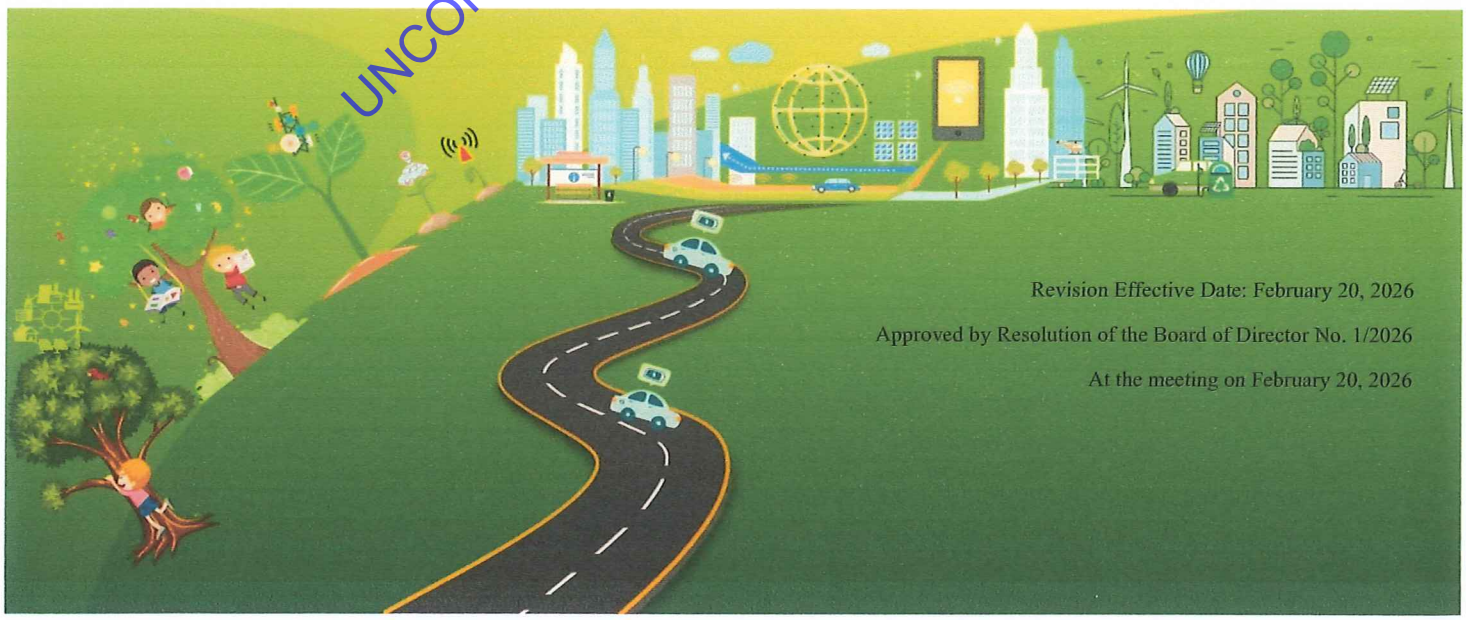
Risk Management Policy

ALT Telecom Public Company Limited and Affiliated Companies



Revision Effective Date: February 20, 2026

Approved by Resolution of the Board of Director No. 1/2026

At the meeting on February 20, 2026

ALT Telecom Public Company Limited and affiliated companies

Table of Contents

ALT Telecom Public Company Limited and affiliated companies

ALT Telecom Public Company Limited and affiliated companies

1. Background

The Board of Directors recognizes and highly values the importance of risk management. Consequently, a Risk Management Committee has been established, consisting of independent directors and senior executives from various departments who possess knowledge and understanding of the company's operations. This committee is responsible for overseeing and managing risks at both the organizational and departmental levels, ensuring comprehensive and effective risk governance.

The Risk Management Committee has established the fundamental framework for risk management by adopting the principles of enterprise risk management based on the standards of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the ISO 31000 "Risk Management - Principles and Guidelines." These frameworks and methodologies are applied to manage risks within an acceptable level to achieve the company's objectives, strategies, mission, and vision as determined by the Board of Directors.

This risk management manual includes content related to the definition, key components of risk management, risk management guidelines, risk management policies, risk management structure, roles and responsibilities under the risk management framework, as well as risk management processes and business continuity management. It serves as a guideline for risk-owning departments, providing them with tools to help all areas of the company achieve their objectives and goals, ultimately contributing to the creation of added value and the sustainable growth of the organization.

2. Principles and Objectives

Risk management constitutes an essential element of good corporate governance. It not only facilitates the organization's achievement of its strategic objectives but also enhances value creation for stakeholders by fostering long-term sustainability and aligning with their interests. Therefore, the company has implemented the Enterprise Risk Management – Integrated Framework (COSO ERM) to develop its risk management system. This ensures that executives, managers, and employees share a common understanding of risks and recognize the importance of risk management at all organizational levels. The goal is to foster shared responsibility and ensure that operations are aligned efficiently and effectively.

The Risk Management Policy has been established with the following objectives:

1. To provide guidelines for executives, managers, and employees to integrate risk management principles into their operations, supporting the organization's strategic goals.
2. To create a structured framework that enables the organization to systematically respond to events that may impact risk, ensuring standardization and establishing the foundation for long-term risk prevention.

3. To enhance risk management knowledge among executives, managers, and employees, fostering a sustainable risk management culture within the organization.
4. To strengthen awareness and understanding of risk management objectives, ensuring collaboration across all levels to enhance stakeholder satisfaction and increase organizational value. This approach aligns with Good Corporate Governance (GCG) principles and regulatory requirements.

3. Risk Management Planning Guidelines

To ensure that risk management is effective and aligned with the organization's objectives, the Board of Directors has established the following policies, operational guidelines, and risk management plans:

1. Focus on managing risks that may impact organizational goals, policies, and fraud risks that could affect the company's reputation and image.
2. Control and manage risks within an acceptable level while encouraging employee participation in the risk management process.
3. Promote awareness among employees regarding potential risks and enable them to prevent or mitigate adverse impacts effectively.
4. Continuously monitor, track, and assess risks, considering both internal and external environmental factors.
5. Foster a corporate culture that prioritizes risk management to support sustainable growth.
6. Prevent and combat fraud at all organizational levels to enhance transparency and corporate governance.

Current Risk Management Practices

The company applies various tools and approaches in risk management, including:

- Good Corporate Governance (GCG): Ensuring ethical business conduct and compliance with governance standards.
- Performance Evaluation Systems & Key Performance Indicators (KPIs): Measuring and assessing operational effectiveness.
- Quality Standards (e.g., ISO): Ensuring operations comply with established guidelines and industry standards.

ALT Telecom Public Company Limited and affiliated companies

Key Principles for Risk Management Planning

1) Alignment with the Organization's Operations and Environment: Risk management plans must be tailored to the company's nature, scope, and environmental changes to ensure consistency with policies, strategies, and business plans.
2) Compliance with Regulatory Standards: Risk management must align with legal requirements, regulatory guidelines, and best practices established by governing bodies.
3) Annual Review and Continuous Improvement: The risk management plan must be reviewed at least once a year or immediately following significant events that may impact organizational objectives to ensure its effectiveness and adaptability.

4. Risk Management Structure

The company's risk management framework involves personnel at all levels, from general employees to the Board of Directors. The structure ensures a comprehensive approach to risk management, with clearly defined responsibilities and oversight mechanisms.

5. Roles and Responsibilities

Based on the risk management structure, the roles and responsibilities of each department are defined as follows:

Department	Roles and Responsibilities
Board of Directors	The Board of Directors assumes a critical responsibility in approving and providing oversight of the organization's risk management framework. It ensures the effective implementation of risk management plans through the Risk Management Committee. 1. Strategic Oversight – Define the organization's strategies and policies while ensuring continuous risk analysis and management. 2. Risk Awareness & Culture – Promote awareness at all levels and encourage an organization-wide risk management process, embedding it into the corporate culture. 3. Training & Support – Ensure that employees receive the necessary knowledge and training on risk management. 4. Risk Management Review – Assess risk management reports and ensure that the risk mitigation measures are sufficient, appropriate, and consistently applied within an acceptable level. 5. System Improvement & Monitoring – Continuously review and enhance the company's risk management system, regularly evaluating and aligning it with organizational policies. 6. Decision-Making & Advisory – Provide recommendations and make key decisions regarding critical risk management issues. 7. Reporting – Present the performance and findings of the Risk Management Committee to the Board of Directors at least once a year for acknowledgment and/or further consideration.
Risk Management Committee	1. Comply with the Charter of the Risk Management Committee.
Chief Risk Officer (CRO)	1. Assume overall responsibility for the development, implementation, and maintenance of the Enterprise Risk Management (ERM) framework.

	2. Assess organizational risk management needs and establish, implement, and maintain appropriate risk management processes and systems. 3. Foster a strong risk and compliance culture, and support management in understanding and taking meaningful ownership of risk management and regulatory compliance. 4. Regularly review and align risk management processes with the organization's core strategies to ensure enterprise-wide integration and momentum, while maintaining an appropriate balance among cost efficiency, operational effectiveness, and performance outcomes. 5. Establish and strengthen a robust risk culture throughout the organization. 6. Provide coaching, guidance, and proactive support across the organization to ensure effective implementation of the risk management framework. 7. Collaborate with senior management to promote and embed a sustainable risk management culture. 8. Identify and report to the Managing Director significant risks and emerging risks arising from business units or identified through strategic risk assessments. 9. Ensure that the risk management framework remains fit for purpose and aligned with organizational objectives. 10. Review and assess the risk implications and potential impacts associated with business planning initiatives. 11. Monitor changes in business operations and industry developments, including emerging trends and contemporary knowledge, that may pose risks to the organization.
Risk Management Committee Secretary	1. Risk Data Collection – Gather risk-related information and risk management reports from various departments and present them to the Risk Management Committee for review. 2. Risk Management Reporting – Prepare and submit risk management reports to the Risk Management Committee, ensuring accuracy, completeness, and alignment with organizational policies.

ALT Telecom Public Company Limited and affiliated companies

Department	Roles and Responsibilities
Quality Management Department	1. Coordination & Advisory – Provide guidance and support to different departments in analyzing, assessing, and managing risks according to the company's risk management approach. 2. Monitoring & Review – Track the effectiveness of risk management practices in each department, issuing reminders to risk owners to ensure continuous risk management and periodic reviews.
Internal Audit Unit	1. Review & Assessment – Evaluate the effectiveness and efficiency of internal controls and risk management processes to ensure that the organization has an adequate and appropriate internal control system for managing risks within a controllable level. 2. Audit Follow-up – Monitor audit results and ensure that the audited units implement the recommended improvements to enhance operational efficiency, effectiveness, and cost savings.
Departments/Units	1. Risk Analysis & Reporting – Identify and assess risks specific to each department/unit and report them to supervisors regularly. 2. Compliance & Implementation – Ensure that operations within the department/unit adhere to risk management policies and strategies while maintaining an effective risk management system. 3. Daily Risk Monitoring – Ensure that daily operations include adequate risk assessment, management, and reporting. 4. Risk Awareness Promotion – Encourage staff within the department/unit to recognize the importance of risk management. 5. Execution of Risk Management Plans – Ensure that risk management plans are fully implemented and followed through.

ALT Telecom Public Company Limited and affiliated companies

6. Definitions

Enterprise-Wide Risk Management (ERM) refers to risk management that integrates both internal and external risk factors affecting an organization. Internal factors include organizational structure, operational processes, personnel, and corporate culture, while external factors encompass politics, competitors, and economic conditions. Key characteristics of ERM include:

- Integration into Business Operations – Risk management should align with business plans, objectives, and decision-making, ensuring it integrates with other aspects of corporate management.
- Comprehensive Risk Consideration – Covers both corporate-level risks (Corporate Risk) and functional-level risks (Functional Risk), including strategic and policy risks, operational risks, financial risks, legal and regulatory risks, and information technology risks. These risks may lead to damage, uncertainty, or opportunities that impact organizational goals and stakeholders' expectations.
- Future Risk Identification – Organizations must anticipate potential risks and evaluate their impact on objectives, enabling proactive risk management strategies.
- Key Risk Indicators (KRIs) and Risk Monitoring Systems – The implementation of Key Risk Indicators (KRIs) and Risk Dashboards ensures effective tracking and reporting of significant risk factors. These indicators help measure and identify potential threats, serving as early warning signals that foster a risk-aware culture across the organization.
- Three Lines of Defense Approach – Defines accountability for enterprise risk management at three levels:
    1. First Line – Business units that directly encounter and manage risks.
    2. Second Line – Risk management and compliance functions that support the first line in managing risks.
    3. Third Line – Internal audit units responsible for evaluating the adequacy of risk control measures, under the oversight of external auditors and regulatory bodies.
- Organization-Wide Support and Participation – ERM requires engagement from all levels of the organization, including the board of directors, executives, and employees, to ensure effective risk management practices and a strong risk-aware culture.

ALT Telecom Public Company Limited and affiliated companies

Technical term	Definitions
Risk	Uncertain events may occur and negatively impact the achievement of objectives and goals.
Inherent Risk	The level of risk that exists before any controls or management measures are implemented.
Residual Risk	The level of risk that remains after control or management measures have been implemented.
Likelihood	The likelihood or probability of an event occurring.
Impact/Consequence	The impact of an event, both financial and non-financial.
Risk Identification	Risk identification is the process of determining which risk factors may impact the objectives.
Risk Owner	Risk owners or individuals directly exposed to risks have the ability to manage and mitigate risk levels.
Risk Criteria	Risk Levels/Categories
Degree Of Acceptance	Risk tolerance levels.
Risk Matrix	A 2D chart of size 5*5 consisting of the impact axis and the likelihood of the occurrence axis. Each axis is divided into 5 levels of severity, with the objective of displaying the risk level.
Risk Profile	A group (set) of risks that shows the various risks that may affect the objectives of different departments, including information that indicates the characteristics of the risks, the types of risks, the potential impacts from those risks, and other related information. These can be displayed using a Risk Map.

ALT Telecom Public Company Limited and affiliated companies

Technical term	Definitions
Risk Appetite	The overall level of risk that the organization is willing to accept in order to achieve its mission or vision.
Risk Tolerance	The level of deviation that the organization is willing to accept from the criteria or performance indicators related to achieving its objectives.
KRIs (Key Risk Indicators)	Quantitative risk indicators, activities, or events that signal changes in significant risks impacting objectives. These indicators can be used in risk management to track whether the risk management results align with the goals. If necessary, adjustments can be made to improve or modify the risk management plan for greater efficiency. In cases where the indicators serve as leading indicators, they can be utilized to develop a risk management plan with an early warning system.
Risk Factor	A risk factor refers to something that arises from an event or the details of an event that helps identify what causes the risk.

7. The key elements in risk management

The company has adopted COSO-ERM 2017 (Enterprise Risk Management-Integrating with Strategy and Performance), which categorizes the components of the organization's risk management process into 5 principles and 20 components. These are:

1. Governance and Culture
2. Strategy & Objective Setting
3. Performance
4. Review & Revision
5. Information, Communication & Reporting

These serve as the framework for the company's risk management to ensure that business operations align with the sustainable development goals.

ALT Telecom Public Company Limited and affiliated companies

Source: Committee of Sponsoring Organizations of the Trading Commission (COSO)

Principle 1: Governance and Culture

1. Establishes Board Risk Oversight

The board of directors is responsible for overseeing the execution of various strategies and governance. This includes assigning specific roles and responsibilities for risk management, ensuring members possess the knowledge and expertise required, maintaining independence, and avoiding conflicts of interest.

2. Establishes Operating Structures

The organization should establish an operational structure that aligns with business strategies and objectives. This includes defining an appropriate organizational structure, command hierarchy, and risk management processes. It also involves clearly defining authority, duties, and responsibilities in line with business strategies.

3. Defines Desired Culture

The organization should define desired behaviors that reflect the intended corporate culture. Both the board and management should establish this culture for the organization and its employees, ensuring that it emphasizes risk awareness. Corporate culture is shaped by internal factors like decision-making autonomy, communication among employees, management standards, workplace layout, and compensation systems, as well as external factors like legal requirements and stakeholder expectations.

4. Demonstrates Commitment to Core Values

The organization should demonstrate commitment to adhering to core values, such as integrating risk management into the corporate culture, strictly following responsibilities, fostering accountability, and ensuring appropriate communication.

5. Attracts, Develops, and Retains Capable Individuals

The organization should support the development of human resources aligned with business strategies and objectives. This includes providing risk management training, enhancing employee skills, and offering appropriate incentives and benefits for roles at all levels.

Principle 2: Strategy and Objective-Setting

Risk management should be integrated with the organization's strategic planning process. The organization should define its risk appetite to align with its strategy and business objectives. Business objectives determine the approach to strategies, including operational activities and priorities for identifying, assessing, and responding to risks. Principle 2 has four components:

6. Analyzes Business Context

The organization should consider the potential impact of business operations on overall risk levels. This includes understanding the business context and considering external environments and stakeholders.

7. Defines Risk Appetite

The organization should define its risk appetite to create, sustain, and promote awareness of its values. This involves setting acceptable levels of risk and communicating them clearly. Risk appetite is not standardized and will vary between organizations based on their unique business contexts.

8. Evaluates Alternative Strategies

The organization should assess alternative strategies and their potential impacts on the organization's risk profile. This includes conducting SWOT analysis, valuation assessments, revenue forecasting, competitor analysis, and scenario planning. Strategies must support the organization's mission, vision, core values, and acceptable risk appetite.

9. Formulates Business Objectives

When formulating business objectives, the organization should consider risks at different levels that align with and support strategies. This includes determining acceptable risk deviations based on performance, while staying within the defined risk appetite.

Principle 3: Performance

This principle starts with identifying and assessing risks that may impact the ability to achieve business strategies and objectives. Risks are prioritized based on their likelihood and potential impact, considering the organization's risk tolerance. The organization then selects various risk responses and assesses the overall risk exposure, making necessary adjustments to improve performance and develop a comprehensive view of the risks that may affect the achievement of strategic goals. There are five components in this principle:

10. Identifies Risk

The organization should identify risks that affect its strategies and business objectives, including strategic, operational,

financial, and compliance risks. All identified risks should be documented in a risk profile for further management.

11. Assesses Severity of Risk

The organization should assess the severity of risks by evaluating their likelihood and the potential impact on the organization if they occur.

12. Prioritizes Risks

The organization should calculate the level of risk exposure and prioritize risks. This prioritization helps determine the response strategy. Risk level is calculated by multiplying the likelihood and potential impact of each risk to prioritize and make decisions on which risks to address first.

13. Implements Risk Responses

The organization should implement appropriate responses to mitigate risks, based on the severity and priority of each risk.

14. Develops Portfolio View

The organization should develop and evaluate risk in the context of the entire organization. Tools like Risk Maps or Risk Matrices are commonly used to visualize and manage risks.

Principle 4: Review and Revision

Organizations should periodically review their risk management processes, assess their risk management capabilities, and consider improvements to enhance value. This is especially important in response to significant changes in the organization or external environment. There are three components in this principle:

15. Assesses Substantial Change

The organization should identify and assess substantial internal and external changes that could impact business strategies and objectives, such as the departure of senior management, mergers and acquisitions, rapid technological changes, regulatory shifts, or pandemics.

16. Reviews Risk and Performance

The organization should review its performance and risk management outcomes regularly. This includes assessing whether business objectives are being met, evaluating the accuracy of risk assessments, ensuring that the risk level aligns with organizational goals, and identifying any emerging risks that may impact the organization.

17. Pursues Improvement in Enterprise Risk Management

The organization should continually improve its risk management processes, especially during periods of significant change, such as organizational restructuring or changes in external environments that impact risk management systems.

Principle 5: Information, Communication, and Reporting

Communication is an ongoing process of gathering and sharing necessary information across the organization. Management uses relevant information from both internal and external sources, supporting enterprise-wide risk management.

ALT Telecom Public Company Limited and affiliated companies

The organization leverages information systems to collect, process, and manage risk-related data, and reports on risks, organizational culture, and performance. This principle includes three components:

18. Leverages Information Systems

The organization should ensure that sufficient, appropriate, and timely information is available. It can use processes like big data analytics to identify relationships and patterns within data, leading to better risk identification and management.

19. Communicates Risk Information

The organization should communicate risk information through various channels, using both top-down and bottom-up approaches. Risk communication should be sufficient both internally and externally.

20. Reports on Risk, Culture, and Performance

The organization should report on risks, organizational culture, and performance at all levels across the organization. Even when the responsibility for reporting is delegated to specific departments or individuals, management remains responsible for overseeing the reporting process.

8. Risk Management Process (COSO ERM Framework)

8.1 Risk Management Concepts

The diagram of the risk management process according to the COSO ERM standard outlines the essential elements in establishing a risk management framework and ensuring the organization achieves its objectives. The process includes the following components:

ALT Telecom Public Company Limited and affiliated companies

- Internal Environment

  The internal environment is a crucial component in defining the risk management framework. It sets the foundation for the organization's risk management direction. This includes several aspects such as organizational culture, management policies, employee practices, work processes, and information systems.

- Objective Setting

  The organization must define objectives that align with its strategic goals and risk tolerance to ensure a clear and appropriate risk management approach. These objectives guide the organization's risk management strategy.

- Event Identification

  This involves gathering potential events that could affect the organization, considering both internal and external risk factors. Events that occur can hinder the achievement of objectives. These risks could be related to management policies, human resources, operations, finance, information systems, or regulations. Identifying these events helps in understanding the potential risks, allowing management to determine strategies and policies for managing them.

- Risk Assessment

  Risk assessment involves evaluating the severity of risks by assessing the likelihood of occurrence and the potential impact. The evaluation considers both financial impacts (e.g., revenue loss) and non-financial impacts (e.g., strategic failure, operational disruption, or human resource losses such as employee turnover or loss of key personnel). This assessment helps prioritize risks.

- Risk Response

  After identifying and assessing risks, the organization must respond by minimizing the likelihood of these risks occurring or reducing their impact to an acceptable level. This is done by selecting the most appropriate and cost-effective risk management strategies.

- Control Activities

  Control activities involve setting up actions and procedures to mitigate or manage risks. These activities help ensure that risks are managed properly, enabling the organization to achieve its objectives while reducing risk to an acceptable level.

- Information and Communication

  An effective information system and communication process are essential for managing risks. This serves as the foundation for considering and implementing risk management activities based on the framework set by the organization.

- Monitoring

  Continuous monitoring is necessary to assess whether the risk management actions are effective and whether the

risks are being managed efficiently. Monitoring helps determine if adjustments are needed to ensure optimal risk management. These eight components form a comprehensive approach to risk management, ensuring that organizations can identify, assess, respond to, and control risks effectively, while continuously improving their risk management practices.

8.2 Types of Risks

The classification of organizational risks is divided as follows:

8.2.1 Risks from Internal Factors:

- Strategic Risk (S): This is the risk arising from the formulation of inappropriate strategies or policies, which result in the organization failing to achieve its objectives or increase its value. Examples include errors in setting vision or strategic plans, organizational structure changes, and the improper implementation of strategic plans. It also includes misalignment between policies, goals, strategies, organizational structures, competitive conditions, resources, and external environments such as economic, political, social conditions, competition, technology, and legal factors impacting the organization's objectives or goals.
- Operational Risk (O): This risk arises from daily operational processes, including the lack of proper supervision or internal controls, personnel, work systems, equipment, information technology, work environment, and asset safety, which may affect the efficiency and effectiveness of the organization. Examples include ineffective human resource management, workplace safety issues, errors in operations, unexpected disasters, and inefficient document and transaction management.
- Financial Risk (F): This is the risk related to liquidity, financial management, and financial statements. It results from the lack of planning, analysis, and financial control, which affects the financial stability of the organization. Examples include liquidity issues, inefficient budget management, financial reporting errors, and risks from market fluctuations (Market Risk) and the risk of counterparties failing to meet obligations (Credit Risk), as well as risks from interest rate and exchange rate fluctuations.
- Corruption Risk: This refers to the risk of corruption, embezzlement, misappropriation, or acceptance/transfer of organizational or external benefits for personal gain.

8.2.2 Risks from External Factors:

- Compliance Risk (C): This is the risk arising from non-compliance with laws, regulations, or relevant standards. Examples include violations of laws applicable to the organization, policies or practices that cannot be effectively

implemented, products or services not meeting standards, risk from breach of contract obligations, and failure to report according to regulations or legal compliance.

- Emerging Risk: This refers to a risk that has not yet manifested but may emerge in the future due to changes in the environment. This type of risk is typically slow to materialize, difficult to identify, and has a low frequency of occurrence but may have significant impacts when it does. Emerging risks often arise from changes in political, legal, social, technological, environmental, or natural conditions. For example, risks from nanotechnology, climate change, or pandemics.
- Business Interruption Risk: This refers to situations where the business has to halt temporarily for repairs or corrections due to damage to assets from cyber threats, information technology, natural disasters, political protests, pandemics, or other disruptions.
- Environmental Risk: This refers to the risk that causes negative environmental impacts resulting from the organization's operations.
- Risks of Climate Change: Global warming is a significant cause of climate change, affecting natural resources (e.g., water, soil, ecosystems, biodiversity, small coastal areas, and islands) and the livelihoods of rural communities (e.g., food security and health) at various levels. The larger and more widespread the changes, the more severe the impact. Climate change also affects agriculture in many ways, such as increased carbon dioxide levels, changing atmospheric moisture and rainfall patterns, and other climate interactions.
- IT Risk: This refers to risks related to the use of digital technology and information systems in operations, which may impact the organization. Examples include risks from digital transformation (the organization failing to adapt to technological changes, losing competitive advantage), cybersecurity risks (attacks from external intruders that could harm or damage networks or databases), lack of an IT strategy, inappropriate technology choices, system security breaches, and IT system failures affecting operations.

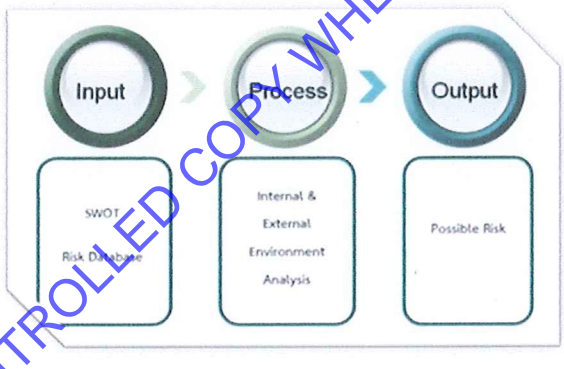
8.3 Risk Management Process

The risk management process must be carried out continuously within the organization and should be integrated into regular business activities. This enables the organization to execute its defined strategies, leading to the achievement of its mission and objectives. The risk management process consists of seven main steps as follows:

8.3.1 Risk Identification and Risk Analysis

Risk identification is the first step in the risk management process, which helps the organization analyze and understand the factors that may impact its operations and objectives. This is divided into three main parts:

- Input: The data used for analysis includes SWOT Analysis and a Risk Database. SWOT is used to analyze the organization's strengths, weaknesses, opportunities, and threats. The Risk Database contains historical risk data that serves as a reference for future risk management.
- Process: Analyze both internal and external environments of the organization. The internal environment includes factors like organizational structure, policies, organizational culture, and management practices. The external environment includes factors such as economic conditions, market competition, legal changes, and technological developments.
- Output: The result of this process is the identification of Possible Risks, which are the potential risks that could affect the organization. This information will be used for further risk management actions



Risk Factor Identification Process

The main steps of the risk factor identification process are as follows:

8.3.1.1 Analysis of Internal and External Environments

- Internal Factors: These include organizational policies, organizational structure, organizational culture, resources, competitiveness, and work processes.
- External Factors: These include economic conditions, legal changes, business competition, domestic and international politics, market characteristics, the ability of competitors, technological advancements, and social factors.

8.3.1.2 Defining Organizational Objectives

Identifying strategic objectives and goals of the organization, considering the linkage between objectives and potential risks. The organization's objectives must be consistent throughout the organization to ensure that departments, executives, managers, and employees work in the same direction to achieve the organization's goals.

- Vision is the starting point for setting the organization's direction. Senior executives define organizational objectives through the annual planning process. Each department must align its objectives with the organization's primary goals. When defining objectives for various projects or processes, the linkage with the department's and organization's objectives must be considered. Organizational objectives may involve various aspects such as:
  - Resources (personnel, budget, equipment)
  - Information technology (data management, information systems)
  - Operational performance (efficiency, effectiveness, process quality)

8.3.1.3 Risk Data Collection

- Data collection methods such as interviews, workshops, surveys, or historical data analysis are used.
- Feedback from stakeholders such as employees, partners, and customers are also gathered.

8.3.1.4 Analyzing Business Processes and Key Activities

- Each business process is reviewed to identify risk points.
- Consider which risk factors may affect the success of the process.

8.3.1.5 Categorizing and Classifying Risks

Categorize the risks according to the types specified in section 8.2.

8.3.1.6 Documenting and Reporting Risks

- Create documents or databases specifying details of the risk factors, including their sources and risk trends.
- Prepare reports for executives and relevant parties to use as data for managing risks.

8.3.2 Evaluation of Internal Control Adequacy and Developing Internal Control Improvement Measures (Internal Control & Existing Plan)

8.3.3 Risk Assessment

Risk assessment is a process that involves analysis, evaluation, and risk ranking based on the impact on achieving the organization's operational objectives. The company has defined risk assessment criteria, including the likelihood of a risk occurring and the severity of its impact. These criteria can be both quantitative and qualitative, used as a basis for evaluating

various risks. Reference is made to Appendix G for evaluating fraud or corruption risks, which are identified, assessed, and reviewed according to Appendix C, and to raise awareness of risks that could impact the organization's objectives and operations. Risk assessments must comply with the company's anti-corruption policy.

8.3.4 Risk Prioritization

Risk prioritization involves creating a Risk Profile based on the likelihood of risk occurrence and its impact. The risk profile defines the acceptable risk level (Risk Appetite Boundary), as referenced in Appendix K.

Risk Level = (Likelihood of Event Occurrence) × (Impact of Event Occurrence)

8.3.5 Developing a Risk Mitigation Plan

Employees directly involved in the risk management process are responsible for managing risks based on their assignments. The risk management plan is presented at an executive meeting for consideration and approval of resource allocation (if needed). In selecting the best risk management approach, factors such as acceptable risk (Risk Tolerance), cost-benefit analysis, legal and regulatory requirements, and social responsibilities must be considered.

Risk management strategies include:

- Risk Acceptance (Take): When the benefits and returns from the risky activity outweigh the costs of personnel, resources, and budget, the organization accepts the risk, increasing controls to minimize the risk as much as possible.
- Risk Control (Reduce) (Treat): Additional risk control activities are implemented to ensure the risk is reduced to an acceptable level. This may include reducing the likelihood of the risk event or the severity of its impact.
- Risk Avoidance (Terminate): A different operational approach is chosen to avoid the risk event, while still achieving the original operational goals.
- Risk Transfer (Transfer): Responsibility for the risk is transferred to another party or organization, relieving the business of direct responsibility for the risk, but not eliminating it.

8.3.6 Information and Communication

The company recognizes the importance of risk management and ensures that its employees are informed about the organization's risk management policies. These are communicated through the company's website (alt.co.th), Google Sites, training sessions, or hands-on workshops.

8.3.7 Monitoring and Evaluation

Monitoring and reporting activities are used to track and review the risk management plan, ensuring its effectiveness and appropriateness. If the plan is found to be insufficient, adjustments should be made. Key data for monitoring and the

frequency of reviews should be set, and risk assessments should occur at least annually or whenever significant changes occur. to evaluate whether risks are within acceptable levels or if new risks have emerged.

Monitoring Results

Monitoring is generally conducted by management and internal personnel of the organization. However, external parties such as consultants or independent experts may also assist in monitoring risk management on occasion. Risks and their management may change over time. A risk management strategy that was previously effective might become inappropriate, control activities may become less effective or unnecessary, or there may be changes in objectives or processes. Therefore, management should regularly evaluate the risk management process to ensure its continued effectiveness.

Key Characteristics of Risk Monitoring:

- Effective Assessment – The evaluation should assess the effectiveness and continuity of control activities and other activities used to manage risks.
- Establishing Acceptable Risk Levels – Define acceptable risk levels that are appropriate and consistent with the business strategy.
- Accurate and Timely Data Collection – Collect and document data completely, accurately, and on time.
- Consistent and Transparent Communication – Communicate regularly and transparently about risks and processes, both formally and informally.
- Defining Key Risk Indicators (KRIs) – Set Key Risk Indicators (KRIs) that reflect the root causes of risks to monitor the organization's internal control systems and the status of risks in each risk category. This helps departments plan for appropriate and effective risk management and enables timely prevention and control of damaging events.

  A good risk indicator should not only reflect past risks (Lagging Indicators) but also can indicate or predict potential future risks (Forward-Looking/Leading Indicators).

This will take effect from February 20, 2026, onwards.

Mrs. Preeyaporn Tangpaosak

President

ALT Telecom Public Company Limited

ALT Telecom Public Company Limited and affiliated companies

Appendices

Appendix A: Criteria for Business Risk Assessment

Table A-1: Assessment of Positive Risks and Stakeholder Needs: ALT GROUP

❖ The level of likelihood of a risk occurring (Likelihood) is defined into 5 levels.

Likelihood	Level	Probability / Likelihood
Very high	5	● The chance of worsening significantly without promotional activities.
High	4	● The chance of worsening if there are no promotional activities.
Medium	3	● The chance of change is low, whether there are promotional activities or not.
Low	2	● The chance of improvement, but promotional activities are needed.
Very low	1	● The chance of continuous improvement without any actions being taken.

❖ Severity of Impact is categorized into 5 levels.

Impact	Level	Impact/Consequence
Very high	5	● There is a very high impact that cannot be controlled.
High	4	● There is a high impact, but it can be controlled (with difficulty)
Medium	3	● There is a medium impact, but it can be controlled.
Low	2	● There is a low impact, and it can be easily controlled.
Very low	1	● There is a very low impact or no direct impact.

ALT Telecom Public Company Limited and affiliated companies

Table G-2: Negative Risk Assessment - ALT GROUP

❖ Likelihood of Risk Occurrence (Likelihood) - Defined in 5 Levels

Likelihood of Occurrence	Level	Probability of Occurrence	Actual Event Status	Possibility of Misconduct Occurrence
Very high	5	Probability of occurrence is more than 75% or once per month or more.	The event has occurred, has been reported, and is currently under investigation.	Very likely to occur if no control measures are in place.
High	4	Probability of occurrence is 51-75% or every 2-6 months, but no more than 5 times.	The event has occurred and is being managed.	Likely to occur if no control measures are in place.
Medium	3	Probability of occurrence is 26-50% or once every 1-2 years.	The event has occurred and has been addressed.	Possible to occur if no control measures are in place.
Low	2	Probability of occurrence is 10-25% or once every 2-4 years.	The root cause of the event is being resolved.	Unlikely to occur even if no control measures are in place.
Very low	1	Probability of occurrence is less than 10% or once every 5 years.	The root cause of the event has been fully resolved (possibility of recurrence is reduced).	Very unlikely to occur even if no control measures are in place.

ALT Telecom Public Company Limited and affiliated companies

❖ Impact Severity Levels (Impact) - Defined in 5 Levels

1. Impact on Policy / Quantitative / Financial Aspects

Impact	Level	Impact/Result	Company
Very high	5	● Financial damage exceeds 20% of the financial target.	All group
High	4	● Financial damage exceeds 10-20% of the financial target.	All group
Medium	3	● Financial damage exceeds 5-10% of the financial target.	All group
Low	2	● Financial damage exceeds 3-5% of the financial target.	All group
Very low	1	● Financial damage is less than 3% of the financial target.	All group

2. Impact on Operations/Performance

Impact	Level	Impact/Result	Company
Very high	5	● Unable to execute the project.	ALT, GTS, IH, IG
		● Unable to produce/deliver work.	INN, EMAX
		● Unable to conduct testing.	LAB 17025
High	4	● Project success rate is less than 50% of the plan.	ALT, GTS, IH, IG
		● Production/delivery success rate is less than 70% of the plan.	INN, EMAX

ALT Telecom Public Company Limited and affiliated companies

Impact	Level	Impact/Result	Company
		• Unable to confirm test results.	LAB 17025
Medium	3	• Project success rate is between 50-69% of the plan.	ALT, GTS, IH, IG
		• Production/delivery success rate is between 70-79% of the plan.	INN, EMAX
		• Significant impact on some test results.	LAB 17025
Low	2	• Project success rate is between 70-89% of the plan.	ALT, GTS, IH, IG
		• Production/delivery success rate is between 80-89% of the plan.	INN, EMAX
		• Minor impact on some test results.	LAB 17025
Very low	1	• Risks commonly encountered in normal business operations.	All group

3. Legal Impact

Impact	Level	Impact/Result
Very high	5	Investigation, criminal prosecution, claims for damages, and/or an order to suspend any transactions.
High	4	Investigation, potentially including criminal prosecution and/or significant claims for damages.
Medium	3	Major lawsuits, including significant fines or claims for damages.
Low	2	Lawsuits with minor fines or damages.
Very low	1	Non-compliance with regulations or rules without significant impact.

4. Impact on Reputation/Corporate Image

Impact	Level	Impact/Result
Very high	5	• Severe damage to the company's image and reputation. • Significant impact on business objectives and strategy.
High	4	• Major damage to the company's image and reputation. • Strong impact on business objectives and strategy.
Medium	3	• Moderate damage to the company's image and reputation. • Moderate impact on business objectives and strategy.
Low	2	• Minor damage to the company's image and reputation. • Low impact on business objectives and strategy.
Very low	1	• Risks commonly encountered in normal business operations.

ALT Telecom Public Company Limited and affiliated companies

Appendix B: Fraud Risk Assessment Criteria

Table B-1: Fraud Risk Assessment – ALT GROUP

Levels of Likelihood of Risk Occurrence (Likelihood) are Defined in 5 Levels

Likelihood	Level	Frequency of Occurrence	Probability of Misconduct
Very high	5	Once per year	Events that are certain or regularly occur in every business operation.
High	4	Once every 2 years	Events that are highly likely or commonly occur in most business operations.
Medium	3	Once every 3-5 years	Events that are possible or may occur occasionally in business operations.
Low	2	Once every 5-7 years	Events that are very unlikely to occur in business operations.
Very low	1	Once every 7-10 years	Events that are highly improbable in business operations.

ALT Telecom Public Company Limited and affiliated companies

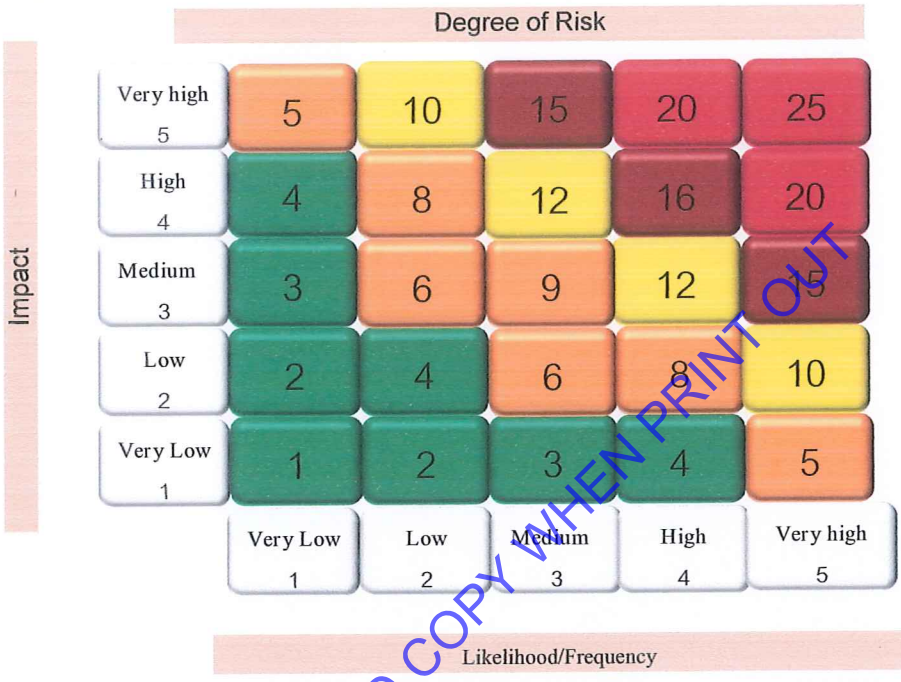
Severity Levels of Impact (Impact) – Defined in 5 Levels

Likelihood	Level	Reputation & Image	Financial Impact	Legal Impact	Customer/ Shareholder Impact
Very high	5	Company is blacklisted; severely negative corporate governance reputation	>30% of revenue	Business contracts/licenses revoked; senior executives imprisoned	Lawsuits filed by shareholders/ customers for damages
High	4	Continuous media coverage, growing public attention	Between >20% and 30% of revenue	Investigation initiated, potential criminal prosecution, and/or significant damage claims	Board and executives required to explain and justify actions
Medium	3	Corruption-related cases involving the company reported on social media	Between >10% and 20% of revenue	Company may need to provide evidence and clarification if regulatory authorities investigate	Complaints filed by customers/ shareholders to the board
Low	2	Rumors potentially implicating company personnel or the organization	Between >5% and 10% of revenue	Minor violations that may result in warnings or insignificant fines	Questions raised through various channels about transparency concerns
Very low	1	Almost no negative media coverage	≤5% of revenue	Minor non-compliance with insignificant regulatory impact	Nearly nonexistent

ALT Telecom Public Company Limited and affiliated companies

Appendix C: Risk Assessment Levels (Risk Map)

Degree of Ris



Level	Score Range	Color Indicator	Description
1	1-4	Very low	"Low/Very Low Level" – No risk management required.
2	5-9	Low	"Acceptable Level" – Controls must be in place to prevent risk from escalating to an unacceptable level.
3	10-14	Medium	"Moderate Level" – Acceptable but efforts should be made to reduce the risk to a more acceptable level.
4	15-19	High	"High Level" – Unacceptable, risk must be managed to bring it to an acceptable level.
5	20-25	Very high	"Very High Level" – Unacceptable, urgent risk management actions are required to reduce it to an acceptable level.

ALT Telecom Public Company Limited and affiliated companies

Status of Revisions and Updates

Revision No.	Effective Date	Details of the Revision
00	16/07/2015	New document
01	27/02/2017	Annual review
02	26/02/2018	Annual review
03	26/06/2019	Annual review
04	23/02/2021	Annual review
05	23/02/2022	Annual review
06	09/05/2023	Appendix B revised
07	25/02/2025	Full document revision
08	20/02/2026	- Section 4: Risk Governance Structure - Section 5: Roles and Responsibilities of the Risk Management Committee and the Chief Risk Officer (CRO)