นโยบายการบริหารความเสี่ยง

(Risk Management Policy)

Kijcharoen Engineering Electric Public Company Limited

Creator

(Pongsakorn Prawetwattanakul)

Company Secretary

Approver

(Varut Taymeya)

Chairman of the Risk Management Committee

KIJCHAROEN ENGINEERING ELECTRIC PLC

History of Document Amendments

Revision No.	Date	Details	Approver
00	30 March 2022	Initial Issue	Risk Management Committee
01	6 June 2022	Add Risk Assessment Information	Risk Management Committee
02	20 February 2025	1) Revise the format / Adjust the layout 2) Regroup headings to align with the content 3) Move the "Policy Review" section to item 1.5	Risk Management Committee
03	20 February 2026	Annual Review	Risk Management Committee

Introduction

Kijcharoen Engineering Electric Public Company Limited (**"the Company"**) recognizes the importance of risk management in its governance and operational systems. The Company aims to embed risk management as a core culture for all employees. Effective risk management not only helps the organization achieve its key objectives and targets but also supports the Company in creating tangible value. To ensure that all departments operate under a unified approach to risk management, the Risk Management Committee has established this Risk Management Policy. This policy serves as a guideline for all employees in managing risks, promoting organization-wide alignment in risk management practices, and maximizing benefits to the Company.

Risk Management Committee

KIJCHAROEN ENGINEERING ELECTRIC PLC

Table of Contents

นโยบายการบริหารความเสี่ยง

Risk Management Policy

1. Guidelines and Benefits of Risk Management

1.1. Definitions

"**Risk Management**" refers to the process of managing risks in the Company's operations in alignment with its established objectives. The Company establishes systems and structured practices for risk management to ensure that risks affecting the Company are managed at a level and scale that are acceptable. This includes systematic assessment, control, and monitoring, with a primary focus on achieving the Company's objectives.

"**Risk**" refers to any event or action that may occur under uncertain circumstances and that could create an impact, cause damage, failure, or reduce the likelihood of achieving the Company's defined goals and objectives. The impacts may be financial, reputational, or affect the Company at the organizational, departmental, or individual level.

"**Personnel**" refers to all managers, department heads, and employees within the organization.

1.2. Objectives of Risk Management

1.2.1. To manage obstacles and challenges in the course of business operations.

1.2.2. To prevent or reduce the likelihood of undesirable events and their potential impacts, which could hinder the achievement of the organization's objectives and goals.

1.2.3. To promote good corporate governance and provide assurance that the Company has clearly defined responsibilities for managing the identified risks appropriately.

1.3. Scope of Risk Management

To ensure continuity of operations and the achievement of the Company's objectives, all departments are required to implement risk management. Risk management should be integrated as a part of the daily operations of all employees, with the aim of embedding risk management as an integral element of the organizational culture.

1.4. Risk Management Policy

All departments must implement risk management in a systematic and continuous manner under a standardized risk management process. Information technology should be utilized to facilitate rapid communication and processing. Additionally, risk management activities must be regularly monitored and evaluated, with risk management plans adjusted periodically to ensure that objectives are achieved.

1.5. Policy Review

The Risk Management Policy must be reviewed annually and submitted to the Company's Board of Directors for approval.

1.6. Benefits of Risk Management

When the Company implements effective and appropriate risk management, it directly gains the following benefits:

1.6.1. Ensures that the Company's operations achieve its established objectives and goals, while promoting continuous and sustainable business growth, creating added value for the Company and its stakeholders, and supporting good corporate governance.

1.6.2. Enhances employees' knowledge and awareness of the importance of risk management, leading to increased caution in operations and reducing the likelihood of operational losses.

1.6.3. Enables the Company to incorporate risk analysis results into decision-making

when planning and executing projects that may impact the Company.

1.6.4. Improves the completeness and feasibility of setting the Company's objectives and strategies, ensuring alignment with acceptable levels of risk.

1.6.5. Promotes preparedness and development of mitigation strategies for potential issues that could affect the Company's operational performance.

1.6.6. Provides an information technology system that supports accurate, complete, and timely data collection, calculations, reporting, and verification.

1.6.7. Provides management with reliable information to support faster and more accurate decision-making.

1.6.8. Facilitates appropriate allocation of resources, considering the cost-effectiveness of investments.

1.6.9. Encourages employee engagement and integration with other organizational systems, collectively driving the organization toward achieving its objectives.

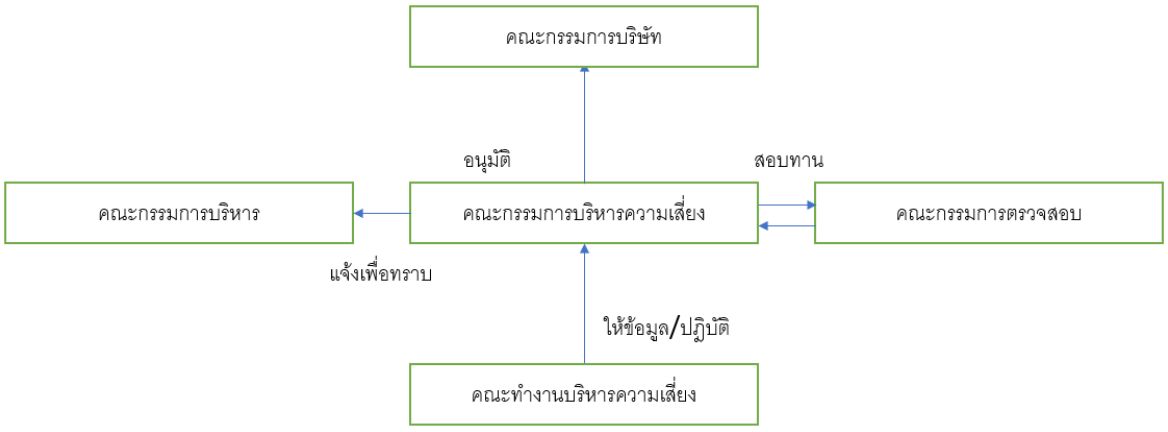
2. **Company's Risk Management Structure**

The risk management structure consists of the Risk Management Committee and risk management working teams at the departmental level as follows:

2.1. Organizational Level The Risk Management Committee, chaired by the Chairman of the Risk Management Committee, is responsible for duties and responsibilities in accordance with the company's risk management practices.

2.2. Departmental Level ("Working Teams") This includes division managers, department managers, and all employees within the organization, who perform risk management activities under the supervision of the Risk Management Committee.

Figure 1 Risk Management Structure



3. Roles and Responsibilities of Committees in the Risk Management System

3.1. Roles and Responsibilities of the Risk Management Committee

The Risk Management Committee is entrusted with the following duties and responsibilities:

3.1.1. Define the overall risk management policy and structure of the company, covering key risks such as financial risks, investment risks, and risks that may affect the company's reputation. These policies are proposed to the Board of Directors for approval, ensuring alignment with the risk management guidelines of the Stock Exchange of Thailand and the Institute of Internal Auditors of Thailand.

3.1.2. Establish strategies and approaches for risk management in accordance with the company's risk management policy. This ensures that each type of risk can be assessed, monitored, and controlled to an acceptable level, with active participation from relevant departments in managing and mitigating risks.

3.1.3. Oversee and monitor compliance with approved risk management policies and frameworks endorsed by the Board of Directors.

3.1.4. Set risk assessment criteria and determine the acceptable risk appetite for the company.

3.1.5. Define appropriate measures for managing risks in response to prevailing circumstances.

3.1.6. Assess organizational-level risks and establish management approaches to keep risks within acceptable thresholds, while ensuring effective implementation of risk management practices.

3.1.7. Review and update risk management policies regularly to ensure their adequacy, efficiency, and effectiveness in controlling risks.

3.1.8. Exercise authority to request explanations from relevant personnel, appoint responsible parties, and assign risk management duties to all operational levels as appropriate, with reporting to the Risk Management Committee to ensure objectives are achieved.

3.1.9. Report on the company's risk management operations, overall risk profile, significant changes, and required corrective actions to the Audit Committee for review, and subsequently to the Board of Directors on a regular basis.

3.1.10. Prepare the annual corporate risk management handbook.

3.1.11. Implement an integrated risk management system linked with information technology systems.

3.2. Roles and Responsibilities of the Risk Management Working Teams

The Working Teams are responsible for the following:

3.2.1. Adopt the company's risk management guidelines and develop risk mitigation plans relevant to their areas of responsibility.

3.2.2. Implement and report on risk management activities in line with the directions outlined by the Risk Management Committee and as specified in the company's "Annual Corporate Risk Management Handbook".

3.2.3. Assess and prepare departmental or divisional risk management reports for submission to the Secretary of the Risk Management Committee within the prescribed timeframe, under the supervision of the Risk Management Committee.

3.2.4. Carry out any other duties as assigned by the Risk Management Committee.

3.3. Roles and Responsibilities of the Audit Committee

3.3.1. Review the company's risk management policies and the Corporate Risk Management Handbook to ensure that the company has an appropriate and effective risk management system in place to support good corporate governance.

3.3.2. Independently monitor the company's risk management practices.

3.3.3. Communicate with the Risk Management Committee to ensure understanding of key risks and their linkage with internal controls.

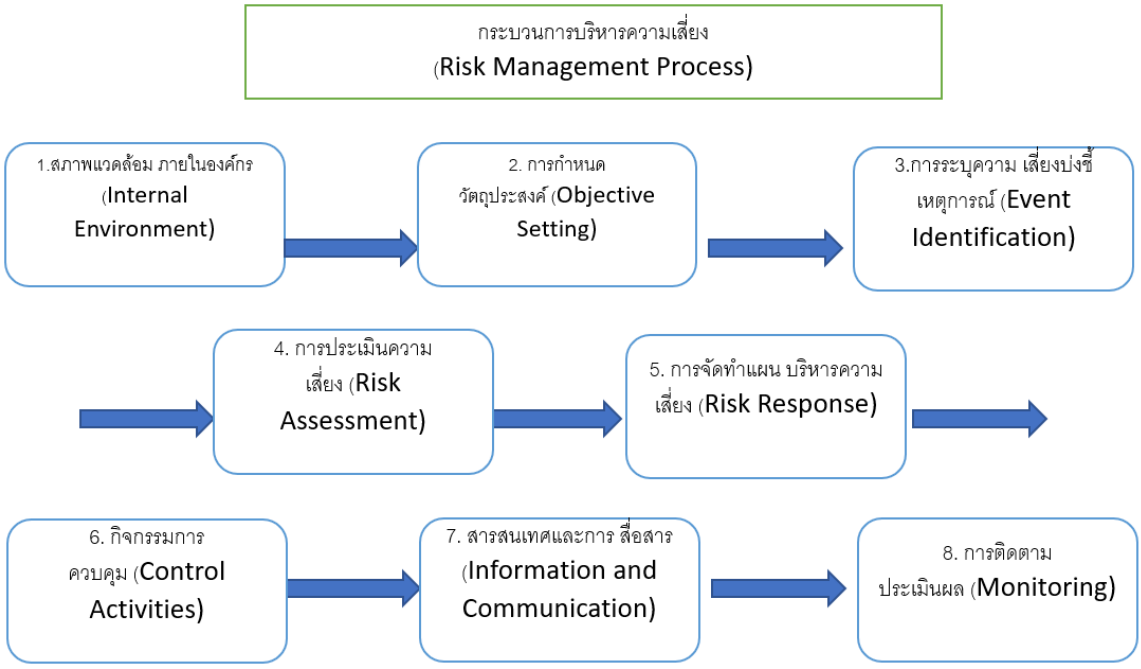
3.4. Roles and Responsibilities of the Internal Audit Function

The Internal Audit function is responsible for reviewing and assessing the effectiveness of the company's risk management processes to ensure that the risk management system is appropriate and contributes to effective corporate governance.

4. Risk Management Process Based on the COSO Framework

The Company has adopted the Enterprise Risk Management – Integrated Framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as a guideline for enterprise risk management. Under this framework, all departments are required to continuously follow an eight-step risk management process, as outlined below:

Figure 2 Risk Management Process



4.1. Step 1: Internal Environment Analysis

The organizational environment is a critical component in establishing the risk management framework. It comprises several factors such as corporate culture, management policies, employee practices, work processes, and information systems.

The internal environment forms the foundation for defining the organization's risk management direction. At this stage, the process involves identifying the internal environment, where data is collected from user responses to questionnaires and analyzed to generate reports.

The company should foster an enabling environment and atmosphere that serves as the basis for other stages of enterprise risk management. Without a strong internal environment, the company's strategy and objectives may be negatively affected. Therefore, it is necessary to establish activities for risk identification, assessment, and management. Key components of the internal environment include:

(1) Philosophy, beliefs, and risk management culture aimed at creating long-term

value for the company.

(2) The role of the Audit Committee as a key factor in overseeing risk management.

(3) Recruitment of competent and ethical personnel, along with their continuous development to match assigned responsibilities.

(4) Establish an appropriate organizational structure

Define appropriate roles, responsibilities, and authorities to enable employees to perform their duties effectively and achieve the company's objectives.

4.2. Step 2: Objective Setting

At this stage, users are required to record the plans or projects of their departments, clearly specifying the objectives, organizational-level indicators aligned with those plans or projects, the strategic issues supported, and the main activities under each plan or project, along with the control objectives of each key activity. This ensures clarity of scope at every level and allows for a comprehensive risk analysis. Therefore, effective risk management objectives at the departmental level should be aligned to achieve the overall organizational goals, with the following characteristics:

4.2.1. Objectives must be clear, measurable, achievable, reasonable, and time-bound, in line with the "SMART" principle:

Specific: Clearly defined and precise

Measurable: Quantifiable and assessable

Achievable : Realistic and attainable

Reasonable : Rational and aligned with practical constraints

Time Constrained: Defined within a specific timeframe

4.2.2. Objectives must be linked to corporate goals, aligned with departmental indicators, and consistent with the company's accepted level of risk (Risk Appetite) and its permissible level of deviation (Risk Tolerance).

Risk Appetite refers to the types and levels of risk that the company is willing to accept in order to achieve its vision and mission.

Risk Tolerance refers to the degree of variation from the defined risk appetite that the company is willing to allow.

4.3. Step 3: Risk Identification / Event Identification

At this stage, the company collects potential events that may affect each department, covering both internal and external risk factors. These may include management policies, personnel, operations, financials, information systems, regulations, laws, accounting systems, and taxation. The purpose is to fully understand the possible events and circumstances so that management can define effective strategies and policies to address potential risks. The risk identification process involves the following steps:

4.3.1. Review activities, projects, and processes under the company's annual operational plan, annual business plan, and other initiatives that could prevent objectives and targets from being achieved.

4.3.2. Identify risks and their causes by considering both internal and external factors that could hinder the achievement of objectives at the activity, project, or process level.

4.3.2.1. Risk Identification Methods

(1) Workflow and document analysis, or process analysis

(2) Brainstorming

(3) Workshops

(4) Collection of past incident and loss data

(5) Others

4.3.2.2. Internal Risk Factors may arise from:

(1) Company objectives

(2) Policies, strategies, and operational processes

(3) Organizational structure and management systems

(4) Accounting and financial information

(5) Others

4.3.2.3. External Risk Factors may arise from:

(1) Government policies

(2) Economic conditions

(3) Competition within the industry

(4) Laws, regulations, and compliance requirements

(5) Natural disasters, wars, or pandemics

(6) Others

4.3.3. Risk Classification can be categorized into seven major types:

4.3.3.1. Strategic Risk: Arising from inappropriate strategic planning or execution, as well as misalignment between policies, strategic goals, organizational structure, and market competition.

4.3.3.2. Operational Risk: Arising from day-to-day operations, including risks related to processes, technology, equipment, and personnel.

4.3.3.3. Compliance Risk: Stemming from the inability to comply with laws, rules, or regulations, or from regulations that are inadequate or obstructive to business operations.

4.3.3.4. Fraud Risk Governance: Reflecting the “Tone at the Top” from the Board in anti-corruption efforts. The Audit Committee proactively monitors fraud risk management (FRM), while management establishes and implements a Fraud Risk Management Program (FRMP). Employees must be trained to recognize “red flags” and report potential fraud immediately. Internal Audit is responsible for assessing FRMP effectiveness to provide assurance to the Board.

4.3.3.5. ความเสี่ยงด้านเทคโนโลยีสารสนเทศมีความเสี่ยงหลักๆ ดังนี้ Information Technology Risk: Including risks such as:

(1) System unavailability (Availability)

(2) Unauthorized access to data or systems (Access)

(3) Inaccuracy or outdated data (Accuracy)

(4) Lack of agility in adapting IT systems to support business strategy (Agility)

4.3.3.6. Financial Risk: Risks that could lead to financial volatility, both directly and indirectly, such as:

(1) Weakness in banking and financial institutions

(2) Market downturns and asset depreciation

(3) Ineffective financial system governance

(4) Accounting standards affecting accuracy of financial reporting

(5) Public fiscal conditions

(6) Responsiveness of financial institutions to market volatility

(7) Implementation of Basel II or other international financial stability standards

4.3.3.7. Economic, Social, and Political Risk:

(1) Economic Risk

This refers to the possibility of national economic weakness at a fundamental level, which may negatively affect business performance, revenue stability, and business volume. In general, economic risk factors include economic growth or slowdown, the financial and fiscal status of the government, international trade transactions, balance of payments, and overall economic growth and stability trends.

(2) Social Risk Management

Global interconnectedness has given rise to increasing social risks, both directly and indirectly. This is particularly evident in the

growing interdependence between nations in trade, supply chains, cross-border financial flows, labor migration, and communication technologies that have removed barriers to information exchange.

At the domestic level, new patterns of interaction are also emerging. For example, governments may ask the private sector to provide public goods or services such as education or security systems. Conversely, the private sector may request NGOs to safeguard intellectual property rights, while NGOs may demand that private companies uphold human rights. Such interdependencies create new forms of social risk, requiring businesses to adopt approaches beyond traditional strategies.

Social risk for businesses generally arises from four key elements:

- Social and environmental issues: For example, global climate change, disease outbreaks, or rural-to-urban migration.
- Expanded stakeholder expectations: New stakeholders beyond traditional groups, such as environmental organizations, child and women's rights groups, and even individuals with growing influence in social advocacy.
- Negative public perception: The spread of unfavorable information about the company through news outlets, social media, or even disclosures by internal personnel, which can lead to accumulated negative sentiment.
- Channels of reputational damage: Dissemination of opinions through small and large networks, such as forwarded emails, public commentary, boycotts, or protest campaigns.

(3) Political Risk

This refers to the possibility of inefficient government administration, which may include:

- Frequent changes in government leadership or instability in state governance
- Social division and unrest, including political protests or riots
- Inadequate law enforcement systems
- Localized unrest in specific areas
- International political conflicts
- Weakness in national security infrastructure
- Inappropriate or inconsistent government policies

4.4. Step 4: Risk Assessment

Risk assessment involves identifying and prioritizing existing risks by evaluating both their likelihood of occurrence (Likelihood) and potential impact (Impact). Risks may be assessed based on both external and internal factors affecting the organization.

In essence, risk assessment measures the severity of risks to determine their significance. Risks identified in Step 3 (Risk Identification) are evaluated using the following process:

4.4.1. Assess risks arising from operations prior to implementing risk control measures. This step considers the severity and likelihood of risks before applying any control measures, referred to as Inherent Risk.

4.4.1.1. Assessing the severity of risk impacts (Severity of Impact). This involves evaluating the level of severity from multiple perspectives, including:

(1) Customer Satisfaction Perspective

Severity Level	Description of Damage/Impact	Score
Very High	Significant disruption to delivery, making it impossible to deliver products to customers due to process shutdowns	5
High	Major impact on delivery, causing delays in product delivery and resulting in formal written complaints from customers	4
Medium	Moderate impact on delivery, causing delays in product delivery and leading to verbal complaints from customers	3
Low	No customer complaints regarding delivery, but inconvenience in the delivery process occurs (e.g., increased transportation costs), resulting in failure to achieve company objectives	2
Very Low	No impact on delivery; operations proceed according to plan	1

(2) Company Reputation Perspective

Severity Level	Description of Damage/Impact	Score
Very High	News about the company is published in more than 3 media outlets, including online media or newspapers	5
High	News about the company is published in 3 media outlets, including online media or newspapers	4
Medium	News about the company is published in 2 media outlets, including online media or newspapers	3
Low	News about the company is published in 1 media outlet, including online media or newspapers	2
Very Low	No news about the company is published	1

(3) Business Continuity Perspective

Severity Level	Description of Damage/Impact	Score
Very High	Company operations or internal processes are halted for more than 1 month	5
High	Significant impact on company processes and operations, lasting approximately 2–4 weeks	4
Medium	Noticeable disruption to company processes and operations, lasting approximately 1–2 weeks	3
Low	Minor impact on company processes and operations, lasting approximately 3–7 days	2
Very Low	No disruption to company processes and operations	1

(4) Information Technology & Systems Perspective

Severity Level	Description of Damage/Impact	Score
Very High	Complete loss of critical IT systems, causing significant damage to customer or business data security	5
High	Issues with critical IT systems and security, affecting the accuracy of some data	4
Medium	System problems occur with limited loss	3
Low	Minor incidents that can be resolved	2
Very Low	Insignificant incidents	1

(5) Product or Service Quality Perspective

Severity Level	Description of Damage/Impact	Score
Very High	- Product or service quality fails to meet critical requirements or is non-compliant with legal regulations - Causes significant reputational damage, fines, legal complaints, or business closure	5
High	- Product or service quality significantly fails to meet requirements, causing customer dissatisfaction - Leads to complaints, legal claims, or fines from customers	4
Medium	- Product or service quality moderately fails to meet requirements, causing some customer dissatisfaction, but parts of the product/service meet acceptable quality standards. - Impacts downstream departments, causing dissatisfaction in related units. - Subsequent processes experience deviations, delays, and increased costs (affecting the relevant departments).	3
Low	- Product or service quality slightly fails to meet requirements but is acceptable to customers - Affects departments, requiring corrective actions during the process	2
Very Low	- No impact on product or service quality - No damage to the company or stakeholders	1

4.4.1.2. Consideration of Risk Likelihood

The likelihood of potential risks is assessed from two perspectives: the company's reputation (L1) and the operational process image within the company (L2), as shown in the table below.

Likelihood of Potential Risk			
Likelihood	**Definition**	**Average Frequency**	**Score**
Very High	Very frequent	Once a month or more	5
High	Frequent	Once every 1–6 months, but not more than 5 times per year	4
Medium	Infrequent	Once a year	3
Low	Rare	Once every 2–3 years	2
Very Low	Possible	Once every 5 years	1

4.4.2. Risk assessment involves analyzing both the likelihood of a risk occurring (Likelihood) and the severity of its impact (Impact) based on the established criteria for assessing risk likelihood and impact severity. This assessment can be conducted both qualitatively and quantitatively. The company has defined a five-level scale for evaluation. The "Risk Level" is calculated as the product of the average Likelihood and the average Impact.

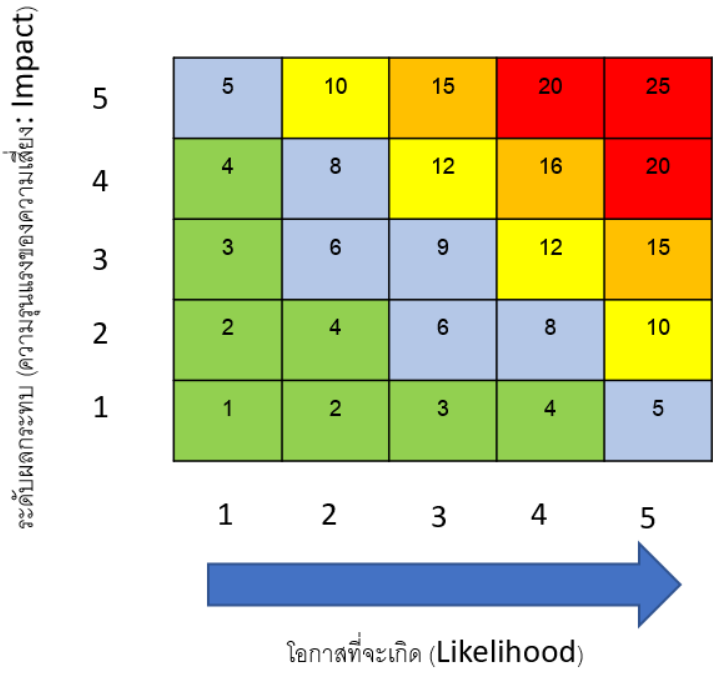
4.4.3. The **"Risk Level"** assessed according to section 4.2 is ranked by importance into 5 levels as follows:

Risk Level	Risk Score	Description	Impacted Events	Management Timeframe
Level 5 – Extremely Risk (E)	20-25 Very High	Very high; unacceptable level, requires immediate action to reduce risk to an acceptable level	- Employee or personal safety -Illegal actions - Significant damage to assets -Actions affecting company reputation -Lack of internal control	Immediate action; to be controlled within 1 month
Level 4 – High Risk (H)	15-19 High	High; unacceptable level, requires risk management to bring it to an acceptable level	-Operational activities not meeting objectives -Lack of adequate internal control -Damage to assets	Within 1 month
Level 3 – Moderate Risk (M)	10-14 Medium	Moderate; acceptable level, requires effort to reduce risk to an acceptable level	- Lack or inefficiency of internal controls - Financial statements or reports are inaccurate or inappropriate	Within 4 months
Level 2 – Low Risk (LR)	5-9 Low	Low; acceptable, but controls needed to prevent risk from escalating	Events affecting financial statements or internal controls with moderate operational impact	Within 6 months
Level 1 – Least (L)	1-4 Very Low	Minimal; acceptable, no additional risk management required	Events affecting financial statements or internal controls with minor or insignificant operational impact	Use existing internal controls or within 12 months

Risk assessment must be conducted both before implementing the risk management plan and after executing the risk management plan. This allows the organization to determine the effectiveness and efficiency of the risk management plan and to decide whether the plan needs to be reviewed or improved.

The Risk Matrix and acceptable risk levels are defined by the Risk Management Committee, with the acceptable risk level set at no more than Level 5.

Figure 4 Risk levels and impacts table



4.5. Step 5: Developing a Risk Response Plan (Risk Response)

This step is carried out after the organization has identified its risks and assessed their significance. The identified risks must be addressed with appropriate response measures to reduce potential losses or the likelihood of impacts to an acceptable level for the organization.

Developing a risk response plan means defining actions to reduce the likelihood of loss, using the results of the risk assessment from Step 4. The plan is prepared based

on the priority of risks, with the risk-owning unit responsible for developing the plan. This unit is most familiar with the risks associated with its operations and will analyze potential mitigation measures, using one or more methods to reduce the likelihood of occurrence and/or minimize impact to a level acceptable to the unit. The outcome is the unit's risk management plan.

4.5.1. Risk Response Methods (AT Methods): Responsible personnel should analyze how to manage the identified risks using the following approaches:

(1) Take – Risk Acceptance (Risk Acceptance): Accept the risk when the cost of control measures or systems may exceed the benefits. However, monitoring and oversight measures should be in place, such as defining an acceptable impact level and preparing contingency plans.

(2) Treat – Risk Reduction / Control (Risk Reduction / Control): Design control systems or improve operations to prevent or limit impact and the likelihood of loss. Examples include installing safety equipment, training to improve skills, or implementing proactive measures.

(3) Terminate – Risk Avoidance (Risk Avoidance): Stop or change activities that pose risks, such as eliminating unnecessary steps that create risk, modifying workflows, or reducing operational scope.

(4) Transfer – Risk Sharing / Spreading (Risk Sharing / Spreading): Distribute or transfer risk through assets or processes to reduce potential loss. Examples include insuring assets, outsourcing some tasks, creating duplicate document copies, or distributing valuable assets across locations.

Note: The choice of risk response must consider the cost of implementation versus the potential damage.

4.5.2. Developing a Risk Action Plan for High-Risk Cases. For risks assessed as High to Very High, responsible personnel should jointly prepare a risk management plan using the following steps:

(1) Identify alternative measures from the 4T methods to ensure residual risks

remain at an acceptable level and align with objectives.

(2) Compare feasibility and costs of each alternative, considering both financial and non-financial investment value. Implementation costs should not exceed the expected damage.

(3) Select the best method, assigning responsibilities, timeline, budget, and preparing an actionable implementation plan.

4.6. Step 6: Establishing Control Activities (Control Activities)

Control activities refer to the policies and procedures established by management to ensure that the risk management or risk response plans are effectively implemented. These activities specify responsibilities and timelines for actions and serve as a method to manage or mitigate risks.

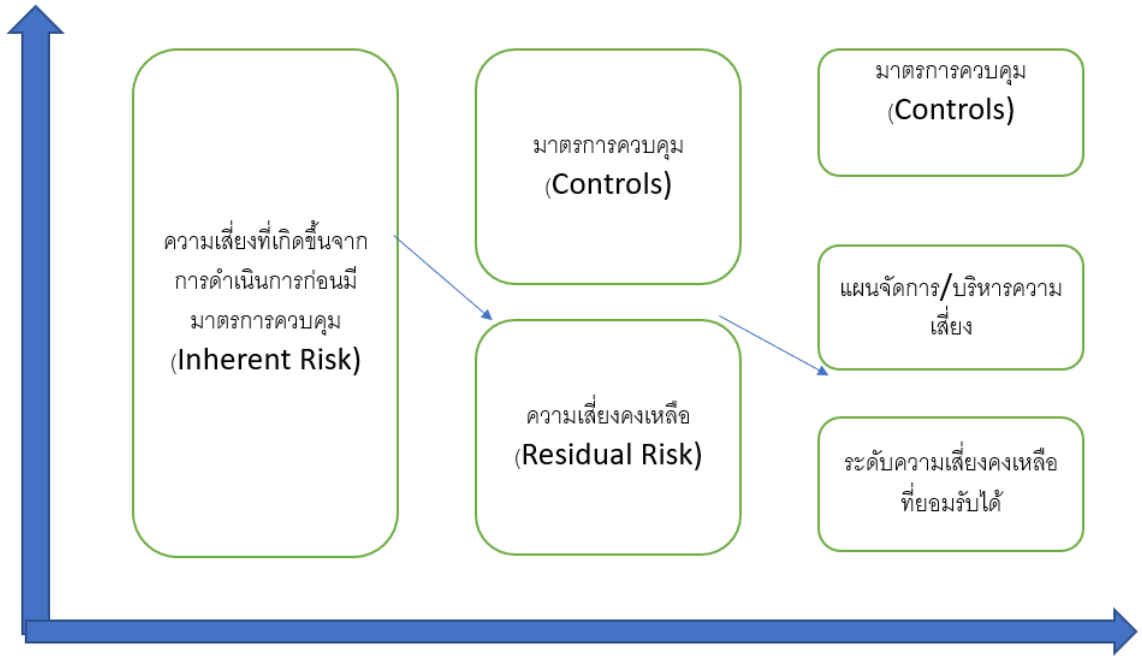
Control activities involve defining tasks and operations designed to reduce risk and ensure that organizational objectives and goals are achieved. Examples include establishing operational procedures related to risk management for staff, ensuring that risks are addressed properly and objectives are met.

The most effective control activities should be integrated into processes, preventing and mitigating risks to an acceptable level, while ensuring that the cost of implementation does not exceed the expected damage.

Clearly defining control activities ensures that the risk management plan achieves its objectives. This involves setting policies, procedures, responsible personnel, and timelines. In some cases, additional internal control processes may be established, such as reviews, supervision, and segregation of duties.

Control activities are a component of the internal control system, often in the form of suggestive controls, aimed at improving operational and internal control systems. These activities are designed to reduce risks, ensure cost-effectiveness, and give management confidence in the effectiveness of existing internal controls.

Figure 5 Reduction of risk as a result of control activities



4.7. Step 7: Information and Communication

The organization must have an effective information and communication system, as it serves as a fundamental basis for managing risk according to the organizational framework and procedures. This system enables reporting on risk management at both the departmental and organizational levels, based on information gathered from Steps 1 to 6. Reports are mainly divided into two parts: Internal control reports and Risk management reports, which summarize the risks and risk management actions at the departmental level (including sub-department risk management plans).

Additionally, the company should ensure that the information and communication system supports achieving organizational objectives by:

(1) Clear communication from the Board of Directors and senior management regarding the risk management policy, ensuring all employees understand their roles and responsibilities in managing risk. This helps adjust behaviors and activities so that risks remain at an acceptable level.

(2) Identifying sources and collecting information from both internal and external sources, storing and communicating it in a structured manner within a specified

timeframe, so that managers and employees are informed promptly and can perform risk management communication consistently and effectively.

4.8. Step 8: Monitoring and Evaluation

The organization must monitor and evaluate risk management to determine whether it is appropriate and effective.

Monitoring and evaluation refer to the process of quality control of operations and assessment of additional risk management plans or control activities continuously and consistently. Responsible personnel monitor during operations and conduct periodic evaluations as appropriate to ensure effective and efficient risk management.

After monitoring and evaluation, progress, problems, and obstacles in risk management must be reported to the Risk Management Committee to guide the review or improvement of risk management plans.

The risk management report prepared by the committee should include:

(1) Summary of risk factors and risk levels

(2) Existing controls and residual risk management measures

(3) Departments/responsible personnel and the results of risk levels after control

(4) Risks exceeding acceptable limits

(5) The top 5 highest risks

(6) Events that, even if unlikely, could affect:

- Employee or public safety, or involve illegal acts
- Significant damage or impairment to assets
- Departmental reputation
- Inaccurate financial statements or reporting

(7) Reports to senior management or the Board of Directors