management is integrated, efficient, and effective. The Company's management must place importance on fostering a risk management culture within the organization by encouraging and promoting all employees to develop awareness and actively participate in managing risks related to their respective responsibilities. Risk management must be embedded as an integral part of employees' daily work practices.

Risk Governance Structure

The Company's risk governance structure is based on the Three Lines of Defense principle. The first line of defense involves risk management within the operational functions of each business unit, which operates under the oversight of the Board of Directors, the Chief Executive Officer, and senior management.

The second line of defense is responsible for overseeing the effectiveness and efficiency of enterprise-wide risk management, carried out by the Risk Management Committee, the Risk Management Function, and the Compliance Function.

The third line of defense provides independent assurance on the effectiveness of risk management through audit mechanisms, consisting of the Audit Committee, the Internal Audit Function, and external auditors.



First Line of Defense – Risk Management in Operational Functions of Each Business Unit

Board of Directors

The Board of Directors has the following responsibilities:

1. Establish business strategies that are aligned with the Company's risk management framework, policies, and risk appetite.
2. Review and approve the Company's risk management framework and policies, business strategies and plans, and risk appetite levels.
3. Oversee the Company in the following areas:
 - * Ensuring that the Company's risk management is maintained within the defined risk appetite.
 - * Reviewing summarized risk status reports, which have been filtered by the Risk Management Committee, and submitting them to the Board of Directors for consideration at least on a quarterly basis.
 - * Reviewing the risk management framework and policies at least annually, and whenever significant events occur that may materially impact the Company's financial stability.
 - * Maintaining the Company's capital at a stable and sufficient level to appropriately support both current and future business operations.
 - * Supporting the operations of the Risk Management Committee and the Risk Management Function to ensure they can perform their duties effectively and completely, with adequate allocation of resources.

Chief Executive Officer and Management

The Chief Executive Officer and management have the following responsibilities:

1. Define the direction for the development of the Risk Appetite Framework.
2. Be responsible for overseeing daily business operations in alignment with the business strategy, risk management framework, and risk management policies.
3. Ensure that employees are educated on the risk management framework and policies, and confirm that such knowledge is effectively applied in their actual work practices.

Departments / Business Units

Departments or business units have the following responsibilities:

1. Act as the owners of the risks within their respective units.
2. Integrate strategy, risk management, and capital management into their operations, and ensure that risks within their units are maintained within the defined risk appetite.
3. Continuously review and improve risk management measures to ensure they remain appropriate and up to date.

Second Line of Defense – Oversight of the Effectiveness and Efficiency of Enterprise-wide Risk Management

Risk Management Committee

The Company shall establish a Risk Management Committee consisting of at least five members, appropriately sized to align with the scale, nature, and complexity of the Company's operations, in accordance with the following criteria:

1. Members must be appointed by resolution of the Board of Directors or the shareholders' meeting to serve as Risk Management Committee members.
2. At least one member of the Risk Management Committee must also be a member of the Board of Directors.
3. Other members of the Risk Management Committee may include members of the Board of Directors, executives of the Company, or qualified individuals with knowledge and understanding of the risks associated with the Company's business operations.

The Risk Management Committee has the following responsibilities:

1. Establish the risk management framework and policies and propose them to the Board of Directors for approval, ensuring that they appropriately cover key risks.
2. Oversee the Company's overall risk management and ensure that the Company operates in accordance with the risk management framework and policies.
3. Hold regular meetings at least quarterly to monitor the Company's risk status and changes in risk exposures, follow up on risk management progress, and provide recommendations for additional actions to ensure alignment with the Company's risk management framework, policies, and risk appetite, and report to the Board of Directors at least quarterly.
4. Assess the adequacy, efficiency, and effectiveness of the Company's risk management, and review the appropriateness of the risk management framework and policies at least annually, or when significant events occur that may materially affect the Company's financial stability.
5. Ensure that the Company's risk management is conducted in compliance with regulatory requirements and good practices prescribed by supervisory authorities and other relevant organizations.
6. Perform any other duties as assigned by the Board of Directors.

Risk Management Function

The Risk Management Function has the following responsibilities and/or shall ensure the implementation of the following:

1. Support the Board of Directors, the Risk Management Committee, and management on matters related to the Company's risk management.
2. Identify key risks currently faced by the Company as well as those that may arise in the future.

3. Assess, consolidate, and monitor risks, and assist internal units in managing risks to ensure that they remain within the Company's defined risk appetite.
4. Develop a forward-looking risk assessment approach by continuously evaluating both internal and external risk environments to identify and assess risks that may arise in a timely manner.
5. Conduct scenario analysis and stress testing in accordance with the risk management framework and policies.
6. Prepare risk status reports identifying risks faced by the Company and compliance with risk management policies, and present such reports to the Board of Directors and management.
7. Prepare documentation and reports on significant changes affecting the risk management framework and policies, and present them to the Risk Management Committee to ensure ongoing implementation and continuous improvement.
8. Perform other activities necessary to ensure that the Company maintains its overall risk profile within acceptable levels at both the Company and group levels.
9. Conduct self-assessments of performance quality and monitor necessary improvements to enhance the effectiveness of the Risk Management Function.

Head of Risk Management Function

The Company shall appoint a Head of Risk Management who possesses the knowledge, understanding, and skills necessary for managing risks associated with the Company's insurance business operations, and who has full access to relevant information sources.

The Head of Risk Management has the following responsibilities:

1. Ensure that risk management results are reported to the Risk Management Committee and management on a regular basis, at least quarterly, including at a minimum:
 - * Reporting on activities related to enterprise-wide risk management, including changes in the risk management framework, risk management policies, and business plans;
 - * Providing evidence of monitoring processes for key risks from the risk register.
2. Ensure that risk management results are reported to review the adequacy of the risk management framework and policies to the Risk Management Committee at least annually, or when events occur that may significantly affect the Company's financial stability or overall risk profile.

Compliance Function

The Compliance Function has the following responsibilities:

1. Serve as a central unit for providing guidance and consultation on legal and regulatory compliance, including preparing written compliance manuals and conducting regular training for employees.
2. Develop a compliance risk management system by identifying risks, assessing risks, determining mitigation measures, monitoring, and reporting on changes in compliance risk, including causes of

non-compliance and corrective actions, as well as resolved issues, and present such reports to management, relevant sub-committees, or the Board of Directors.

3. Coordinate with relevant departments to prepare and implement annual compliance risk management plans, including resolving issues that may lead to non-compliance.
4. Monitor compliance with laws and regulations, and report annual compliance results to the Board of Directors or relevant oversight sub-committees, including reporting legal violations, investigations of management, and any penalties or legal actions imposed by regulatory or governmental authorities.
5. Act as the Company's liaison with regulatory authorities and perform specialized duties, including anti-money laundering (AML) and counter-terrorism financing (CTF) functions.
6. Promote and maintain an ethical corporate culture that emphasizes responsible conduct and compliance with internal and external obligations.
7. Identify, assess, report, and comply with key laws, regulations, and regulatory obligations, including risks associated with such compliance.
8. Ensure that appropriate monitoring systems, policies, procedures, and controls are in place for key legal, regulatory, and ethical requirements.
9. Provide regular training on key laws and regulations to employees in high-responsibility positions or those involved in high-risk activities.
10. Coordinate and support confidential reporting processes to prevent data leakage and ensure regulatory reporting requirements are fulfilled.
11. Oversee, monitor deficiencies and violations of compliance, and ensure appropriate disciplinary actions are taken and required reports are submitted to regulatory authorities.
12. Conduct self-assessments of the Company's compliance monitoring processes and follow up on necessary improvements to enhance the effectiveness of the Compliance Function.

Third Line of Defense – Assurance of Risk Management Effectiveness through Audit Mechanisms

Audit Committee

The Audit Committee is responsible for reviewing and assessing whether the Company has an appropriate, effective, and robust internal control system, internal audit system, and risk management system, in accordance with internationally recognized frameworks and applicable regulatory requirements.

Internal Audit Function

The Internal Audit Function has the following responsibilities:

1. Evaluate whether the Company has adequate, efficient, and effective internal control systems to manage risks within acceptable levels and in line with good corporate governance practices.

2. Assess whether internal units comply with applicable laws and regulations relevant to the Company's business operations.
3. Evaluate the efficiency and effectiveness of the risk management system in accordance with the risk management framework and policies approved by the Board of Directors.
4. Review and assess risks related to fraud, errors, omissions, and other irregularities, as well as the adequacy of related mitigation measures.
5. Establish, implement, and maintain a risk-based audit plan (Risk-Based Audit Plan).
6. Monitor and assess the adequacy and effectiveness of policies, procedures, documentation, and operational controls at both the Company and group levels.
7. Evaluate the reliability, accuracy, completeness, and effectiveness of information management processes, including methods used to identify, measure, classify, and report data used within the Company.
8. Monitor and assess the performance of Company units and communicate significant findings to relevant units for improvement.
9. Coordinate with external auditors to enhance audit efficiency and reduce duplication of audit activities.
10. Evaluate the quality of external auditors' work (if applicable).
11. Summarize and report annual internal audit results, which are reviewed by the Audit Committee or the Board of Directors at least annually.

External Auditors

External auditors are responsible for reporting findings related to risks, control deficiencies, and weaknesses in corporate governance (if identified) to the Audit Committee at least annually.

Management Support (Tone at the Top)

Support from senior management is a critical factor in the success of risk management. Such support helps ensure that risk management is effectively implemented across the Company and elevates its importance. Management must lead by example in risk management and continuously promote a risk-aware culture within the organization. A lack of management support may result in insufficient awareness, low engagement, and reduced understanding among personnel, making it difficult to establish a strong risk management culture.

Management must define the direction, policies, and practices for risk management and communicate the objectives and benefits of risk management to all employees to foster awareness and appreciation of its importance.

Risk Management Integration

The Company must integrate risk management into business decision-making, capital maintenance, corporate governance, and internal control processes. This is to ensure that existing organizational risks are systematically managed and that business decisions consider both risks and expected returns simultaneously.

The Company must estimate the required capital for conducting its business, assess the quality and accessibility of its financial resources, consider limitations on capital increases, and establish mechanisms to control the ability to raise capital in urgent situations. Furthermore, the Company must perform business continuity analyses by defining the factors used for appropriate scenario testing.

The Company must develop management action plans resulting from business continuity analyses in cases where the scenario testing outcomes exceed the Company's acceptable risk levels. In addition, the Company must prepare a Business Continuity Plan (BCP) to address events that may disrupt the Company's ability to conduct daily operations in a continuous and normal manner.

Risk Management Awareness

The Company must provide training and development for its personnel to ensure knowledge, understanding, vigilance, and awareness of risks that may affect departments/units, the organization, and stakeholders. The Company must also promote the exchange of risk information among different departments/units within the organization to ensure that risks are managed within acceptable levels.

The Company must instill a culture where all decisions consider the associated risks, costs, and expected benefits simultaneously.

Section 3 – Scope of Risk Management

The scope of the Company's risk management must cover the following risks and core activities:

Types of Risk

The Company's risk management encompasses the following nine types of risks:

1. Strategic Risk

Refers to risks arising from the implementation of policies, formulation of strategic plans, operational plans, and their execution, which may be inappropriate or misaligned with internal factors and the external environment.

2. Operational Risk

Refers to risks arising from inadequate governance or control related to internal processes, personnel, systems, information technology systems, data governance, information security, or external events.

3. Market Risk

Refers to risks arising from changes in interest rates, foreign exchange rates, asset prices, money and capital market instrument prices, and commodity prices.

4. Credit Risk

Refers to risks arising from counterparties' inability to fulfill their agreed obligations to the Company, including the possibility of counterparties being downgraded in credit rating.

5. Liquidity Risk

Refers to risks arising from the Company's inability to meet its liabilities and obligations when due, due to an inability to convert assets into cash, or the need to raise funds at an unacceptably high cost.

6. Reputation Risk

Refers to risks resulting from damage to the Company due to reputational deterioration, caused by negative perceptions from customers, business partners, shareholders, and/or regulators.

7. Information Technology Risk

Refers to risks that may arise from the use of information technology in business operations, which may affect the Company's reputation, systems, or operations, including risks arising from cyber threats.

8. Emerging Risk

Refers to new or emerging risks that may result in previously unforeseen losses, which are difficult to estimate in terms of both likelihood and impact, due to changes in environmental factors such as political, legal, social, technological, physical environment, and natural changes.

9. Group Risk

Refers to risks that the Company may be adversely affected by events (both financial and non-financial) arising from entities within the same business group. This also includes risks arising from the financial stability of the entire group or individual entities within the group that are impacted by events affecting one business within the group, whether such events originate internally within the group or externally impacting the group as a whole.

Core Activity

The Company's risk management must comprehensively cover all relevant core activities.

Section 4 – Risk Management Process

The Company must implement the risk management process, which consists of the following steps:

1. Risk Identification

The Company must identify potential risks that may arise from both internal and external sources, which may impact the Company's reputation, strategy, operations, and the achievement of its objectives, in both financial and non-financial aspects, and may alter the Company's overall risk profile.

In identifying risks, the Company must also determine the relevant root causes and the potential impacts of such risks in various dimensions, such as reputational impact, financial impact (capital, revenue, profit, and liquidity), operational impact (business interruption), and human resource impact.

The Risk Management Department is responsible for facilitating risk identification using appropriate techniques, such as conducting questionnaires to gather opinions from executives, utilizing internal company data to support decision-making, using external data to understand the conditions and trends of emerging risks, and organizing meetings to brainstorm and consolidate opinions.

The Risk Management Department is responsible for presenting the summary of key risk identification results to the Risk Management Committee for consideration in prioritizing and summarizing the Company's key risks on an annual basis. The Risk Management Committee shall determine the Risk Owners responsible for managing each key risk to remain within acceptable levels and within acceptable deviation ranges for each risk.

2. Risk Assessment

After identifying the Company's key risks, Risk Owners must assess the risks by continuously evaluating the likelihood and/or impact of such risks on the Company.

Risk Owners are responsible for proposing acceptable deviation ranges and establishing appropriate risk indicators and risk limits that are consistent with the acceptable risk levels and acceptable deviation ranges. The approved acceptable deviation ranges, risk indicators, and risk limits—endorsed by the Risk Management Committee—shall be used to monitor the status and changes of the Company's key risks at appropriate intervals.

3. Risk Response

The Company must respond to risks in a manner consistent with the established acceptable risk levels, acceptable deviation ranges, and risk limits. Risk Owners are responsible for assessing the effectiveness and efficiency of current risk management measures, both in the short term and the long term.

The Company's risk response should focus on identifying ways to prevent the root causes of risks. However, if preventive measures are insufficient or if unforeseen events occur beyond control that result in undesirable risks, Risk Owners should respond using existing mitigation measures and consider additional risk management measures to be implemented in the future, along with defined completion timelines. This is to ensure that risks can ultimately be managed within acceptable levels.

4. Risk Control and Monitoring

The Company must control and monitor risk management performance to ensure that risk responses are implemented as planned and that key risks are managed within acceptable levels.

Given that both internal and external environments are constantly changing, existing risks may evolve or new types of risks may emerge. Advances in knowledge, techniques, and technology may also introduce more effective risk management approaches. Therefore, the Company must continuously monitor risks, regularly review key risks that may impact the organization in the future, and proactively prepare methods and mitigation measures in advance. In addition, the Company must periodically review and improve risk management measures, risk indicators, and risk limits to ensure that they remain appropriate in line with changing circumstances.

5. Risk Reporting

The Company shall establish a reporting system for risk management information and risk status as follows:

No.	Report	Requirements	Reporting Information
1	Risk management reports covering risk status, risk indicators, and the efficiency and effectiveness of risk management measures.	At least once a year	Management and the Risk Management Committee
2	Reports on significant events that may materially affect the Company's financial stability (if any)	At least once a year	Management and the Risk Management Committee
3	Summary of risk status reports and summary of compliance with the risk management policy.	At least once a year	Board of Directors
4	Risk management reports to support the review of the adequacy of the risk management framework and the risk management policy.	At least once a year	Management and the Risk Management Committee
5	Summary of the annual audit assessment results,	At least once per year	The Audit Committee

No.	Report	Requirements	Reporting Information
	prepared by the Internal Audit Department.		and the Board of Directors