Risk Management Policy

ALT Telecom Public Company Limited and affiliated companies

evision effective date: February 23, **2022**
Approved by Resolution of the Board of Directors **No. 1/2565**
At the meeting on February 23, **2022**

Revision/Update Status

Revision:	Effective Date	Revision Details
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

Risk Management Policy

ALT Telecom Public Company Limited and affiliated companies

Table of Contents

1. Background

The Board of Directors is aware of and highly appreciates the importance of risk management. Therefore, a Risk Management Committee has been set up, composed of independent directors and senior management of each department who understand the company's operation. To jointly manage risks at both the corporate and the agency level and to supervise the management of corporate risks thoughtfully and thoroughly.

The Risk Management Committee has laid the foundations for risk management by applying corporate risk management elements in accordance with the standards of the Committee of Sponsoring Organization of the Tredway Commission: COSO, Operational Framework, and Risk Management Procedures in accordance with ISO 31000 "Risk Management - Principles and Guidelines" to risk management to an appropriate or acceptable level to achieve the objectives, strategy, and vision set by the Committee.

This risk management manual contains content on the definition of risk management elements, risk management practices, risk management policies, risk management structures, responsibilities according to risk management structures, risk management frameworks and processes, business continuity management to be used by the risk management entity as a management approach, which is a tool that helps all sectors of the company to achieve objectives/goals and achieve operational success, leading to the creation of added value and sustainable growth of the organization.

2. Definition

2.1 Definition of risk management

2.1.1 **Risk** refers to uncertain events that may occur in the future that, if they occur, hurt the achievement of an organization's objectives, mission, or operational opportunities, or lose business opportunities**.**

2.1.2 Identifying/indicating risks means considering what events will hinder the achievement of objectives.

2.1.3 Risk Factor refers to what causes or is the source of risks and events that will not achieve the objectives and goals set. In each factor, the true causes of the factors are determined. It can be explained that the cause of the risk factor results in any risk. And measures can be taken to manage the factors to reduce the risk of occurrence**.**

2.1.4 **Risk Assessment** refers to measuring the severity of the risk to prioritize it based on its likelihood and impact.

2.1.4.1 **Likelihood** refers to the frequency or likelihood that a risk event will occur.

2.1.4.2 **Impact** is defined as the severity of the damage or the consequences of a risk event.

2.1.4.3 **Degree of Risk** is defined as the state **of** risk derived from assessing the opportunity and the impact of each risk factor, divided into five levels: high, very high, medium, low, and very low.

2.1.5 The source of risk comes from two factors: internal and external factors.

2.1.5.1 **Internal factors** include organizational objectives, policies and strategies, operations, work processes, structure and management systems, finance, corporate culture, and information technology.

2.1.5.2 **External factors** such as state policy, economic, social, political conditions, the actions of relevant external entities, competition, vendors or service providers and, natural disasters, etc.

2.1.6 Risk Management refers to the management of factors and control activities and operational processes by reducing the reason for the risk and reducing the potential adverse consequences of uncertainty to an acceptable level. The organization can be assessed, controlled, and monitored systematically. Taking into account the achievement of the organization's objectives or goals or maximizing the organization's value under business uncertainty.

After risk assessment, the evaluator chooses the appropriate method of risk management, as follows:

2.1.6.1 Risk avoidance (**Terminate)** is the choice of another operational process that will keep the enterprise from facing the risk event but still proceed to achieve the original target performance.

2.1.6.2 Risk transfer**(Transfer)** is a transfer of responsibility to another person or other company to carry out risk activities that will cause risk on behalf of the group without limiting the risk only that the risk is the responsibility of other operators**.**

2.1.6.3 Risk control (**Treat**) sets up additional risk control activities to ensure that it is sufficient to reduce risk status. This may be downgrading the likelihood of a risk event or the severity of the consequences of a risk event.

2.1.6.4 Risk acceptance (**Take)** is the case that the benefits and rewards resulting from a risk activity exceed the cost of personnel, budget, resources used in that risk activity. The enterprise will allow that risk activity by increasing risk control to reduce the risk level as low as possible.

2.2 Key elements in risk management

Effective risk management in accordance with the guidelines of the COSO (The Committee of Sponsoring Organization of the Treadway Commission) consists of eight components, which cover the following guidelines for policy-making, management, operation, and risk management:

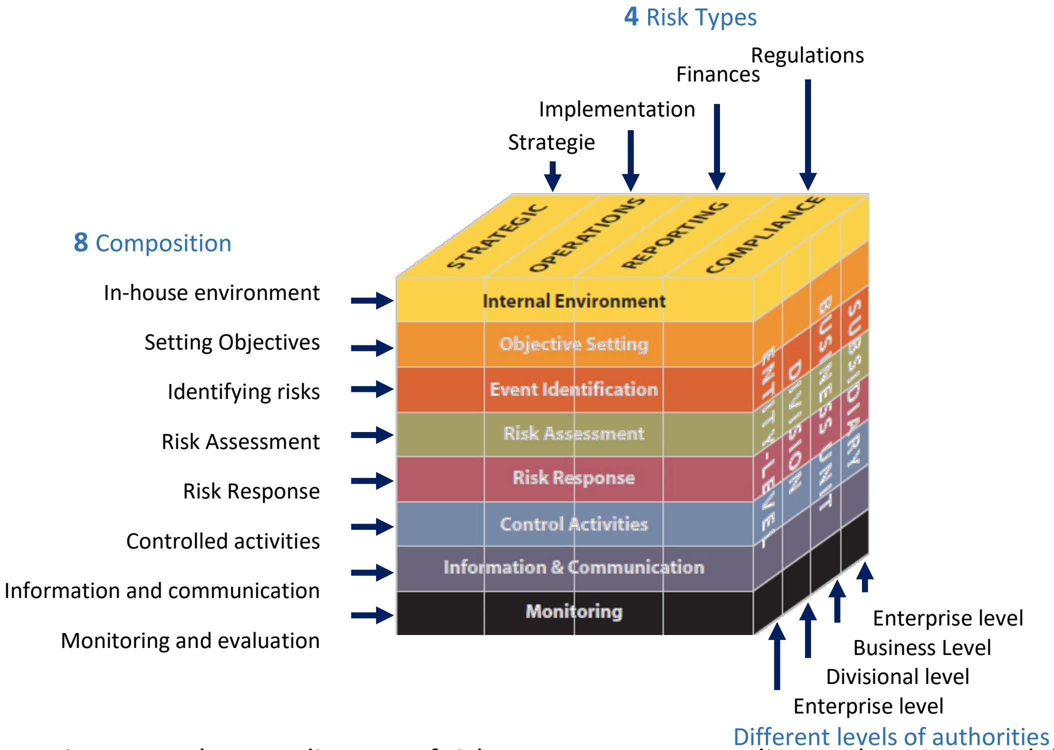


Figure 1.1 shows a diagram of risk management according to the COSO guidelines.

2.2.1. Internal environment

The organizational environment is an important element in defining the risk management framework, and it is an important basis for determining the direction of the organization's risk management framework. It consists of several elements, such as organizational culture, management policies, personnel practices, work processes, information systems, etc.

2.2.2 Objective Setting

The organization must consider establishing risk management objectives in line with the strategic goals and risks acceptable to the organization to clearly and appropriately set the organization's risk management goals.

2.2.3 Risk identification

It is a collection of events that may occur with the organization, both risk factors arising from internal and external factors. When they occur, the organization does not achieve its objectives or goals. The Company considers the risk factors that may occur with personnel management policies, operations, finances, information systems, regulations, etc., in order to understand the events and circumstances. And so that management can consider establishing guidelines and policies to deal well with the risks that may arise.

2.2.4 Risk **Assessment**

Risk assessment measures the degree of severity of a risk to determine its prioritization by assessing its likelihood and impact.

2.2.5 Risk Response

This is done after the organization has identified the organization's risks and assessed the level of risk. Response measures must be implemented to reduce the likelihood of risk occurrence or reduce the severity of the impact to a level acceptable to the organization. The most appropriate risk management method is worth investing in.

2.2.6 Control Activities

Defining activities and practices to help reduce or control risks, ensure that risks are appropriately managed, and enable operations to achieve organizational objectives and goals, preventing and reducing risk to an acceptable level.

2.2.7 Information and Communication

Organizations must have a practical information and communication system, as it is an important basis to consider further risk management in accordance with the frameworks and procedures established by the organization.

2.2.8 Monitoring

The organization need to have a follow-up to know that performance is appropriate and that risks can be effectively managed or not

The company has adopted the COSO-ERM 2017 (Enterprise Risk Management-Integrating with Strategy and Performance), which has grouped the enterprise risk management process elements into five components: 1. Corporate Governance and Culture, 2. Strategy & Objective Setting, 3. Performance Goals, 4. Review & Revision; and 5. Information, Communication & Reporting as a framework for the company’s risk management to achieve the sustainable development goals of the business.

2.3 **Type of risk**

The risk classification has been classified as follows:

2.3.1 Strategic Risk (S) refers to the risk resulting from improper strategic planning and compliance, including inconsistencies between policies, goals, strategies, organizational structure, competing circumstances, resources, and environment that affect the organization's objectives or goals.

2.3.2 Operational risk (O) Refers to the risk resulting from every step of the operation due to a lack of good governance or a lack of reasonable internal control. It covers processes, equipment, information technology, operational personnel, and property safety factors.

2.3.3 Financial risk (F) Refers to risks related to financial liquidity, financial management, and financial statements, such as risks from improper budgeting, mis-budgeting, and overhead, including risks from fluctuations in market factors (Market Risk) And risks from counterparties not complying with obligations (Credit Risk) Risk of fluctuations in interest rates and exchange rates

2.3.4 Legal Risk and Corporate Binding Requirement (**C)** refers to agencies complying with laws and corporate obligations, such as the risk of breach of contract, obligations, lack of compliance reporting, or non-compliance with laws, rules, and regulations.

2.3.5 Emerging Risk refers to losses arising from risks that are not present but may occur in the future due to changing environmental conditions. These types of risks are slowly occurring that are not easy to identify. There is a low frequency of occurrence, but they may have a severe impact once they occur. These emerging risks are often identified based on projections based on existing studies. These emerging risks are often the result of political, legal, social, technological, physical environments, natural changes, or pandemics. Sometimes the effects of these types of risks may not be currently identifiable. For example, problems arising from nanotechnology, climate change, the risk of spreading serious infectious diseases, etc.

2.3.6 Business Interruption Risk refers to the company's temporary stoppage to repair or correct due to damage to property caused by cyber threats, information technology, natural disasters, political rallies, epidemics, including changes that cause the business to stop, etc.

2.3.7 Environmental Risk refers to the risk that negatively impacts the environment caused by the company's operation.

2.3.8 Corruption Risk is defined as the risk of corruption, embezzlement, solicitation, or transfer of an interest of an organization or external entity for personal gain.

2.3.9 Risks of climate change

The global warming crisis is a major cause of climate change, affecting natural resources (such as water, soil, ecosystems and biodiversity, coastal areas, and small islands in the sea) and the lives and well-being of local communities in rural areas (such as food security, health) to a great extent, depending on the degree and magnitude of climate change. Significant and broad-scale changes produce far more severe effects than temporary or small-scale changes. In addition, climate change can affect the agricultural sector in many other ways, including the concentration of carbon dioxide levels, changing atmospheric humidity and rain, the interaction of climate change impacts, etc.

Ref: Department of Meteorology (http://climate.tmd.go.en/content/article/9) Human activity that causes climate change is the activity that increases the amount of greenhouse gases in the atmosphere, causing the greenhouse effect to be more severe than it should be naturally and resulting in an increase in global warming.

Ref: Department of Meteorology (http://climate.tmd.go.en/content/article/9) The company has developed a project to reduce greenhouse gas emissions to reduce global warming. A flood disaster response plan is also prepared annually to guide all employees when an emergency occurs in the company to effectively control emergencies that result in minimal damage to property and person.

2.3.10 IT **Risk**

- Digital Transformation Risk refers to the risk that the company will not be able to adapt to the changes in technology that may affect business operations and thus lose competitiveness.
- Cyber Threat Risk refers to being attacked by an external intruder, destroying or damaging a network or database in an organization's information technology system.

3. Company Risk Management

3.1 Current company risk management

The company currently has various aspects of risk management by using multiple management tools such as the Good Corporate Governance (GCG) Performance Assessment System and Key Performance Indicators (KPIs). Implementation of quality policy according to various standards such as ISO standards etc. In practice, the company has been able to carry out operational risk management well.

However, the Board of Directors has placed great emphasis on risk management. In order to ensure effective and efficient risk management, the Board has appointed a Risk Management Committee to oversee risk management more effectively.

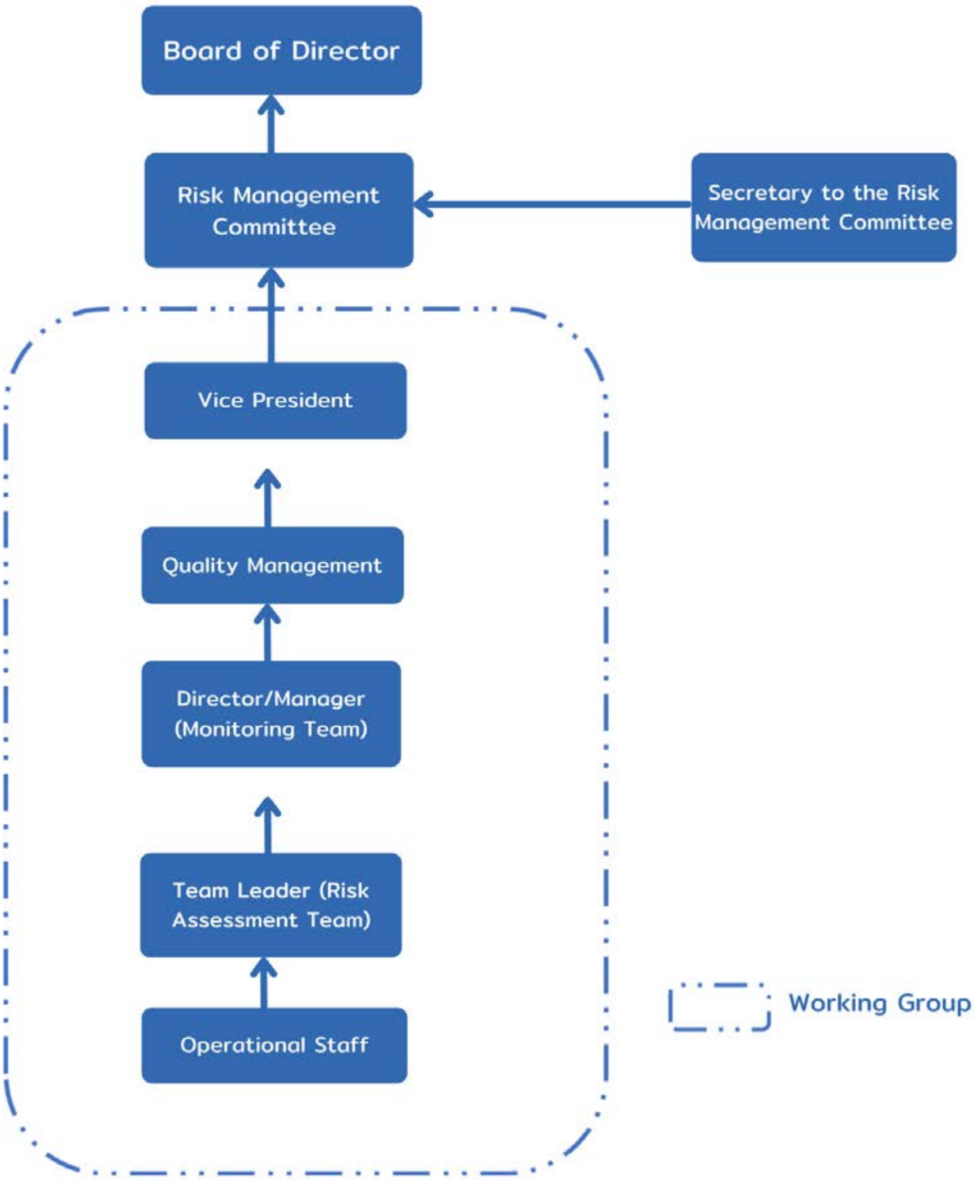
3.2 Risk Management Policy

To ensure clarity in risk management, the Board of Directors has established a policy framework for risk management, operating methods, and risk management plan as follows:

3.2.1 Focusing risk management on the impact on corporate objectives and policies and the risks that corruption poses in the organization and the reputation and image of the company.
3.2.2 Execute risk management to the highest level of efficiency and an acceptable level and involve all employees in the risk management process.
3.2.3 Encourage employees across the organization to be aware of and prevent all imminent risks.
3.2.4 Continuously examine, monitor, and evaluate the risks posed by the changing environment, both from internal and external factors.
3.2.5 Promote risk management as part of a culture leading to value creation for the Group.
3.2.6 Preventing and combating corruption of individual companies

3.3 Risk Management Structure

Those responsible for the company's risk management consist of staff at all levels, from the general staff to the board level. The structure is as follows:



3.4 Role of those involved in risk management

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

Department	Roles and Functions
Company's board of directors	Provide approval for the organization's risk management while ensuring effective compliance with the established plan through the Risk Management Committee.
Risk Management Committee	1. Establish a corporate strategy and operational policies and oversee ongoing risk analysis and management. 2. Supervise and motivate employees at all levels to be aware of risks and encourage an ongoing enterprise-wide risk management process into organizational culture. 3. Encourage employees to acquire knowledge of risk management. 4. Review risk management reports and take steps to ensure that risk management is adequate and appropriate, risks can be managed to an acceptable level. Risk management is implemented on an ongoing basis. 5. Continuously develop and review the company's risk management system to be effective. The risk management process is regularly evaluated and monitored in accordance with established policies. 6. Conducts decisions and advises on key issues arising in the risk management process. 7. Present the Risk Management Committee's performance report to the Board of Directors for acknowledgment and/or consideration at least once a year.
Risk Management Committee Secretary	1. Consolidate the risks and risk management of each section of the Risk Management Committee's presentation. 2. Prepare a risk management report for presentation to the Risk Management Committee.
Quality Management Department	1. Coordinates, advises, and assists departments in analyzing, assessing, and managing risks in accordance with company guidelines. 2. Monitor the risk management results of different functions and alert the risk owners to the ongoing management and risk management review.
Deputy Managing Director (by Function)	1. Regularly supervise the staff to analyze and assess the risks involved. 2. Provide approval for the applicable risk management guidelines.
Director/Sales Manager (by Function)	1. Provide approval for the risk management methodology through affiliated entities' indicators and risk assessment. 2. Present the issue of unmanageable risk to the Deputy Director 3. Risk management monitoring and evaluation

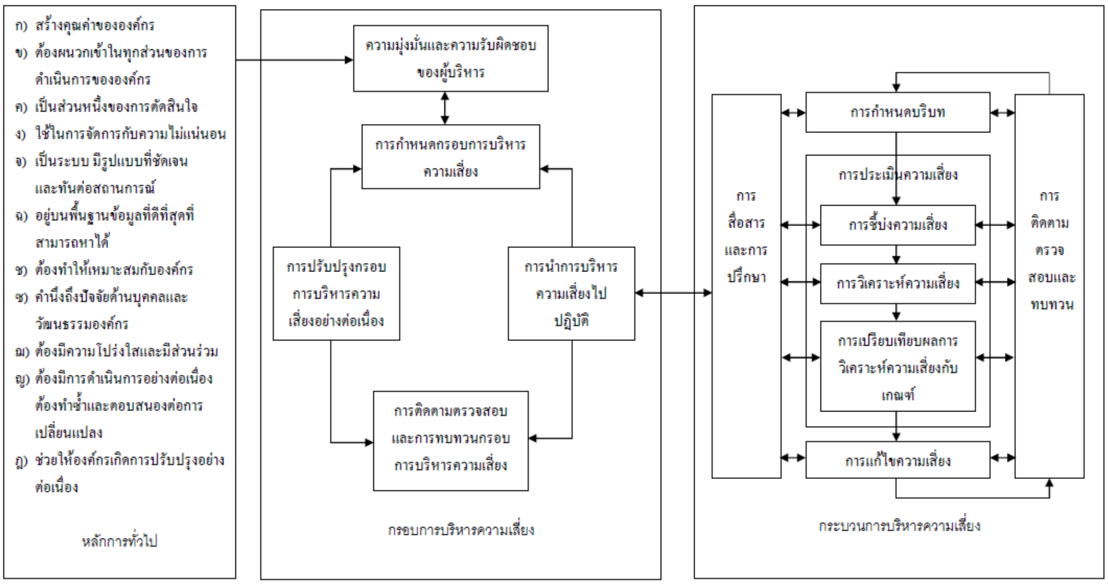
Department	Roles and Functions
Head of Department and Operational Staff (by Function)	1. Analyse and assess the risks of each function and report the risks to the supervisor regularly. 2. Regularly study, analyze and report potential risks to supervisors. 3. Risk Management Report
General Officer	1. Implement an internal control system to prevent risks. 2. Carry out risk management in accordance with established guidelines.

4. Principles of Risk Management

Risk is the chance that an event will occur that will impact the ability to achieve a company's objectives, such as increased competition, corruption, non-compliance, etc. The fundamental principle in risk management is to help create value for the organization by incorporating a risk management perspective into all phases of normal operations and any business decisions. Risk factors must always be considered. There are guidelines for operating under uncertain conditions and must be adaptable. It is appropriate for the organization and the circumstances of the moment. It must take personnel factors, participation, transparency, and corporate culture into account on the best possible basis. And most importantly, it must be implemented continuously and reviewed regularly.

5. Risk Management Process

To increase the chances of achieving objectives, promote proactive management, recognize the need to identify and address risks across the organization, and establish control guidelines to prevent or reduce risks to an acceptable level, the Company has adopted the TIS 31000-2561 (ISO31000: 2017) standard. The risk management processes and procedures are as follows:



6. **Risk Management System Framework**

The Company has adopted the following risk management principles in accordance with the COSO guidelines.

6.1 Identifying incidents

Managers or department heads must identify potential risks that affect both internal and external factors, including risk-related issues. All parties must be transparent and open in identifying risks that affect the implementation of strategies or the achievement of objectives or events necessary to improve risk management.

6.2 Risk Assessment

Risk assessment is a process that consists of the analysis, assessment, and classification of risks that affect the achievement of the objectives of the organization's operations. The company has established risk assessment criteria, including the risk likelihood and severity of the impact, which both quantitative and qualitative criteria can determine, which is used as a basis for assessing various risks. Refer to Annex A

The fraud or corruption risk assessment is set up to identify, assess, and review the fraud and corruption risks referred to in Annex B and raise awareness of the corruption risks that affect the objectives and operations of the organization. The risk assessment must be in accordance with the Company's corruption policy framework.

6.3 Risk Rating

To assess the risk, a Risk Profile is defined based on the risk significance rating from the likelihood and impact and the extent of the acceptable risk level (Risk Appetite Boundary) based on Appendix C.

Level of risk = (likelihood of occurrence of events) X (impact of events)

6.4 Risk Treatment

According to the individual assigned the task, employees directly involved in the risk management process are responsible for risk management. Establishing a risk management plan will be presented to the management committee meeting to consider and approve the allocation of resources needed to implement the action (if any). In selecting the most appropriate approach to risk management, the acceptable risk (Risk Tolerance) will be taken into account with the resulting cost compared to the benefits. This includes legal and other requirements related to social responsibility by choosing the strategy for risk management as follows:

- Risk avoidance **(Terminate)** is the choice of another operational process that will keep the enterprise from facing the risk event but still proceed to achieve the original target performance.
- Risk **Transfer** is a transfer of responsibility to another person or other company to carry out risk activities that will cause risk on behalf of the group without limiting the risk only because the risk is the responsibility of other operators.
- Risk control (**Treat)** sets up additional risk control activities to ensure that it is sufficient to reduce risk status. This may downgrade the likelihood of a risk event or the severity of the consequences of a risk event.
- Risk acceptance **(Take)** is the case that the benefits and rewards resulting from a risk activity exceed the cost of personnel, budget, resources used in that risk activity. The company will allow that risk activity by increasing risk control to reduce the risk level as low as possible.

6.5 Monitoring and Review

The Company will regularly review its risk management policy annually or when there are significant changes and impacts on risk management.

6.6 Information and communication technology

The Company has noted the importance of enterprise risk management. It has established that the risk management policy is communicated to its personnel by publishing it on the Company's website www.alt.co.th, through the Intranet, training, or workshop.

Effective February 23, 2022

ปรียาภรณ์ ตั้งเผ่าศักดิ์

(Mrs. Preeyaporn Tangpaosak)
President
ALT Telecom Public Company Limited

APPENDIX

Appendix A Criteria for assessing business risks

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

❖ The risk likelihood level is set at five levels.

The chance of occurrence.	Level	Probability/Opportunity
Extremely high	5	• A much worse chance of transition if there is no supporting activity.
High	4	• A worse chance of transition if there is no supporting activity
Moderate	3	• Opportunity for change is low despite supporting activities or taking no action.
Few	2	• Opportunities for change are better, but they need to be promoted.
Very little	1	• Opportunities for continuous change in a better way without taking any action.

❖ The severity level of the impact is set at five levels.

Impact	Level	Effects/Consequences
Extremely high	5	• Very high impact, uncontrollable
High	4	• High impact but controllable (difficulty)
Moderate	3	• Has a moderate but controllable effect.
Few	2	• It has little impact and is easily controllable.
Very little	1	• It has very little or no direct impact.

Table 2A - Assessment of downside risks: ALT Group

❖ The risk likelihood level is set at five levels.

The chance of occurrence.	Level	Occurrence Quantity	The status of the event. Actual Occurrence.	Occasion commits an **offense**
Extremely high	5	The chance of occurrence is greater than 75% or one time per month or more.	Incidents have been reported and are currently under investigation.	Happens very quickly without control measures.
High	4	51 - 75% chance of occurrence or Once per 2-6 months but no more than five times	Incidents under management	There is a greater chance of accidents without control measures.
Moderate	3	Chance of occurrence 26- 50% or Once per 1-2 years	The incident has been dealt with.	There is a chance that this will happen without control measures.

The chance of occurrence.	Level	Occurrence Quantity	The status of the event. Actual Occurrence.	Occasion commits an **offense**
Few	2	The chance of occurrence is 10-25% or Once per 2-4 years	The actual cause of the incident In the process of rectifying	Difficult to occur even without control measures
Very little	1	Chance of occurrence < 10% or Once per 5 years	The actual cause of the incident Has been rectified (The case of recurrence has been reduced)	Very rare, even without control measures.

❖ The severity level of the impact is set at five levels.

1. Policy/quantitative/financial implications

Impact	Level	Effects/Consequences	Company
Extremely high	5	• The damage value is more than 20% of the financial target.	All Group
High	4	• The damage value is more than 10-20% of the financial target.	All Group
Moderate	3	• The damage value is more than 5-10% of the financial target.	All Group
Few	2	• The damage value is more than 3-5% of the financial target.	All Group
Very little	1	• The damage value is less than 3 % of the financial target.	All Group

2. Operational Impact

Impact	Level	Effects/Consequences	Company
Extremely high	5	• The project could not be completed.	ALT, GTS, IH, IG
		• The work cannot be produced/delivered.	INN, EMAX
		• Unable to test.	LAB 17025
High	4	• Implement the project successfully, according to the plan, less than 50 percent.	ALT, GTS, IH, IG
		• Produces/delivers less than 70% of planned work	INN, EMAX
		• Unable to confirm test results.	LAB 17025
Moderate	3	• Implement the project successfully, according to the plan, less than 50 percent.	ALT, GTS, IH, IG
		• Produces/delivers less than 70% of planned work	INN, EMAX
		• Significantly impacting some of the test results	LAB 17025

Impact	Level	Effects/Consequences	Company
Few	2	• Implement the project successfully as planned, less than 70-89 percent.	ALT, GTS, IH, IG
		• Produce/deliver work as planned less than 80% -89%	INN, EMAX
		• Insignificant impact on partial test results	LAB 17025
Very little	1	• Risks that are always common in the ordinary course of business.	All Group

3. Legal implications

Impact	Level	Effects/Consequences
Extremely high	5	Criminal investigations, claims for damages, and/or orders to suspend any transactions were carried out.
High	4	The investigation may include criminal proceedings and/or significant claims for damages.
Moderate	3	Significant lawsuits, including substantial fines/damages claims
Few	2	Lawsuit, fine, or small amount of damage taken place.
Very little	1	There is minor non-compliance with regulations.

4. Impact on corporate reputation/image

Impact	Level	Effects/Consequences
Extremely high	5	• Massive damage to the company's image and reputation. • Significant impact on business objectives and strategies
High	4	• Damage that affects the image and reputation of the company a lot. • Greater impact on business objectives and strategies
Moderate	3	• Moderate damage to the company's image and reputation • Moderate impact on business objectives and strategies
Few	2	• Minor damage to the company's image and reputation. • Low impact on business objectives and strategy
Very little	1	• Risks that are always common in the ordinary course of business.

Appendix B Corruption Risk Assessment Criteria

Table 1B - Corruption risk assessment: ALT Group

❖ The risk likelihood level is set at five levels.

The chance of occurrence.	Level	Occurrence Quantity	The status of the event. Actual Occurrence.	Occasion commits an **offense**
Extremely high	5	The chance of occurrence is greater than 75%; or One time per month or more	Incidents have been reported and are currently under investigation.	Happens very quickly without control measures.
High	4	51 - 75% chance of occurrence or Once per 2-6 months, but no more than five times	Incidents under management	There is a greater chance of accidents without control measures.
Moderate	3	26 - 50% chance of occurrence or Once per 1-2 years	The incident was handled.	There is a chance that this will happen without control measures.
Few	2	10 - 25% chance of occurrence or Once per 2-4 years	The actual cause of the incident In the process of rectifying	Difficult to occur even without control measures
Very little	1	Chance of occurrence < 10% or Once per 5 years.	The actual cause of the incident Has been rectified (The chance of recurrence has been reduced)	Very rare, even without control measures.

❖ The severity level of the impact is set at five levels.

Occurrence of Event	Level	in Reputation and Image aspects	Financial aspects	Legal aspects	Customer aspects
Extremely high	5	Widespread news was presented through the media, both within the country and abroad.	> 30% of income	Criminal investigations, claims for damages, and/or orders to suspend any transactions were carried out.	Loses a significant customer and has severe consequences for future growth.

Occurrence of Event	Level	in Reputation and Image aspects	Financial aspects	Legal aspects	Customer aspects
High	4	Negative news in the national media and the Asian region will affect the company's reputation and image in the long term.	between 20% - 30% of income	The investigation may include criminal proceedings and/or significant claims for damages.	Significant loss or impact of relationships with key customers with substantial cost reductions and impact on future growth
Moderate	3	Negative news from the local media is still present and is beginning to affect customers.	between 10% - 20% of income	Significant lawsuits, including substantial fines/damages claims	Loses or impacts relationships with customers to a large extent, with a mid-cost solution.
Few	2	Negative news impacts the company's products and reputation in the domestic market.	between 5% - 10% of income	Lawsuit, fine, or small amount of damage taken place.	Minimal impact on customer relationships, with some fixed costs.
Very little	1	Negative news from the local media was dealt with quickly; events returned to normal.	<5% of income	There is minor non-compliance with regulations.	Very few customer complaints, no impact on costs

Appendix C Risk Consideration Level

Degree of Risk

Degree of Risk

Impact	Extremely Low 1	Low 2	Moderate 3	High 4	Extremely high 5
Very high. 5	5	10	15	20	25
High 4	4	8	12	16	20
Moderate 3	3	6	9	12	15
Few 2	2	4	6	8	10
Very little. 1	1	2	3	4	5

Opportunity/Frequency

Risk Grade	Scale	Replace with a colored bar.	Explain
1	1-4	Very little	"Few/very low level" does not require risk management.
2	5-9	Few	"Acceptable levels" must be controlled to prevent the risk from moving to unacceptable levels.
3	10–14	Moderate	"Moderate" is acceptable, but it takes effort to reduce the risk to remain acceptable.
4	15-19	High	A "high level" is unacceptable, requiring risk management to continue to be acceptable.
5	20–25	Extremely high	"Extremely high level" is unacceptable. Risk management needs to be accelerated to remain acceptable.