Risk Management Handbook

Northeast Rubber Public Company Limited

Year 2025

398 Moo.4 Kok Ma
Sub-district,
Prakhonchai District,
Buriram 31140

044-666928-9

ner@nerubber.com

www.nerubber.com

Foreword

Northeast Rubber Public Company Limited recognizes the importance of risk management as a crucial tool that enables the organization to effectively and efficiently achieve its stated goals and objectives. Good risk management not only helps reduce the likelihood of damage to the organization but also increases opportunities for creating added value in the company's operations amidst volatile economic conditions and rapid global changes. Northeast Rubber Public Company Limited's risk management adheres to the principles of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework to manage risks to an appropriate or acceptable level for the organization.

On this occasion, the Risk Management Committee of Northeast Rubber Public Company Limited has prepared this Risk Management Handbook to serve as a guide for personnel at all levels of Northeast Rubber Public Company Limited to understand the importance and process of risk management, and to apply it until it becomes an organizational culture, leading to the organization's stability and strength.

Risk Management Committee

Northeast Rubber Public Company Limited

Table of Contents

Chapter 1 Organizational Information

History of Northeast Rubber Public Company Limited

Northeast Rubber Public Company Limited (NER) was established and registered on June 12, 2006, and transformed into a public company on June 8, 2018. The company manufactures and distributes Ribbed Smoked Sheet (RSS), Standard Thai Rubber (STR), and Mixtures Rubber to automotive industry manufacturers and intermediate traders, both domestically and internationally, including the People's Republic of China, Japan, Singapore, Bangladesh, and India. Additionally, the company provides rubber quality analysis and testing under its own operations, in accordance with the Rubber Control Act B.E. 2542 (1999). The company is also committed to producing products that meet international standards and continuously improving quality, thereby producing high-quality rubber that is recognized by customers both domestically and internationally.

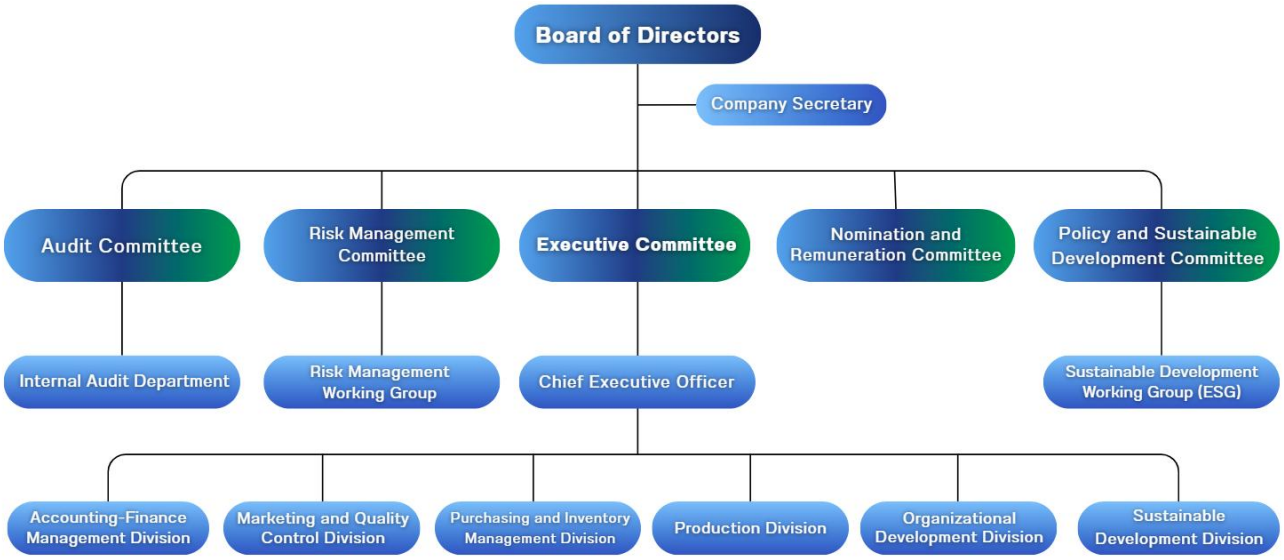
Vision

"To be a leader in natural rubber production, developing the business towards downstream industries with social and environmental responsibility, aiming for sustainable carbon neutrality."

Mission

- To produce and deliver quality products at efficient costs.
- Committed to promoting stakeholders to achieve carbon neutrality.
- Committed to research and development to increase the diversity of finished products.
- Develop the business for sustainable growth, considering environmental, social, governance (ESG), and stakeholder aspects.

Organizational Chart



Chapter 2 Importance of Risk Management

History of Risk Management

Enterprise Risk Management (ERM) is a process established and implemented by the board of directors, management, and personnel, to be applied in setting organizational strategies and planning at all levels. It is designed to identify potential events that may affect the organization and manage risks to an acceptable level, thereby providing reasonable assurance in achieving objectives.

Risk management is defined as one of the key performance indicators (Performance Criteria) to measure the efficiency of organizational operations. The evaluation of risk management considers various important factors, from building knowledge and understanding, risk analysis, risk management, good IT governance, risk management outcomes, and integrating risk management into the performance evaluation and compensation of the board of directors.

Objectives of Risk Management

1) To achieve good governance, ensuring that operations are conducted correctly and appropriately.
2) To enhance operational efficiency by controlling/preventing potential financial and non-financial damages through continuous learning/improvement/correction and development.
3) To ensure that the board of directors, management, and employees at all levels participate in applying risk management principles throughout the organization.
4) To ensure that Northeast Rubber Public Company Limited can operate to achieve its vision, mission, and goals within the organization's acceptable risk appetite and risk tolerance.

Objectives of the Risk Management Handbook

1) To provide executives and operational staff at all levels with knowledge and understanding of the principles, concepts, methods, processes, and steps of risk management, serving as a tool for controlling and supervising risk management throughout the organization.
2) To provide operational staff with guidelines, processes, and an understanding of effective risk management steps/methods.
3) To serve as a tool for communicating and building understanding about risk management at Northeast Rubber Public Company Limited, which will lead to reducing the likelihood and impact of potential risks.

4) To ensure operations align with the organization's policies, vision, mission, and goals, and to reduce the likelihood or impact of future events.

Meaning and Definition of Risk Management

To understand the meaning and definition of risk management, it is important to understand the meaning of related terms:

1. **Risk** Refers to any event or action that may occur in an uncertain situation and will affect or cause damage (both monetary and non-monetary), or lead to failure or reduce the opportunity to achieve organizational objectives or goals, in terms of strategy, operations, finance, and compliance with laws/regulations, which may also have a positive impact. This is measured by the impact received and the likelihood of the event occurring.

Characteristics of Risk

Risk can be divided into 3 parts:

1. Risk Factor: The cause that will lead to the risk.
2. Risk Event: An event that impacts operations or policy.
3. Risk Impact: The severity of the damage likely to result from the risk event.

2. **Risk Factor** Refers to the root cause or origin of a risk that may prevent the achievement of objectives according to defined operational steps, including both internal and external factors. It must be identifiable where, when, how, and why the event occurs. The true cause should be identified to enable accurate and appropriate analysis and determination of strategies/measures/approaches to reduce risk, suitable for the situation and organizational context.
3. **Risk Assessment** Refers to the process of identifying risks and analyzing them to prioritize risks that will affect the achievement of organizational objectives, by evaluating the likelihood of events occurring and their impact. Likelihood refers to the frequency or probability of a risk event, and impact refers to the severity of damage resulting from the event or risk. Once assessed, it determines the Degree of Risk, which refers to the status of risk derived from evaluating the likelihood and impact of each risk factor, divided into 5 levels: Very High Risk, High Risk, Medium Risk, Low Risk, and Very Low Risk.
4. **Risk Management** Is a process applied in defining organizational strategies at all levels, designed to identify potential events that may affect the organization and manage risks to an

acceptable level, providing reasonable assurance in achieving the organization's defined objectives.

There are 4 main strategies for risk management:

1. **Take (Risk Acceptance):** This involves analyzing and determining that no suitable risk management method exists because the cost of managing the risk is not sufficiently worthwhile, or resources are insufficient for implementation within the fiscal year. The risk may need to be accepted, but it should be closely monitored to prepare for potential consequences.
2. **Treat (Risk Reduction):** Reducing the likelihood of risk occurrence and/or the severity of the impact by finding additional methods to manage the risk, such as designing internal control systems, improving/correcting work processes/operations/monitoring, developing emergency plans, establishing safety standards, and providing training to develop skills.
3. **Terminate (Risk Avoidance):** Rejecting and avoiding opportunities for risk to occur by stopping, canceling, or changing activities or projects that could lead to a risk event. The disadvantage is that it may cause excessive changes in the organization's plans, preventing it from achieving its set goals.
4. **Transfer (Risk Sharing):** Shifting the burden of facing and managing risk events to others. This does not reduce the risk of occurrence but guarantees that the organization will be compensated by others in case of damage, such as purchasing insurance or outsourcing certain operations.

Enterprise Risk Management (ERM) Refers to the management of factors and control of activities, including various operational processes, to reduce the causes of each potential loss to the organization, keeping the level of risk and future impact within an acceptable, assessable, controllable, and systematically auditable range. This is primarily focused on achieving objectives in terms of strategy, compliance with regulations, finance, and the organization's reputation, with support and participation in risk management from all levels throughout the organization.

1. **Control**

Policies and practices that help ensure the implementation of planned risk responses. Control activities occur at all levels, functions, and throughout the organization, consisting of various activities

such as authorization, delegation of authority, segregation of duties, and performance reviews. They are divided into 4 types:

1.1 Preventive Control: Controls to prevent or reduce risks from errors or damages from the outset, such as segregation of duties.

1.2 Detective Control: Controls to discover damages or errors that have already occurred, such as reviews or counts.

1.3 Directive Control: Control methods that promote or motivate the achievement of desired objectives, such as rewarding good performers.

1.4 Corrective Control: Control methods to correct damages or errors that have occurred, or to find ways to prevent recurrence in the future.

2. Types of Risks

Risks are categorized into various groups for ease of identification, assessment, prioritization, and control. In developing the enterprise-level risk management system for Northeast Rubber Public Company Limited, risks are divided as follows:

2.1 Strategic Risk : This risk is related to achieving the organization's vision, mission, goals, and objectives. It is a long-term risk affecting the organization, potentially arising from management policies, unclear vision or mission, inadequate budget plans, inappropriate organizational structure lacking control systems, political interference, business decision-making, or economic downturns.

2.2 Operational Risk : This risk is related to day-to-day operational issues faced by personnel or arising from normal operations that the organization must confront to achieve strategic objectives. This type of risk often relates to organizational efficiency and effectiveness, such as:

- Operational Risk: Operations not adhering to the plan, inappropriate for the work nature, or inexperienced staff.
- Delegation of Authority Risk: Decentralization of power within the organization may enhance efficiency and speed, but it can also create problems if the chain of command is unclear, leadership in delegated roles is weak, or incentives for performance are insufficient for the authority granted.

- Technology Change Risk: Changes in technology can lead to operational problems for the organization, including switching to new computer hardware and software, changes in workflow, decommissioning old tools and programs, and database management.

2.3 **Financial Risk :** This risk is related to the organization's financial management and control, such as inappropriate budget allocation, erroneous budget setting, incorrect account classification, or lack of financial liquidity.

2.4 **Compliance Risk (Legal, Regulations, Rules) :** This risk relates to legal issues, regulations, rules, operational criteria, protection of service recipients or stakeholders, confidentiality of information, government policies, and other regulatory aspects.

2.5 **Fraud Risk :** This risk may lead to fraud within the organization, such as misuse of authority or assets for personal gain, family, friends, acquaintances, or any undue benefit, causing damage to the interests of others. Fraud can occur in various forms, including bribery of officials by giving or receiving monetary or non-monetary bribes, conflicts of interest, money laundering, concealment of facts, or obstruction of justice.

"The company has established a written anti-fraud policy. The company does not tolerate any form of fraud, covering all businesses and transactions in all countries and related entities."

Anti-Fraud Policy

The company places importance on combating all forms of corruption and fraud for direct or indirect benefit, whether as a recipient, giver, or offeror of bribes, monetary or non-monetary, to government agencies or private entities with which the company conducts business or interacts. The key principles are as follows:

1. The company does not offer compensation, pay bribes, demand, agree to, or accept bribes from other individuals or entities in any form, whether directly or indirectly, to reciprocate favors or expect benefits related to the company's work.
2. The company does not engage in illegal transactions involving government officials, individuals, or other entities, directly or indirectly.
3. The company does not donate money or provide any financial support to other individuals or entities as a channel for paying bribes.
4. The company does not provide financial or other benefits, directly or indirectly, to political parties, political groups, or any politically related individuals to gain benefits in business operations or for

their own and associates' interests.

The company adheres to ethics and morality as fundamental principles in conducting business and will not condone any actions that may lead to corruption and fraud, even if such actions benefit the company. To ensure that company personnel do not tolerate corruption and fraud, all company personnel must understand and strictly adhere to the anti-fraud policy, the Good Corporate Governance Handbook (Code of Conduct), work practices, relevant operational process manuals, and other company policies, without exception.

Chapter 3 Risk Management Policy and Principles

Risk Management Policy

Northeast Rubber Public Company Limited ("the Company") recognizes the importance of risk management and believes that it is a key approach to achieving organizational objectives and goals. Therefore, a systematic enterprise-wide risk management policy has been established, with the formation of a Risk Management Committee responsible for developing policies, setting up systems, and assessing various risks arising from both external factors and internal management and operational activities. This also includes defining approaches for managing and controlling risks to an acceptable level, communicating, and organizing workshops for employees to raise awareness of the importance of risk management and the company's risk management process.

Identifying and managing risks will lead to better decision-making and mitigate the impact of significant potential events. Additionally, the company encourages partners and stakeholders to be aware of the policy to ensure consistent practices.

1. **Establishing Risk Management Policies and Criteria**

This involves setting policies, objectives, scope, responsibilities, criteria, and risk management guidelines in line with strategies, goals, plans, and business directions. The company will review these annually and prepare them concurrently with business plans to ensure consistency

2. **Risk Identification**

Identifying risks that may impact the achievement of objectives and goals, considering risks arising from internal and external factors such as environment, laws, finance, information systems, data systems for decision-making, investor satisfaction, investment management, human resources, reputation and image, security systems, etc. The company will manage risks by prioritizing them before

considering control systems. If risks are classified as high or very high, the company will analyze them for immediate management, using the COSO-ERM enterprise risk management framework.

3. Risk Analysis

Analysis to assess the remaining risk level after evaluating existing control systems and prioritizing risks. If the remaining risk is still high or very high, risk management measures must be implemented immediately by the responsible senior management. If the remaining risk is medium or low, management measures should be defined at the departmental level or corrected within operational processes.

4. **Risk Management**

Defining methods for preparing plans to manage significant risks as prioritized in the risk analysis phase. Risk management covers processes, guidelines, controls, risk transfer, risk avoidance, risk exploitation, or risk acceptance.

5. Monitoring and Review

The process of monitoring risk management outcomes according to the defined plan, as well as evaluating the effectiveness of risk management. The Risk Management Committee will monitor and report to the Executive Committee, Audit Committee, and Board of Directors.

6. Promotion

The company encourages everyone to be aware of risks and understand that risk management is everyone's duty and responsibility, especially for risk owners. Management has driven risk awareness to become an organizational culture, and has regularly organized training on risk management throughout the organization, as well as on relevant laws and regulations.

Additionally, the company recognizes the importance of both direct and indirect impacts of existing or potential risks on business operations. Therefore, it has established guidelines for managing business risks as follows:

1. Risk from Exchange Rate Fluctuations

As the company's primary revenue comes from exports, exchange rate fluctuations inevitably affect the company's performance.

Company's Risk Management

The company closely monitors exchange rate changes and has a clear policy for appropriate risk management and prevention during each period, utilizing management tools in business planning.

Additionally, the company has attempted to diversify sales into more foreign currencies, considering the suitability of each customer group and country. The currency for trade is discussed closely with each customer, and the company has no policy of speculating on exchange rates.

2. Risk in Trade Laws and Regulations

Current international trade barriers include both tariff measures and non-tariff measures, such as sanitary and phytosanitary measures and various quality standard systems. These measures have been increasingly adopted and play a greater role.

Company's Risk Management

The company closely monitors trade regulations and laws of importing countries, tracking, analyzing impacts, and preparing recommendations for readiness. Simultaneously, it maintains communication with relevant government and private agencies, as well as foreign partners, to exchange information and opinions. This helps the company receive timely and comprehensive information, which is then analyzed and used to develop work processes, controls, and prevention measures to align with standards and requirements.

3. Risk from Raw Material Situation Fluctuations

The company's products rely on agricultural raw materials, which fluctuate with climate, environment, and natural disasters, both in Thailand and other raw material-producing countries. This leads to significant fluctuations in both price and quantity of raw materials, thus significantly impacting the company's performance.

Company's Risk Management

The company has developed and enhanced the capabilities of its purchasing and procurement department to source sufficient raw materials from various locations, diversified supply sources, and increased the number of raw material producers. It also closely monitors information from all sides to analyze the raw material situation appropriately and quickly. Furthermore, the company manages raw material stock at appropriate and sufficient levels for production. Additionally, the company collaborates with business partners on forward purchasing and delivery contracts to ensure timely raw material procurement at suitable costs.

4. Risk from Labor Shortages and Labor Costs

The situation of labor shortages, coupled with the burden of labor costs from minimum wage policies, as well as other welfare burdens, has led to an unavoidable increase in overall labor costs, thus impacting production costs.

Company's Risk Management

The company has developed and increased labor efficiency, reduced production losses, and improved production processes by investing more in machinery and technology. The company has also increased employee relations activities to maintain good relationships with employees, enhance their quality of life, and improve working conditions.

5. **Risk from Natural Disasters**

Currently, global environmental and climatic conditions have changed significantly, increasing the likelihood of natural disasters in all regions worldwide. Such events impact the company's operations, making this a risk that requires careful attention.

Company's Risk Management

The company has implemented prevention and contingency measures in case of natural disasters to help reduce the severity of impacts. It has defined plans for data monitoring, situational analysis during each period, planning for rectification, prevention, and recovery, as well as developing team skills to manage work efficiently and promptly under crisis conditions.

Policy Review and Improvement

The company's risk management policy must be reviewed and updated regularly, at least once a year, to align with the changing organizational environment. Any changes to the risk management policy must be approved by the Board of Directors, and its suitability and effectiveness must be reported.

Sources of Risk

Risks arise from two factors: internal factors and external factors.

1) Internal Factors organizational Objectives, policies and strategies, operations, work processes, organizational structure and management systems, financials, organizational culture, and information technology.
2) External Factors government policies, economic/socio-political conditions, the actions of relevant external agencies, competition (business rivals), suppliers/service providers, and various natural disasters.

Risk Assessment is the process of identifying the severity and prioritizing risk factors by evaluating their

- **Likelihood** refers to the frequency or probability of a risk event occurring.

- **Impact** refers to the severity of damage or the consequences resulting from a risk event.

Degree of Risk refers to the status of a risk, determined by evaluating the likelihood and impact of each individual risk factor. It is categorized into five levels: Very High, High, Moderate, Low, Very Low

Table 1: Criteria for Risk Prioritization

Green Zone (Very Low)			Green Zone (Low)			Yellow Zone (Moderate)			Orange Zone (High)			Red Zone (Very High)		
Ranking	Likelihood	Impact	Ranking	Likelihood	Impact	Ranking	Likelihood	Impact	Ranking	Likelihood	Impact	Ranking	Likelihood	Impact
1	1	1	4	1	3	9	1	5	13	2	4	20	3	5
2	2	1	5	1	4	10	2	3	14	2	5	21	4	4
3	1	2	6	2	2	11	3	2	15	3	3	22	4	5
			7	3	1	12	5	1	16	3	4	23	5	3
			8	4	1				17	4	2	24	5	4
									18	4	3	25	5	5
									19	5	2			

Risk Prioritization (Levels 1 to 25) This prioritization system, ranging from Level 1 to Level 25, is used to assess the likelihood and impact of risks. It serves as a fundamental criterion for risk assessment.

Very High
High
Moderate
Low

Table 2 : Organizational Risk Assessment Matrix

Very Low

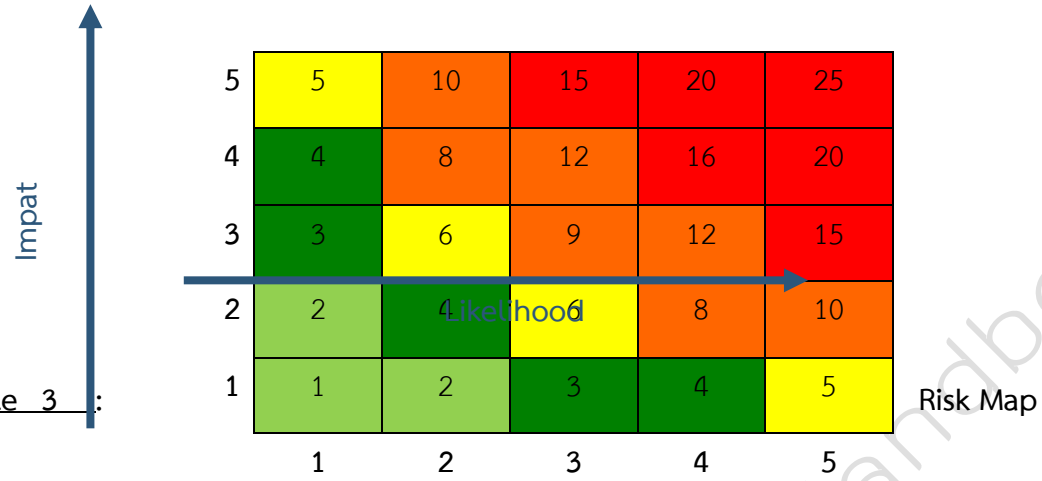


Table 3 : Risk Map

Overall Risk Level	Score Level	Description
Very Low	1-2	**Acceptable Risk Level** no specific action plan is required, but continuous effort must be made to maintain the risk within this category, even if future environmental conditions change.
Low	3-4	**Tolerable Risk r**elevant personnel and stakeholders must be informed to ensure awareness of these risks.
Moderate	5-7	**Manageable Risk** level Continuous control and monitoring of these risks are required.
High	8-14	**Unacceptable Risk Level** risk management actions are necessary to bring these risks down to an acceptable level.
Very High	15-25	**Immediately Unacceptable Risk Level** urgent risk management is required to bring these risks to an acceptable level without delay.

Risk Likelihood	Level Definitions

1 (Very Low)	This event is expected to occur only under abnormal conditions, with a less than or equal to 5% chance of occurring within the next 12 months.
2 (Low)	This event is expected to occur only at certain times, with a greater than 5% but not exceeding 25% chance of occurring within the next 12 months.
3 (Moderate)	This event is expected to occur only at certain times, with a greater than 25% but not exceeding 50% chance of occurring within the next 12 months.
4 (High)	This event is expected to occur under most conditions, with a greater than 50% but not exceeding 90% chance of occurring within the next 12 months.
5 (Very High)	This event has a very high likelihood of occurring under all conditions, with a greater than 90% chance of occurring within the next 12 months.

Risk Likelihood and Impact Assessment assessing the likelihood and impact of risks involves evaluating each identified risk and risk factor to determine the probability of various risk events occurring. This also includes assessing the severity or monetary value of potential damages. This process helps to identify different levels of risk, enabling the establishment of appropriate risk controls. Consequently, the organization can plan and allocate resources effectively within limited budgets, personnel, or timeframes, using the predefined standard criteria. The operational steps are as follows:

1) **Consider the Likelihood and Frequency of Events:** Evaluate the probability and frequency of various events based on the established standard criteria.

2) **Consider the Severity of Risk Impact:** Assess the severity or extent of damage from the risk's impact on the organization or department, according to the defined standard criteria.

Risk Level Analysis after evaluating the likelihood and frequency of events and the severity of each risk factor's impact, the results are used to analyze the relationship between the likelihood of the risk occurring and its impact on the organization or department, determining the resulting risk level.

Risk Prioritization once the risk levels are determined, they are prioritized based on their severity to Northeast Rubber Public Company Limited. This prioritization guides the selection of appropriate control activities for each significant cause of risk. This is done by considering the risk level

derived from the relationship between the likelihood of the risk occurring and its assessed impact, as per the risk assessment matrix. Risks are arranged in descending order: Very High, High, Moderate, Low, and Very Low. Risks identified as "Very High" and "High" will proceed to the next stage for risk management planning.

In risk assessment, a Risk Profile must be established. This profile is derived from considering the prioritization of risks based on their Likelihood and Impact, and by defining the Risk Appetite Boundary.

Risk Level (R) = Likelihood (L) x Impact (I)

The calculated risk level from the formula above, if very low, means the risk is in the Very Low category. As the value increases, the risk level also increases, using the following criteria for categorization:

1. Very Low Risk: A risk score of 1 – 2. This risk is acceptable and designated as light green (). No additional management measures are required for these risks.

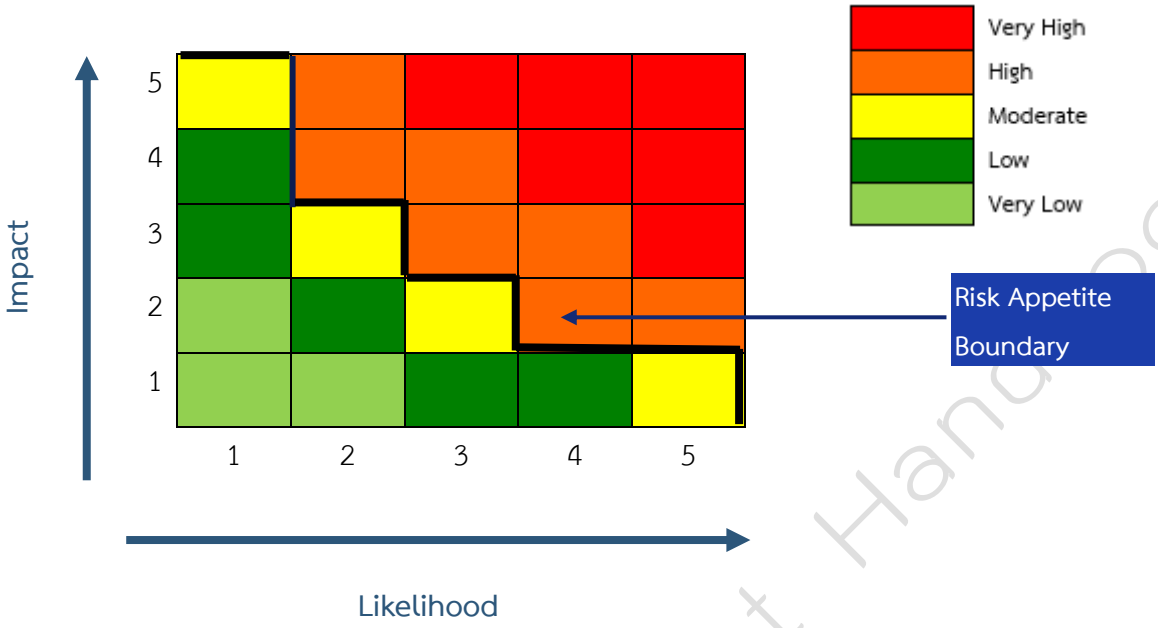
2. Low Risk: A risk score of 3 – 4. This risk is acceptable and designated as green (). No additional management measures are required for these risks. Conversely, the internal control system may be reviewed to allow for a certain degree of control relaxation.

3. Medium Risk: A risk score of 5 – 7. This risk is acceptable, but a risk control plan is required and designated as yellow (). This includes assigning clear responsibilities and timelines. Additionally, strict adherence to current internal control systems (current risk management practices) is necessary to prevent the risk from escalating to an unacceptable level.

4. High Risk: A risk score of 8 – 14. A risk reduction plan is required and designated as orange (). This represents an unacceptable risk level that must be managed to become acceptable. This involves using strategies such as Treat (reducing/controlling the risk), Terminate (canceling/avoiding the risk), or Transfer (distributing/transferring the risk), along with clearly defined responsibilities and timelines. The operational importance or budget allocation for these risks will be less than that for the red zone.

5. Extreme Risk: A risk score of 15 – 25. A plan to reduce and re-evaluate or transfer the risk is required and designated as red (). Immediate additional risk management measures must be implemented. This involves using strategies such as Treat (reducing/controlling the risk), Terminate

(canceling/avoiding the risk), or Transfer (distributing/transferring the risk), along with clearly defined responsibilities and timelines.



Risk Map

Operating Procedures

1. The Risk Management Working Group, comprising representatives from each department, shall assess risks for each risk factor using the company's designated risk management form.

2. **Evaluate the likelihood** of various risk events and **assess the impact level** from the analyzed risk factors. Record these evaluations comprehensively on the form for all risk factors, based on the established standard assessment criteria.

Risk Response Guidelines Defining risk response guidelines aims to enable the organization to manage risks to an acceptable level. Risk response approaches can be implemented in various ways and adjusted to suit the situation, depending on the discretion of the responsible party. However, risk management approaches must be cost-effective in reducing the impact level of the risk.

There are four primary options or strategies for risk management:

1. **Acceptance (Risk Acceptance):** This involves accepting a risk because the cost of managing it or implementing control systems might outweigh the benefits. However, monitoring and oversight

measures should still be in place, such as defining acceptable impact levels or preparing contingency/response plans.

2. **Treatment (Risk Reduction/Control):** This involves designing control systems, modifying, or improving operations to prevent or limit the impact and likelihood of damage. Examples include installing safety equipment, providing training to develop skills, and implementing proactive measures.
3. **Termination (Risk Avoidance):** This involves stopping or changing activities that pose a risk. Examples include eliminating unnecessary steps that introduce risk, modifying work processes, or reducing the scope of operations.
4. **Transfer (Risk Sharing/Spreading):** This involves distributing assets or processes to reduce the risk of loss. Examples include insuring assets to transfer risk to an insurance company, outsourcing certain tasks to external companies, or making multiple copies of documents.

Operating Procedures

The Risk Management Working Group shall define risk response guidelines in the **Risk Register** form, considering each case individually as follows:

1. External Factors: High and Extreme Risk Levels (without existing mitigation measures)

For these risk factors, the Risk Management Working Group shall determine risk response guidelines, considering the following:

1.1 If the risk factor aligns with the department's mission, falls within the department's management scope, and is cost-effective to address, adopt the **Risk Reduction** approach. Define measures/activities to reduce the risk.

1.2 If the risk factor aligns with the missions of multiple departments within the organization, falls within the scope where relevant departments can collaborate, and is cost-effective to address, adopt the **Risk Reduction** approach. The departmental Risk Management Working Group shall prepare a proposal for risk response guidelines, including measures/activities to mitigate the risk, and submit it to the Risk Management Committee for consideration.

1.3 If the risk factor is outside the mission of all departments but aligns with the mission of another department within the organization, the departmental Risk Management Working Group shall prepare a proposal for risk response by **transferring the risk** to the directly responsible department. This proposal, including measures/activities to mitigate the risk, shall be submitted

to the Risk Management Committee for consideration and assignment to the relevant department to further reduce that risk.

1.4 If the risk factor is outside the mission of all departments within the organization, the departmental Risk Management Working Group shall assess whether cost-effective mitigating measures/activities can be defined. If so, new measures/activities to mitigate the risk shall be established and submitted to the Risk Management Committee for consideration.

2. External Factors: Medium, Low, and Very Low Risk Levels

For these risk factors, the Risk Management Working Group shall consider each case individually as follows:

2.1. If the risk factor is acceptable, and normal operational activities/procedures can control the risk to an acceptable level, but there's a perceived possibility of the risk still occurring and potentially impacting the department's objectives/goals, choose the **Risk Control** approach (manage according to the organization's internal control guidelines).

2.2. If the risk factor is acceptable but no normal operational activities/procedures can control it, and there's a perceived possibility of the risk impacting the department's objectives/goals, the departmental Risk Management Working Group shall consider choosing the **Risk Control** approach (manage according to the organization's internal control guidelines) and define new risk control measures and activities.

2.3. If the risk factor is acceptable under existing controls, and the departmental Risk Management Working Group determines that no further action is necessary (e.g., in cases where the risk is minor and not cost-effective to address), choose the **Risk Acceptance** approach.

3. Internal Factors: High and Extreme Risk Levels for these risk factors, the Risk Management Working Group shall consider each case individually as follows:

3.1. If the risk factor may arise directly from the department's operations, falls within the department's management scope, but lacks existing control measures or activities, and is deemed cost-effective to address, adopt the **Risk Reduction** approach and define new measures/activities to reduce the risk.

3.2. If the risk factor may arise from the operations of multiple departments within the organization, falls within the scope where relevant departments can collaborate, and is cost-effective

to address, adopt the **Risk Reduction** approach. The departmental Risk Management Working Group shall prepare a proposal for risk response guidelines, including measures/activities to reduce the risk, and submit it to the Risk Management Committee for consideration.

3.3. If the risk factor is outside the department's mission but aligns with the mission of another department within the organization, the departmental Risk Management Working Group shall prepare a proposal for risk response by **transferring the risk** to the directly responsible department. This proposal, including measures/activities to mitigate the risk, shall be submitted to the Risk Management Committee for consideration and assignment to the relevant department to further reduce that risk.

3.4. If the risk factor is outside the mission of all departments within the organization, the departmental Risk Management Working Group shall assess whether cost-effective mitigating measures/activities can be defined. If so, adopt the **Risk Reduction** approach and define new measures/activities to reduce the risk, then submit them to the Risk Management Committee for consideration.

4. Internal Factors: Medium, Low, and Very Low Risk Levels for these risk factors, the Risk Management Working Group shall consider each case individually as follows:

4.1. If the risk factor is acceptable and normal operational activities/procedures can control the risk to an acceptable level, but there's a perceived possibility of the risk still occurring and potentially impacting the department's objectives/goals, choose the **Risk Control** approach (manage according to the department's internal control guidelines).

4.2. If the risk factor is acceptable but no normal operational activities/procedures can control it, and there's a perceived possibility of the risk impacting the department's objectives/goals, the departmental Risk Management Working Group shall consider choosing the **Risk Control** approach (manage according to the organization's internal control guidelines) and define additional risk control measures and activities.

4.3. If the risk factor is acceptable under existing controls, and the departmental Risk Management Working Group determines that no further action is necessary (e.g., in cases where the risk is minor and not cost-effective to address), choose the **Risk Acceptance** approach.

5. Defining Control Activities

After the Risk Management Working Group has identified the risk response approach for each risk factor, the working group shall define control activities to reduce **High** and **Extreme** level risks to an acceptable and practicable level. This also requires considering the cost-effectiveness of expenses and investment costs for implementing such measures or action plans, compared to the expected benefits.

Operating Procedures

1. Determining Activities for Risk Mitigation: The identification of activities to address various risks can be conducted concurrently with defining risk response approaches. After a risk response approach has been determined, specific risk control measures/activities should be defined and recorded in the company's designated form. The guidelines for recording these measures/activities are considered on a case-by-case basis as follows:

1.1. **For Risk Acceptance:** Identify current risk control measures/activities and evaluate their effectiveness in controlling the risk.

1.2. **For Risk Control:** If current risk control measures/activities exist, evaluate their effectiveness to determine if additional measures/activities are necessary. If no current risk control measures/activities exist, proceed to define additional measures/activities.

1.3. **For Risk Reduction:** If current risk control measures/activities exist, evaluate their effectiveness to understand why they are insufficient in controlling the risk. Then, define additional measures/activities to reduce the risk to an acceptable level, prioritizing feasibility and cost-effectiveness. If no current risk control measures/activities exist, define additional measures/activities, also prioritizing feasibility and cost-effectiveness.

1.4. **For Risk Termination or Avoidance:** As this represents an unacceptable risk, it must be managed to be outside operational conditions. Methods for managing risks in this category include halting operations or activities that generate the risk, changing operational objectives, or reducing the scope of tasks or activities.

1.5. **For Risk Transfer:** This approach is chosen when a risk is outside operational conditions, and transferring it to another party is more cost-effective for risk mitigation. Examples include purchasing insurance for property/assets from an insurance company, or outsourcing certain tasks,

such as security services, to external individuals or companies. Appropriate measures/activities must be defined, and the responsible party for such measures identified, then presented to the Risk Management Committee for consideration.

2. **Evaluating the Cost-Effectiveness of Risk Mitigation Measures/Activities:** The departmental Risk Management Working Group must assess the cost-effectiveness of chosen measures/activities. Specifically, after identifying risk mitigation measures/activities, estimate the cost of each activity and compare it to the estimated value of potential damage caused by that risk. The cost of implementing the measures/activities must be lower than the value of the damage caused by the risk. If the value of potential damage cannot be estimated, consider whether the expenditure will not impact the department's budget and if the defined measures/activities will enhance operational efficiency. If the activity is deemed necessary but the department's budget is insufficient, requiring additional funding, the proposal should be submitted to the Risk Management Committee for further consideration.

Developing the Risk Management Action Plan

The departmental Risk Management Working Group shall prepare the department's Risk Management Action Plan using the company's designated form. This plan must thoroughly detail the risk factors, defined control activities, specific measures/activities, timelines, budget, outputs/outcomes/key performance indicators (KPIs), and responsible parties. The department's risk analysis results, using the company-specified form, must be submitted to the Secretary of the Risk Management Working Group within the stipulated timeframe. This enables data processing and the preparation of the overall Risk Management Plan for submission to the Risk Management Committee of Northeast Rubber Public Company Limited for further consideration.

Key Operating Principles

1. **Maintain Balance between Risk and Return:** Ensure the achievement of operational objectives, stakeholder expectations, and the maximum benefit for Northeast Rubber Public Company Limited, all within an acceptable risk appetite.
2. **Alignment with Acceptable Risk Levels:** Risk management plans must align with the risk levels deemed acceptable by the Committee.
3. **Integral Organizational Culture:** Risk management is a vital part of the organizational culture and must be carried out effectively and efficiently by all executives and employees.

4. **Timely and Continuous Management of Impactful Risks:** Risks that may affect the achievement of organizational objectives and missions must be managed promptly and continuously as follows:

4.1 Risks must be identified comprehensively and in a timely manner.

4.2 Risks must be assessed in terms of their **Likelihood** of occurrence and their **Impact** if they materialize.

4.3 Risks must be managed to a level acceptable to the Committee and management, while also considering the appropriateness of costs versus expected benefits.

4.4 Risks must be regularly monitored and reported to ensure that Northeast Rubber Public Company Limited's risk management is appropriate and timely.

Relationship between Good Corporate Governance, Risk Management, Management Control, and Internal Audit

Risk management adheres to the principles of **Good Corporate Governance**, with **Internal Control** and **Internal Audit** forming integral parts of the risk management process. This relationship is illustrated in the following diagram.

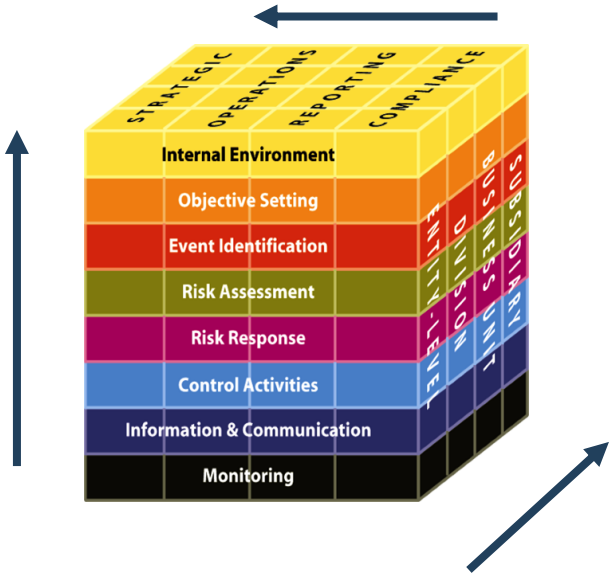
The primary objective of Good Corporate Governance is to monitor, supervise, control, and ensure that processes are established to utilize resources efficiently, align with objectives, be cost-effective, and economical. This aims to maximize benefits for all stakeholders. Therefore, the foundational elements that support good corporate governance include:

1) Risk Management: This is a process designed to identify potential events that could impact the organization. Risk management is applied from the objective-setting stage through every step of operations.

2) Management: This involves enabling the organization to work collaboratively towards achieving shared organizational objectives. Management encompasses planning, organizing, staffing, leading or directing, and controlling the organization, or efforts to achieve common goals. Resource management includes the utilization and deployment of human, financial, technological, and natural resources to ensure the organization's prosperity.
3) Internal Control: This refers to the various operational processes established by the organization to ensure that, when these processes are followed, the organization can smoothly achieve its objectives.
4) Internal Audit: This is a function established to assess the efficiency and effectiveness of various good governance processes. It serves as a mechanism to drive improvements in internal control and appropriate risk management, thereby contributing to the achievement of the organization's objectives and goals.

Key Principles of Risk Management

Effective risk management, following the **COSO ERM (The Committee of Sponsoring Organizations of the Treadway Commission)** framework, refers to a process where personnel throughout the entire organization participate in thinking, analyzing, and anticipating potential events or risks. This also includes identifying approaches to manage such risks to an acceptable level, enabling the organization to achieve its goals in line with its objectives, vision, and mission. This framework comprises eight components, covering guidelines for policy setting, administration, operations, and risk management, as follows:



1. **Internal Environment**

The organization's environment is a crucial component in defining the risk management framework and forms the fundamental basis for setting its direction. It comprises several factors, such as organizational culture, management policies, personnel operating guidelines, work processes, and information systems.

2. **Objective Setting**

Organizations must define risk management objectives that align with strategic goals and the organization's risk appetite. This ensures clear and appropriate targets for organizational risk management.

3. **Risk Identification**

This involves gathering potential events that could impact the department, including risk factors originating from both internal and external sources. These events, if they occur, would prevent the organization from achieving its objectives or goals. Examples include management policies, personnel, operations, finance, information systems, and regulations. This step aims to foster an understanding of these events and situations, enabling management to effectively determine approaches and policies for addressing potential risks.

4. **Risk Assessment**

Risk assessment involves measuring the severity of risks to prioritize existing risks by evaluating their Likelihood and Impact.

5. **Risk Response**

This is the action taken after the organization has identified and assessed its risks. Risks must be addressed to reduce the likelihood of occurrence and mitigate the severity of impact to an acceptable level, utilizing the most appropriate and cost-effective risk management methods.

6. Control Activities

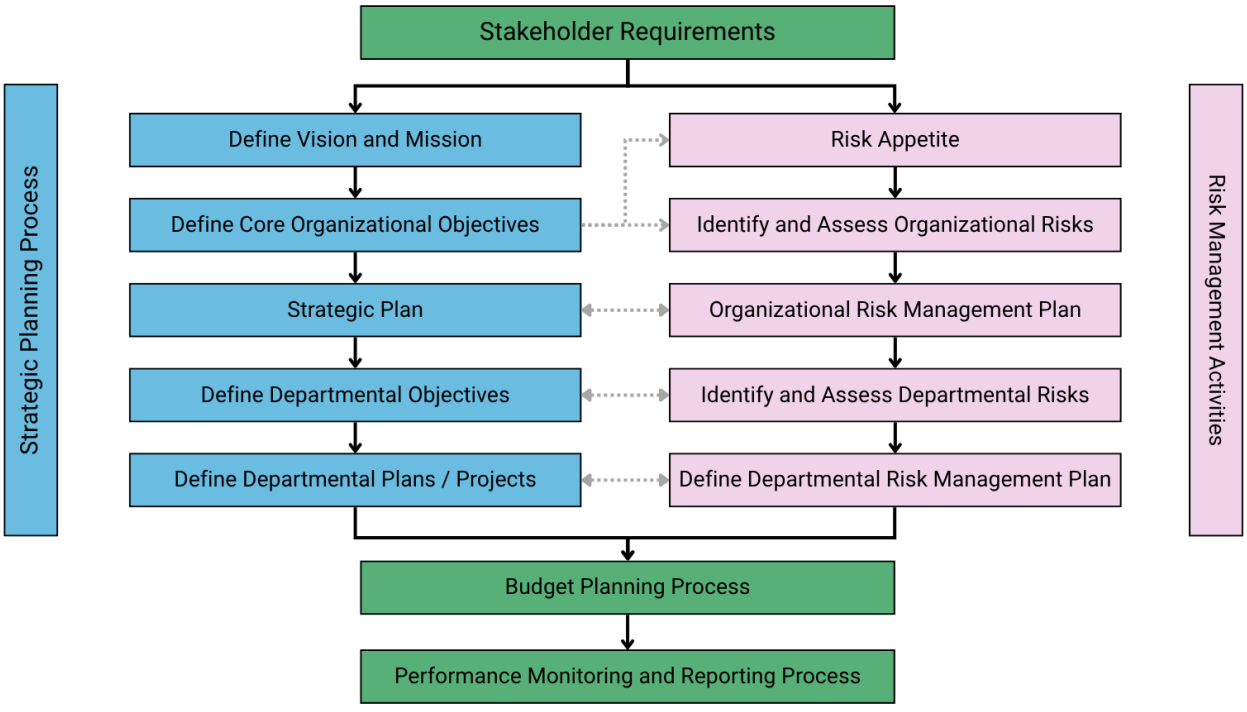
This involves defining and implementing various activities to help reduce or control risks. These activities ensure that risks can be managed correctly and that operations achieve organizational objectives and goals, preventing and reducing risks to an acceptable level.

7. Information and Communication

Organizations must maintain an efficient information and communication system. This serves as an essential foundation for proceeding with risk management in accordance with the organization's defined framework and operational procedures.

8. Monitoring

Organizations must monitor results to ascertain if operations are appropriate and whether risks are being managed effectively.



Key Success Factors for Risk Management

To ensure that the organization benefits from risk management, management must establish processes to support the continuous identification, assessment, management, and reporting of risks. This must be integrated into normal operations. The following eight critical factors will contribute to the successful implementation of the organization's risk management framework:

1. Top Management Support

The success of Enterprise Risk Management (ERM) is highly dependent on the commitment, support, and active involvement of the Board of Directors and top management. They must prioritize and ensure that everyone within the organization understands the importance and value of risk management; otherwise, ERM cannot be effectively implemented.

2. Standardized Terminology

The consistent use of common definitions for risk and risk management terms is essential for efficiently setting objectives, policies, and processes. This standardization facilitates effective risk identification, assessment, and the determination of appropriate risk treatment methods. Organizations must establish a clear Enterprise Risk Management Framework and Policy that clearly defines its components, ensuring that all executives and employees use a common risk language and share a unified goal in risk management.

3. Continuous Adherence to the Risk Management Process

Organizations that successfully implement risk management processes are those that can

apply them comprehensively across the entire organization and maintain them consistently and continuously.

4. Change Management Process

When introducing new management processes and systems, organizations must implement change management. The development of risk management is no different; it requires clear communication to all executives and employees regarding the organizational and individual benefits resulting from the changes.

5. Effective Communication

The objective of effective communication is to ensure that:

1. Executives receive accurate and timely risk information.
2. Executives can manage risks according to their priority, responding to changes and new risks effectively.
3. Risk management plans are continuously monitored for improvement in organizational management and to address various risks, thereby maximizing the organization's opportunity to achieve its objectives/goals.

Communication regarding risk management strategies and practices is profoundly important, as it highlights the connection between risk management and organizational strategy. Explaining and ensuring every employee understands their individual responsibilities within the risk management process will foster acceptance of the process and lead to successful risk management development.

6. Risk Management Measurement

Risk management measurement comprises two forms:

1. Measuring risk in terms of potential impact and likelihood. Successful risk management helps ensure that residual risks are maintained at an acceptable level for the organization.
2. Measuring the success of risk management using performance indicators, which may be defined at the organizational, departmental, or individual level. The use of these performance indicators can be integrated with human resource processes.

7. Training and Human Resources Mechanisms

All directors, executives, and employees within the organization must receive training to understand the Enterprise Risk Management Framework and their individual responsibilities in

managing risks and communicating risk information. Organizational training should consider the following points:

1) Differences in levels of responsibility for risk management.
2) Existing knowledge within the organization regarding risk and risk management. All new employees should also receive training to understand their responsibilities regarding risk and the risk management process.

The performance appraisal system is a crucial tool for promoting individual accountability. Responsibilities related to risk management should be integrated into each individual's job responsibilities and job descriptions. Performance appraisals concerning risk management should assess the following:

1) The individual's responsibility for and support of the risk management process and framework within the organization.
2) The effectiveness of risk management for the risks under that individual's responsibility.

8. Monitoring the Risk Management Process

The final step among the success factors for risk management is to define appropriate methods for monitoring risk management. Monitoring the risk management process should consider the following aspects:

1) Reporting and reviewing steps within the risk management process.
2) Clarity and consistency of top management's involvement and commitment.
3) The role of leadership in supporting and monitoring risk management.
4) The application of performance evaluation criteria related to risk management

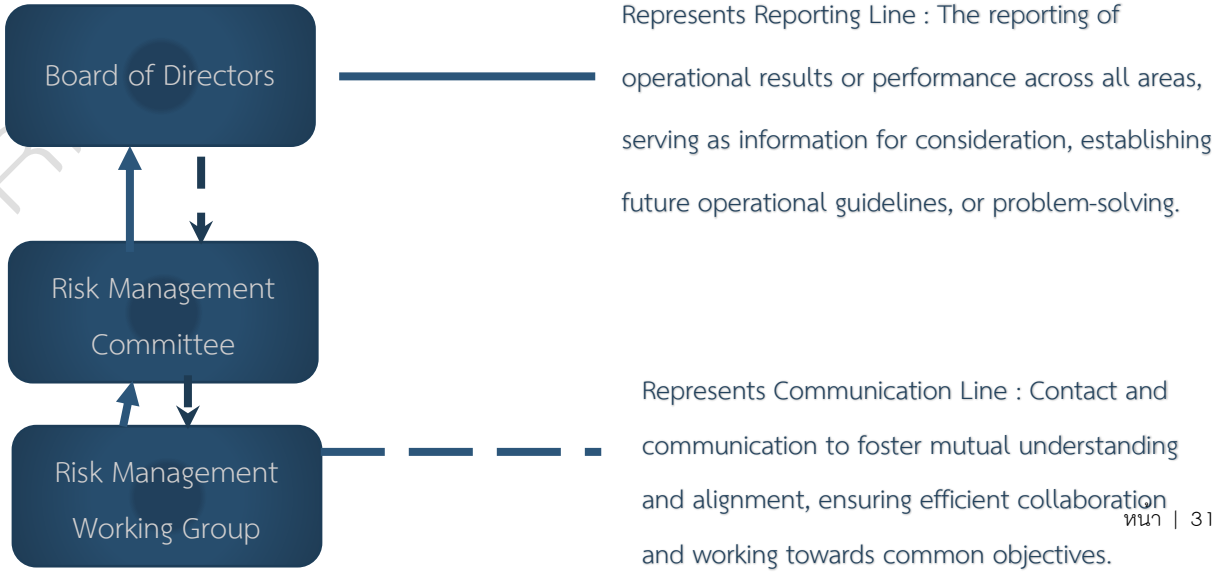


Table : Roles and Responsibilities of the Risk Management Structure of North East Rubber Public Company Limited

Involved Party	Roles and Responsibilities
Risk Management Committee	1) Review and propose risk management policies and frameworks to the Board of Directors for approval. 2) Review and approve the acceptable risk level (Risk Appetite), report to the Audit Committee, and present to the Board of Directors for acknowledgement. 3) Oversee the continuous development and implementation of risk management policies and frameworks to ensure the company has an effective, organization-wide risk management system that is consistently adhered to. 4) Review risk management reports to monitor material risks and take action to ensure that the organization has adequate and appropriate risk management in place. 5) Coordinate with the Audit Committee regarding significant risks, and have the internal audit function review to ensure the company has appropriate internal control systems for risk management, including the proper adoption and organization-wide implementation of the risk management system. 6) Regularly report to the Audit Committee and present to the Board of Directors on significant risks and risk management. 7) Provide guidance and consultation to the Executive Committee, and/or relevant departments, and/or working groups involved in risk management, including considering appropriate approaches for addressing various information related to the development of the risk management system. 8) Consider appointing additional or replacement personnel to the Risk Management Working Group, and/or relevant departments, and/or working groups involved in risk management as appropriate, and define roles, duties, and responsibilities for the benefit of achieving objectives.

	9) Perform any other risk management-related tasks assigned by the Board of Directors. Furthermore, executives, and/or the Risk Management Working Group, and/or relevant departments, and/or working groups involved in risk management, and/or internal auditors, and/or external auditors, must report or present relevant information and documents to the Risk Management Committee to achieve the assigned objectives and duties.
Involved Party	**Roles and Responsibilities**
Risk Management Working Group	1. Define roles, duties, and participation in setting actionable targets, consistent with and in accordance with risk management principles, policies, and manuals. 2. Ensure the following activities are conducted efficiently and effectively: - Identify additional controls required to manage risks to an acceptable level for the organization. - Assess residual risks after current risk management measures have been implemented. - Establish definitive timelines for each operational step to align with the defined plan. - Ensure appropriate allocation of resources for risk management. 3. Monitor the progress of each department according to the risk management plan and Key Risk Indicators (KRIs) to enable timely prevention and the establishment of additional risk management measures. 4. Define necessary control activities and recommendations for proper implementation, and develop the risk management system to meet international standards. 5. Determine appropriate risk management measures and continuously monitor and evaluate the effectiveness of risk management operations. 6. Ensure organizational risks are communicated to all levels of employees, fostering awareness of risk factors that may impact the

	company's objectives, and promoting the importance of risk management among employees to become an organizational culture. 7. Ensure monthly reporting of risks to the Risk Management Committee.

Chapter 4: Risk Management Process of North East Rubber Public Company Limited

The risk management process, aligned with the COSO: ERM (Enterprise Risk Management) framework, is an integrated, organization-wide risk management process consisting of eight components, presented as follows:

1. Internal Environment

Establishing an internal environment that supports risk management is crucial. The internal environment should be appropriate for the organization's nature, encompassing the definition of the organizational structure, Risk Management Policy, Risk Management Philosophy, Risk Appetite, Risk Tolerance, and the roles and responsibilities of the Board of Directors. It also includes defining reporting lines, delegation of authority, and the assignment of Risk Owners responsible for managing specific risks. Furthermore, it covers setting personnel standards, human resource operational guidelines, operational procedures, information systems, and various regulations. The internal environment serves as the foundation for all other components of risk management.

For North East Rubber Public Company Limited, the internal environment comprises the company's structure and the risk management structure. The Risk Management Committee is

responsible for defining the organizational risk management policy and overseeing risk management efforts to achieve the organization's objectives. Risks arising from the internal environment primarily stem from two main causes: people and systems. Therefore, if management can select capable, honest, and responsible personnel for their respective roles, and implement well-planned and systematic work guidelines, risk management can be conducted effectively.

2. Objective Setting

Defining clear organizational objectives is the initial step in the risk management process. Objectives should be clearly documented, align with strategic goals and the acceptable risk level for the respective units, and be communicated to all departments to ensure a common understanding. The SMART framework can be utilized for objective setting :

- Specific Goals are clearly defined and specific, aligning with the core business model.
- Measurable Quantifiable and qualitative measurements are possible.
- Attainable Objectives can be realistically achieved.
- Relevant Objectives are consistent with the organization's overall goals and mission.
- Timely Objectives have clear and appropriate timelines.

3. Event Identification

Event identification involves identifying potential events that could affect the organization, encompassing both opportunities and risks. This requires a thorough understanding of both internal and external factors, including past occurrences and future predictions. Adequate and accurate relevant information is essential for identifying risk events, and experts with relevant knowledge should be involved in this process. If risk identification is not meticulously conducted, overlooked risks may become residual risks for the organization, remaining unanalyzed and unmanaged, potentially leading to severe losses for the organization.

Risk identification should consider the sources of risk that may significantly impact the objectives/goals of activities or cause direct and indirect damage. Risk analysis should focus on identifying risk factors or damaging events related to key activities, covering both inherent risk and residual risk.

- **Inherent Risk :** Refers to the risk inherent in the nature of the business; whenever any business or task is undertaken, risks will always arise.

- **Residual Risk** : Refers to the risk remaining after controls have been implemented to manage a particular risk.

Approaches to Risk Identification

In this step of risk identification, the risk management team should prioritize identifying as many risks faced by the organization as possible. Common methods for risk identification include:

1. **Experience:** Utilizing the assessor's experience to identify past events. This involves analyzing the likelihood of risk by collecting data on past problems/errors in work processes that have been recorded, which can serve as a guideline and preliminary information.
2. **Procedure:** Using procedures to sequence work processes and consider whether various events might occur at each step, potentially disrupting the activity or leading to errors that cause damage.
3. **Brainstorming Group:** Engaging employees or departments involved in the activity, both internal and external to the organization, to collaboratively identify events that have caused damage to their areas of responsibility.
4. **Checklist:** Enabling management and departmental employees to self-check work processes and operational standards using a prepared checklist. A clear timeframe for internal departmental assessment using the checklist should also be defined, e.g., every 3, 6, or 12 months.

Risk identification and the causes of risk should cover the following:

1. Damage or events that may negatively impact the organization.
2. Uncertainties that may affect the achievement of organizational objectives and strategies.
3. Events that may cause the organization to lose opportunities for revenue generation, business opportunities, or external recognition.
4. Risks that may arise across all dimensions, such as strategic, financial, human resources, operational, reputational, legal, tax, system, and environmental risks, etc.
5. Risks that may arise from both internal and external factors.

4. Risk Assessment

Risk assessment is the process that follows risk identification. Risk assessment involves two

dimensions: Likelihood and Impact. Risk assessment should cover the five fundamental risk areas (S-O-F-C-F): 1. Strategic Risk, 2. Operational Risk, 3. Financial Risk, 4. Compliance Risk, and 5. Fraud Risk. Therefore, in risk assessment, assessors should identify the characteristics of risks based on potential damages that may affect the achievement of organizational objectives, in order to determine appropriate risk control measures.

Likelihood refers to the frequency of events causing loss. This can be categorized as low, medium, high, very high, or as a percentage of occurrence. However, assessing losses that have not occurred frequently in the past can be challenging; therefore, historical data should not be the sole reference. Instead, organizational risk factors should be analyzed using scenario analysis under all plausible circumstances.

Impact refers to the severity or magnitude of damage when an event occurs. Assessing the severity of loss involves forecasting the value of the loss if a hazard materializes, based on several factors, such as historical loss values and the maximum loss the organization can absorb without disruption.

Degree of Risk refers to the status of risk derived from assessing the likelihood and impact of each risk factor.

Risk assessment can be performed both qualitatively and quantitatively, and can be conducted from the organizational level down to the departmental level. Both Inherent Risk and Residual Risk (after risk response) should be assessed. A Risk Map should also be developed, emphasizing interrelated risks, as one event may lead to multiple risks.

Risk assessment comprises three steps:

1. Defining risk assessment criteria.
2. Prioritizing risks.
3. Assessing existing risk control measures.

This involves determining the extent to which risks impact the company, considering the likelihood of risk factors occurring and the severity of their impact, and then assessing the risk level by processing the values of likelihood and impact according to predefined scoring criteria.

5. Risk Treatment or Risk Response

Risk treatment is the process of identifying options for managing risks once they have been identified and assessed. Management must evaluate feasible risk management approaches,

considering the acceptable risk level and comparing the associated costs with the anticipated benefits to ensure effective risk management. Management may choose one or a combination of methods to reduce the likelihood and impact of events. There are generally four main principles of risk response :

Various approaches to risk treatment may be employed. For example:

- For risks with a high potential for damage due to a lack of operational oversight or unqualified staff, the unit may choose to manage the risk by implementing control measures or increasing the budget for employee training to reduce the likelihood of damage.
- In some cases where control measures are already in place but damage still occurs, it may be necessary to review the suitability of these controls and improve their effectiveness.
- For events that cause severe damage to the financial standing and operating results, which may arise from uncontrollable factors such as fire or natural disasters, methods like insurance or developing a contingency plan might be used to mitigate the damage to an acceptable level.
- For risks with a low and acceptable risk level, regular monitoring and review should be conducted to ensure they remain within acceptable limits.

6. Control Activities

Control activities are the policies and operational procedures that assure management that the unit's operations and activities align with the organization's strategic goals. These activities serve to prevent and identify risks that could impact the organization's objectives.

While control activities may vary among organizations depending on their management and operational policies, business type, internal environment, and organizational culture, control activities generally fall into four types:

1. **Preventive Control:** Controls designed to prevent or reduce risks arising from errors and damages, such as approvals, organizational structuring, and segregation of duties.
2. **Detective Control:** Control methods established to discover errors that have already occurred, such as inquiries, analyses, reconciliations, and defect reporting.
3. **Corrective Control:** Control methods established to correct errors that have occurred and to find ways to prevent their recurrence in the future, such such as providing fire extinguishing equipment to reduce severity in case of fire.

4. **Directive Control:** Control methods that encourage or stimulate the achievement of desired objectives, such as rewarding high-performing individuals.

When considering the objectives of control activities based on COSO standards and concepts, three main objectives are observed:

1. **Efficiency and Effectiveness of Operations:** Ensuring operations align with the organization's goals and vision.
2. **Reliability of Financial Reporting:** Financial reports are crucial tools for regulatory compliance to promote good corporate governance, and internal controls play a vital role in ensuring operations adhere to established regulations.
3. **Compliance with Laws and Regulations:** Currently, the government emphasizes compliance with regulations to promote good corporate governance, and internal controls play a significant role in ensuring operations adhere to established regulations.

However, control activities are merely tools that help ensure adherence to established guidelines. If employees within the organization do not cooperate, the organization's risk management efforts will not achieve their objectives. Therefore, the success of the control activity system relies on responsible employees fulfilling these duties.

7. Information & Communication

An effective information and communication system is crucial for the successful implementation of risk management within the organization. Information and communication serve as tools that management can use to convey policies, oversee, and monitor operational performance. A robust information system should ideally include:

1. **User Access Control:** Implementing access controls based on levels of responsibility and job types.
2. **Data Backup System:** A system for data backup to prevent system failures or unforeseen incidents that could impact critical organizational data.
3. **Inter-departmental Connectivity:** A system that allows seamless connection between different departments, enabling efficient shared data management.
4. **Redundant Facilities:** Backup facilities equipped with necessary devices and systems, allowing critical units to resume operations immediately in case of emergencies, such as fire or building collapse.

5. **User-Friendly Asset Management:** An asset management system that meets user needs and is easy to use, facilitating operational convenience.

8. Monitoring

To ensure a complete, efficient, and effective risk management mechanism, a system for continuous and regular monitoring should be in place. This involves an evaluation cycle that is known to all departments, enabling them to conduct assessments at defined intervals, such as monthly, quarterly, or at the end of each fiscal year. This includes establishing a clear risk status reporting system, specifying the frequency of monitoring and reporting, defining report formats, and determining the method of presenting reports to management. Additionally, there should be:

- **Exception Reporting:** Provisions for reporting special events that occur infrequently but have high and significant impact.

The key objectives of monitoring and evaluation are to:

1. Assess the quality and appropriateness of risk management.
2. Track the progress of risk management efforts that have been implemented or are underway, verifying if they meet the established risk management objectives.
3. Verify the progress of control measures in reducing the likelihood or impact of risk events to an acceptable level.

Risk management reports can formally serve as a tool for monitoring and evaluation. Departments can implement successful risk management plans and consider discontinuing or improving plans that are still deficient. Furthermore, each department may develop specific internal monitoring reports, such as creating checklists for departmental use and defining their own internal monitoring frequency.

Appendix A. Announcements/Orders – Risk Management Committee

Members of the Risk Management Committee:

1.	Mr. Tepakul Poonlarp	Chairman of the Risk Management Committee
2.	Mrs. Chanatip Weerasubpong	Risk Management Committee
3.	Mr. Chuwit Jungtanasomboon	Risk Management Committee
4.	Mr. Sakchai Jongstapongpun	Risk Management Committee

5. Mr. Nattapon Inprakhon Risk Management Committee

Scope of Authority, Duties, and Responsibilities of the Risk Management Committee are as follows:

- Review and propose risk management policies and frameworks to the Board of Directors for approval.
- Review and approve the acceptable risk level (Risk Appetite), report to the Audit Committee, and present to the Board of Directors for acknowledgement.
- Oversee the continuous development and implementation of risk management policies and frameworks to ensure the company has an effective, organization-wide risk management system that is consistently adhered to.
- Review risk management reports to monitor material risks and take action to ensure that the organization has adequate and appropriate risk management in place.
- Coordinate with the Audit Committee regarding significant risks, and have the internal audit function review to ensure the company has appropriate internal control systems for risk management, including the proper adoption and organization-wide implementation of the risk management system.
- Regularly report to the Audit Committee and present to the Board of Directors on significant risks and risk management.
- Provide guidance and consultation to the Executive Committee, and/or relevant departments, and/or working groups involved in risk management, including considering appropriate approaches for addressing various information related to the development of the risk management system.
- Consider appointing additional or replacement personnel to the Risk Management Working Group, and/or relevant departments, and/or working groups involved in risk management as appropriate, and define roles, duties, and responsibilities for the benefit of achieving objectives.
- Perform any other risk management-related tasks assigned by the Board of Directors.

Furthermore, executives, and/or the Risk Management Working Group, and/or relevant departments, and/or working groups involved in risk management, must report or present relevant

information and documents to the Risk Management Committee to achieve the assigned objectives and duties.