TCM
CORPORATION

Enterprise Risk Management Manual

Revised 1 (February 2023)

Table of Contents

Chapter 1
General Scope

Risk management is an essential and beneficial tool for managing an organization to achieve its goals and objectives effectively and efficiently. It helps create value, preserve value, and generate the true value of the organization by managing factors and controlling activities throughout the operational processes, reducing the causes of each opportunity that may cause impact. This is to ensure that the level and extent of the impact that may occur to the organization in the future are at an acceptable level or can be systematically controlled throughout the organization.

1.1 Objectives of the Risk Management Manual

(1) To provide executives and employees with knowledge and understanding of the organization's risk management processes to support the organization's operations in accordance with the goals set out in the operating plan and strategic plan.

(2) To serve as a tool for executives and employees to perform their duties according to the risk management process in a systematic and continuous manner, in line with the organization's vision, mission, and core values.

(3) To provide the organization with a framework for responding to events that may result in risks in all areas in a systematic manner, including taking actions to establish a foundation for preventing and managing potential risks in the future.

(4) To serve as a tool to help instill a corporate culture that focuses on building risk management knowledge among executives and personnel at all levels, as a mechanism for developing risk management knowledge and supporting risk management to become a sustainable corporate culture.

1.2 Definition and Terminology of Risk Management

To understand the meaning and definition of risk management, it is necessary to understand the meaning of the relevant terms as follows:

(1) Risk means the possibility of an event occurring and affecting the achievement of strategies and business objectives. The event may have both positive and negative impacts. To cover the organization's operations, the types of risks are divided into 5 areas as follows:

(a) Strategic Risk: This is the risk arising from the formulation of strategic plans and operating plans that are implemented inappropriately or inconsistently with internal and external factors, affecting the achievement of the organization's objectives, vision, mission, or core values.

(b) Operational Risk: This is the risk arising from every step of the operation, covering factors related to processes, equipment, personnel, and information systems in the operation, etc.

(c) Financial Risk: This is the overall financial risk, including financial planning and financial management, which must be in the same direction as the organization's strategy.

(d) Compliance Risk: This is the risk arising from the inability to comply with the rules, regulations, or laws of relevant agencies or organizations, which may affect the company's operations, including the risk from changes in the aforementioned rules, regulations, or laws.

(e) Cyber Risk: This is the risk related to the management of operational efficiency, including technology security, such as unauthorized access to data or work systems, phishing mail, malware, ransomware, etc.

(2) ESG Risk refers to ESG-related risks or opportunities that may impact the organization. E (Environmental) refers to issues related to the environment, such as climate change, natural resource use, pollution emissions, and waste management. S (Social) refers to issues related to society, such as human resource management, treatment of stakeholders, and product and service responsibility. G (Governance) refers to issues related to corporate governance, such as transparency in the organization, compliance with ethical standards, and management responsibility.

(3) Risk Factor means the cause of a risk that prevents the achievement of the stated objectives. Risk factors may originate from both internal and external factors. The organization should identify the root cause in order to analyze and determine strategies/measures/guidelines to reduce risk correctly, appropriately to the situation, and in accordance with the organization's context.

(3.1) External Factors: These are external factors that influence the success of the objectives. These factors cannot be controlled by the organization in terms of the likelihood of occurrence, but the impact can be reduced according to the organization's risk response methods, such as purchasing forward contracts to reduce exchange rate fluctuations, etc. External factors include:

(a) Natural Environment: Natural disasters and environmental events such as floods, fires, earthquakes, tsunamis, and epidemics that cause damage to buildings, property, raw material sources, and labor.

(b) Economic: Inflation, deflation, interest rates, exchange rates, and events related to price movements, funding sources, and competitors.

(c) Political: Events related to the government and executives of the country where the organization operates or does business, the promulgation of laws, regulations, and events that open or restrict opportunities to enter foreign markets, and changes in tax rates.

(d) Social: Events related to population changes, migration, family structure, social standards and preferences, and terrorism.

(e) Information Technology: Events related to changes in computer technology.

(3.2) Internal Factors: These are internal factors that influence the success of the objectives. These factors can be managed and controlled by management, as follows:

(a) Infrastructure: Events related to the need for capital to expand or maintain infrastructure, reducing machine downtime, and increasing customer satisfaction.

(b) Personnel: Events related to personnel in the organization, such as the expiration of employment contracts of key employees, the acquisition of personnel with operational capabilities, and the retention and development of existing personnel.

(c) Process: Events related to work procedures, changes in work methods or procedures, errors in the process, product delivery, inadequate control that affects customer dissatisfaction, loss of market share, and damage to reputation.

(d) Technology: Events related to the organization's IT and information systems, the accuracy and completeness of information, security, system selection, development, system maintenance, data backup, and system recovery.

(4) Risk Assessment means the process of identifying risks and analyzing them to prioritize risks that will affect the achievement of the organization's objectives, by assessing the likelihood of an event occurring and the impact of the risk event after the implementation of risk control measures in the normal operations of various departments in the organization.

(a) Likelihood means the frequency or probability of a risk event occurring.

(b) Impact means the magnitude of the severity or damage that will occur from a risk event.

(c) Degree of Risk means the status of the risk obtained from assessing the likelihood and impact of each risk factor.

(5) Risk Appetite means the type and criteria of risk or overall uncertainty that the organization can accept while still enabling the organization to achieve its goals. The acceptable risk level may be specified as a single value or a range.

(6) Risk Response means the process used to manage remaining risks after risk control measures are in place in normal operations.

(7) Enterprise Risk Management provides a risk management framework for the board of directors, executives, and personnel at all levels in the organization to manage existing risks, including potential risks in the future.

The Board of Directors plays a role in overseeing, which includes governance and culture, strategy and objective setting, performance, information, communication and reporting, as well as reviewing and revising practices to improve business performance, support the creation of business value and prevent deterioration, and determine the organization's acceptable risk level.

Executives are responsible for the overall implementation of the risk management process in the business, including increasing communication with the board of directors and stakeholders regarding the implementation of enterprise risk management to help in developing plans that align with the organization's strategies and objectives.

Employees at all levels participate in creating a culture and awareness of risks in daily work and assigned duties, supporting the organization's risk policies.

(8) Control means the policies and practices that help ensure that actions are taken according to the guidelines for reducing or controlling risks to the specified level. Control activities occur at all levels, in all job functions, and throughout the organization, consisting of different types of activities divided into 4 categories:

(a) Preventive Control: This is control to prevent or reduce the risk of damage from potential errors, such as approvals, segregation of duties, and access control to assets.

(b) Detective Control: This is control to detect damage or errors that have already occurred, such as reviews, reconciliations, and counts.

(c) Directive Control: This is a control method that promotes or encourages the achievement of desired objectives, such as rewarding high performers.

(d) Corrective Control: This is a control method established to correct errors that have occurred to prevent recurrence in the future.

1.3 Benefits of Risk Management

(1) Expands the scope of opportunities by enabling management to identify opportunities for the business and unique challenges, both current and future, by considering the reasonable probability of both positive and negative risks.

(2) Reduces the magnitude or severity of the impact of unexpected events in the future, while potentially increasing positive outcomes for opportunities.

(3) Identifies and manages significant risks in a timely manner.

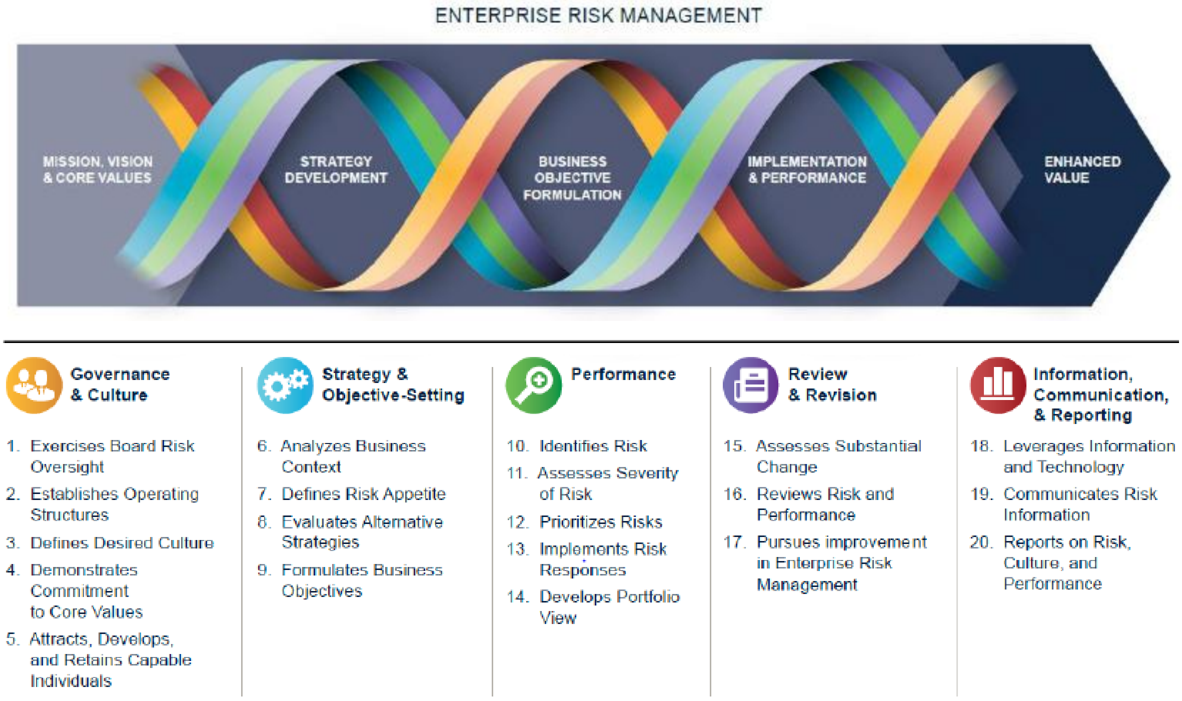
(4) Helps reduce the variability of performance, leading to the successful implementation of the organization's strategies into operations.

(5) Improves resource utilization. Obtaining sufficient risk information allows management to assess overall resource needs and helps allocate resources appropriately.

Chapter 2
Risk Management According to COSO ERM 2017

2.1 Key Principles of Risk Management According to COSO ERM 2017

The framework for enterprise risk management that is recognized as a guideline for promoting risk management and as an international standard is the Enterprise Risk Management Framework of the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which assigned *PricewaterhouseCoopers to develop the Enterprise Risk Management Framework*, as shown in the image.


ENTERPRISE RISK MANAGEMENT
MISSION, VISION & CORE VALUES
STRATEGY DEVELOPMENT
BUSINESS OBJECTIVE FORMULATION
IMPLEMENTATION & PERFORMANCE
ENHANCED VALUE

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Image: Enterprise Risk Management Framework Based on COSO ERM 2017 (Source: www.coso.org)

2.2 Risk Management According to COSO ERM 2017

Enterprise Risk Management – Integrating with Strategy and Performance is the risk management framework according to COSO ERM 2017 to clarify the importance of enterprise risk management in strategic planning and the importance of applying enterprise risk management in conjunction with normal operations throughout the organization. (This is because risk influences every department and function, and risk makes strategy consistent with performance in every department and function.)

This framework is a set of principles divided into 5 components and 20 interrelated principles, with the following key details:

Component 1: Governance & Culture

Governance sets the organization's tone, reinforces importance, and establishes oversight responsibilities for enterprise risk management. The culture relates to ethical values, desired behaviors, and an understanding of risk in the enterprise. It comprises 5 principles:

Principle 1: Execute Board Risk Oversight – The board of directors oversees strategy and governance to support management in pursuing business strategy and objectives.

Principle 2: Establishes Operating Structures – The organization establishes operating structures to achieve business strategy and objectives.

Principle 3: Defines Desired Culture – The organization defines desired behaviors that demonstrate the characteristics of the enterprise's desired culture.

Principle 4: Demonstrates Commitment to Core Values.

Principle 5: Attracts, Develops, and Retains Capable Individuals – The organization is committed to building human resources to align with business strategy and objectives.

Component 2: Strategy & Objective-Setting

The strategic planning process is a collaboration of enterprise risk management, strategy, and objective setting. The organization defines its risk appetite in line with the strategy. Business objectives enable strategic implementation while also serving as criteria for identifying, assessing, and responding to risk. It includes 4 principles:

Principle 6: Analyzes Business Context – The organization considers the potential impact of business context on risk profile.

Principle 7: Defines Risk Appetite – The organization defines risk appetite in the context of value creation, value preservation, and value realization.

Principle 8: Evaluates Alternative Strategies – The organization evaluates alternative strategies and their potential impact on risk profile.

Principle 9: Formulates Business Objectives – The organization considers risk while formulating business objectives at various levels that align with and support strategy.

Component 3: Performance

Risks that may affect the achievement of strategy and business objectives must be identified and assessed. Risks must be prioritized according to their severity in the context of the organization's risk appetite. Subsequently, the organization selects risk responses and considers the overall risk portfolio. The results of the aforementioned process are reported to key risk stakeholders.

Principle 10: Identifies Risk – The organization identifies risks that may affect performance in relation to strategy and business objectives.

Principle 11: Assesses Severity of Risk

Principle 12: Prioritizes Risks – The organization prioritizes risks (to be used as criteria for selecting risk responses).

Principle 13: Implements Risk Responses – The organization identifies and selects risk responses.

Principle 14: Develops Portfolio View – The organization develops and evaluates a portfolio view of risk.

Component 4: Review & Revision

This can be done by reviewing the organization’s performance. The organization can consider how well the components of enterprise risk management have functioned in the past and when significant changes occur, including what needs to be revised.

Principle 15: Assess Substantial Change – The organization identifies and assesses changes that could significantly affect strategy and business objectives.

Principle 16: Reviews Risk and Performance

Principle 17: Pursues Improvement in Enterprise Risk Management – The organization continuously seeks to improve enterprise risk management.

Component 5: Information, Communication, & Reporting

Enterprise risk management requires an ongoing process for obtaining and sharing necessary information, both from internal and external sources, that flows throughout the organization. It comprises 3 principles:

Principle 18: Leverages Information and Technology – The organization leverages the organization's information systems and technology to support enterprise risk management.

Principle 19: Communication Risk Information – The organization uses communication channels to support enterprise risk management.

Principle 20: Reports on Risk, Culture, and Performance – The organization reports on risk, culture, and performance at various levels across the organization.

Chapter 3
Risk Management of TCM Corporation Public Company Limited

3.1 Risk Management Structure of TCM Corporation Public Company Limited

The company's risk management structure consists of the Board of Directors, the Sustainability and Risk Management Committee, and the Risk Management Working Group. They are responsible for managing risks at all levels of the company, including managing risk events that arise from both internal and external factors.

Board of Directors

This refers to the Board of Directors of TCM Corporation Public Company Limited. It is responsible for providing recommendations and appointing the Sustainability and Risk Management Committee, as well as approving the risk management policy.

Sustainability and Risk Management Committee

The Sustainability and Risk Management Committee of TCM Corporation Public Limited Company consists of:

• Chairman of the Sustainability and Risk Management Committee	1 person
• Director of Sustainability and Risk Management (at least)	4 people
• Secretary of the Committee (may also be a committee member)	1 person

The duties and responsibilities of the Sustainability and Risk Management Committee are as follows:

(1) Presenting the risk management policy to the Board of Directors for consideration and recommendations.
(2) Defining risk management guidelines to cover the entire organization.
(3) Monitoring the process of risk identification and assessment presented by the Risk Management Working Group.
(4) Evaluating and approving the risk management plan proposed by the Risk Management Working Group.
(5) Submitting risk management reports to the Board of Directors.
(6) Overseeing the effectiveness of risk management.
(7) Performing other tasks related to risk management within the organization.

Risk Management Working Group

The Risk Management Working Group of TCM Corporation Public Company Limited consists of:

- Managers from every department in the company

The duties and responsibilities of the Risk Management Working Group are as follows:

(1) Managing risks according to the framework specified in the risk management manual.
(2) Assessing risks that affect the company by identifying both internal and external factors.
(3) Prioritizing risks and preparing plans to prevent or reduce the company's risks.
(4) Submitting risk management reports to the Sustainability and Risk Management Committee.
(5) Establishing a risk management system by integrating information technology systems.
(6) Performing other tasks as assigned by the Sustainability and Risk Management Committee.

Secretary of the Sustainability and Risk Management Committee

The Secretary of the Sustainability and Risk Management Committee is responsible for gathering risk information and risk management activities from each department to present to the Sustainability and Risk Management Committee, coordinating the analysis, assessment, and management of risks according to the defined guidelines, preparing risk management reports and presenting them to the Sustainability and Risk Management Committee, preparing and updating the risk management manual, and providing knowledge to various departments in the organization regarding risk management.

3.2 Risk Management System Development Process

This involves analyzing and prioritizing risks by considering the assessment of the likelihood of risk occurrence and the severity of the impact from risk events affecting the achievement of department or organizational objectives, based on established standards. It consists of 4 steps:

(1) Setting Risk Assessment Criteria

This involves setting the criteria used to assess the level of likelihood of risk occurrence, the level of severity of impact, and the level of risk for daily work risk assessment. Each department may set its own assessment criteria, which can be both quantitative and qualitative, depending on the department's environment and the management's judgment.

For the company's risk assessment, the following principles are used:

(a) The likelihood of events occurring, divided into 5 levels: very high, high, medium, low, and very low, represented by the numbers 5, 4, 3, 2, and 1, respectively.

(b) The severity of the impact from events, classified into 5 levels: very high, high, medium, low, and very low, represented by the numbers 5, 4, 3, 2, and 1, respectively.

Likelihood / Frequency of Occurrence

Level	Likelihood	Number of Occurrences	Frequency
1	Very Low	Never occurred in the past 1-3 years	More than 3 years or never
2	Low	Occurred once in the past year	1-3 years
3	Medium	Occurred 2-3 times in the past year	6-12 months
4	High	Occurred 4-5 times in the past year	3-6 months
5	Very High	Occurred more than 5 times in the past year	Less than 3 months

Level of Impact per Occurrence (Strategic Aspect)

Level	Impact	Comparison with Target
1	Very Low	Deviation from target / plan / budget <= 10%
2	Low	Deviation from target / plan / budget > 10 - 15%
3	Medium	Deviation from target / plan / budget > 15 - 20%
4	High	Deviation from target / plan / budget > 20 - 25%
5	Very High	Deviation from target / plan / budget > 25%

Level of Impact per Occurrence (Financial)

Level	Impact	Monetary Value (Baht)
1	Very Low	Less than or equal to 10 million Baht
2	Low	More than 10 million Baht to 35 million Baht
3	Medium	More than 35 million Baht to 75 million Baht
4	High	More than 75 million Baht to 100 million Baht
5	Very High	More than 100 million Baht

Level of Impact per Occurrence (Environment / Health)

Level	Impact	Environment	Safety
1	Very Low	Can be corrected or controlled immediately	Minor injury, no work stoppage
2	Low	Correction time within 1 week	Injury with work stoppage of 1-3 days
3	Medium	Correction time longer than 1 week to 1 month	Injury with work stoppage of 4-7 days
4	High	Correction time longer than 1 month to 6 months	Serious injury, hospitalization required
5	Very High	Correction time longer than 6 months	Disability or death

Level of Impact per Occurrence (Image / Reputation)

Level	Impact	Regulations / Laws
1	Very Low	No impact or correction within 1 day
2	Low	Fine not exceeding 500,000 Baht or correction time within 3 days
3	Medium	Fine more than 500,000 – 1,000,000 Baht or correction time within 7 days
4	High	Fine more than 1,000,000 - 3,000,000 Baht or being marked (Stock Exchange of Thailand)
5	Very High	Fine more than 3,000,000 Baht or criminal penalty or being marked with SP

(c) Degree of Risk is an indicator used to determine the significance of a risk. The risk level value is derived from considering both the likelihood of occurrence and the impact of the risk.

Degree of Risk = Risk Likelihood Level x Risk Impact Level

(2) Objective Setting

Objective setting is for understanding the scope of operations at each level and for comprehensively analyzing potential risks. Company objectives should align with strategic goals and the company's acceptable risk levels. At the department level, objective setting must align with or be in the same direction as the company's objectives to achieve overall goals. Objectives must also consider the SMART principles.

(3) Risk / Risk Event Identification

Risk identification involves considering what or which events might hinder operations and prevent the achievement of objectives or goals at both the organizational and activity levels. It should focus on identifying risks from important tasks/projects/activities/processes that are core to the organization. Risk events can be identified through brainstorming with personnel from various departments/the Sustainability and Risk Management Committee, or interviewing personnel or experts in the field, or analyzing work procedures in each key step, etc. The identified causes of risk should be the actual causes to accurately analyze and determine risk reduction measures later.

(4) Risk Assessment

This involves assessing the level of likelihood of occurrence (Likelihood) and the level of severity or damage value (Impact) of each identified risk and risk factor. Assessors should be knowledgeable and experienced in that area, or a majority vote from a meeting can be used, or attendees can provide scores, and the average score can be calculated.

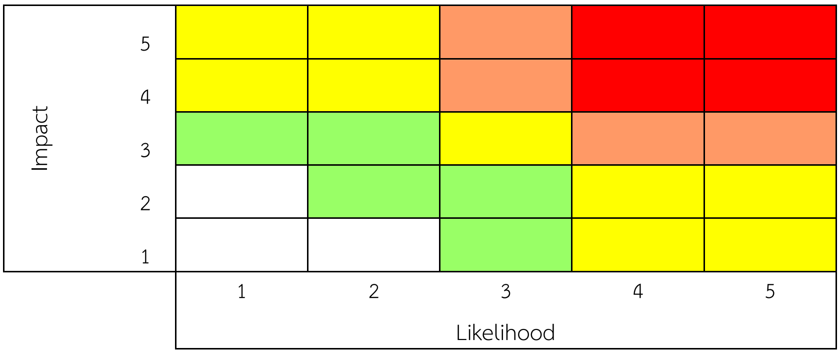
(5) Risk Analysis and Prioritization

Once the department has considered the level of likelihood / frequency of occurrence (Likelihood) and the severity of impact (Impact) of each risk factor, the results are used to calculate and determine the risk level in the risk level table. This allows the organization to identify high-risk items for priority management, determine appropriate risk controls, and enable the organization to plan and allocate resources correctly within limited budgets, personnel, or time.

Color	Meaning	Risk Level
Red	Very High Risk	16 – 25
Orange	High Risk	12 – 15
Yellow	Medium Risk	8 – 10 or Impact or Likelihood (either one) is level 5 or higher
Green	Low Risk	4 – 6
White	Very Low Risk	1 - 3

Table of Risk Levels

After prioritizing the risks that need management, the working group may summarize the overall risk picture in the form of a Heat Map to present to senior management for an overview of the organization's risks.



Impact	1	2	3	4	5
5	🟨	🟨	🟧	🟥	🟥
4	🟨	🟨	🟧	🟥	🟥
3	🟩	🟩	🟨	🟧	🟧
2	⬜	🟩	🟩	🟨	🟨
1	⬜	⬜	🟩	🟨	🟨
	Likelihood				

Risk Diagram in the form of a Heat Map

(6) Risk Profile Development

Once all risk levels have been obtained, the working group should develop a Risk Profile to use as a reference for risk management in the organization. The risk identification method should specify events that have or may have an impact on the organization, whether positive or negative. In addition, the working group should identify the actual causes that cause or may cause those events, so that the working group can accurately identify appropriate measures or controls.

3.3 Risk Management and Risk Management Plan Development (Risk Responses)

After assessing risks and prioritizing them, risk response measures or risk management plans will be determined. This involves finding appropriate ways to manage each remaining risk. There are 4 risk management strategies, collectively known as the 4T's STRATEGIES:

(1) Take – Risk Acceptance: Accepting the remaining risk because the cost of management or control system creation may be higher than the results obtained. However, monitoring and care measures should be in place, such as setting acceptable impact levels and preparing contingency/risk management plans.

(2) Treat – Risk Reduction/Control: Designing additional control systems or revising existing control systems to reduce the severity of the remaining risk. This may involve reducing the impact or likelihood of the event, such as installing safety equipment, providing training to develop skills, and implementing proactive measures.

(3) Terminate – Risk Avoidance: Stopping or changing activities that cause the risk, such as eliminating unnecessary steps that lead to risk, changing work patterns, and reducing investment.

(4) Transfer – Risk Sharing/Spreading: Distributing assets or processes to reduce losses, such as insuring assets to transfer risk to insurance companies, outsourcing certain tasks, making multiple copies of documents, and diversifying the storage of valuables.

Then, develop management plans that address the causes of those risks. Consider whether existing control measures adequately address the causes or whether additional control measures are needed to manage the remaining risks. A single management plan may address multiple causes or manage other risks, and a single cause may have more than one management plan.

However, there is no fixed rule on which plans should be implemented, as it depends on the organization's suitability and readiness. The selection of plans should consider the following principles:

(a) A good risk management plan should be quick to implement, have a low budget, and be effective in reducing, controlling, or preventing risk.

(b) Be cautious that the risk management plan does not cause other damage or disrupt work.

3.4 Reporting and Monitoring

This involves monitoring after the risk management plan has been implemented to ensure its effectiveness. Reporting and monitoring are necessary and beneficial for risk management because they:

(1) Ensure that the risk management plan is implemented correctly and effectively.

(2) Identify errors that may occur after using the risk management plan.

(3) Enable adjustments and revisions to the risk management plan to align with changing circumstances or if the original plan is ineffective.

(4) Provide quarterly reports to assigned management.

The company has defined performance evaluation guidelines in 2 ways:

(1) *Ongoing Monitoring:* Evaluating performance during implementation of the risk management plan to monitor whether processes are being carried out according to the defined control measures/activities and whether they can reduce existing or potential risks, or whether events, situations, or changes occur beyond what was anticipated. This is then presented to the Sustainability and Risk Management Committee and the Risk Management Working Group to adjust the risk management plan and make timely corrections. The frequency of monitoring control activities is semi-annually, and in special cases, if significant changes are found, a special meeting of the Sustainability and Risk Management Committee may be held.

(2) *Separate Evaluation*: Evaluating performance by reporting at the end of a defined period or in special cases. The main department responsible for managing any risk will be responsible for evaluating its own risk management efficiency. The scope and frequency of evaluation will depend on the defined schedule, with evaluations including:

(a) Whether the defined control measures/activities have been fully and completely implemented.

(b) Whether the implementation of control activities can reduce risk effectively and efficiently.

(c) Whether there are any shortcomings or situations that affect risk management that should be addressed, corrected, or improved.

In addition, risk should be reassessed at least once a year to see if any risks are at an acceptable level or if any new risks have emerged. This may include a plan of action and tools for reporting, monitoring, and evaluating risk management performance, including:

- Creating a risk matrix to show the level of risk occurring at both the organizational level and the office/group level for monitoring and evaluating risk management.
- Developing a Risk Profile and risk ranking to show all risks ranked by risk level, which will change according to the defined risk management measures.
- Reporting on the progress of risk management guidelines can be done using a risk management guideline tracking form to monitor additional risk management measures on a monthly or quarterly basis, or as appropriate, by identifying the progress of risk management.

It can be seen that the development of a risk management system must be done continuously and consistently, with regular checks and monitoring, to be truly beneficial.

3.5 Factors Contributing to Successful Risk Management

(1) Consistent adherence to the risk management process.
(2) Having a change management process.
(3) Effective communication.
(4) Measuring risk management performance, including risk measurement.
(5) Training and human resource mechanisms to ensure all employees understand the risk management framework and responsibilities.
(6) Monitoring the risk management process with appropriate methods.

3.6 Factors Leading to Risk Management Failure

(1) Lack of support from middle and senior management.
(2) Lack of a clear vision in strategic planning.
(3) Failure to communicate the vision and future developments to all employees.
(4) Failure to build a powerful support team from top to middle management.
(5) Viewing everything as an obstacle or people in the organization as hindering progress towards the vision.
(6) Failure to define short-term winning strategies for the organization will lead to long-term failure.

Chapter 4
Miscellaneous

(1) Any amendment, improvement, or change to this document under any circumstances can only be made with the approval of the Board of Directors.

(2) This Risk Management Manual shall become effective from November 26, 2015, onwards until there is a written change otherwise.

By resolution of the Board of Directors Meeting No. 5/2015 on November 25, 2015.

(Mr. Pimol Srivikorn)
Chairman