STP&I Public Company Limited

Risk Management Policy

Risk Management Policy of STP&I Public Company Limited

1. Principles and Rationale

STP&I Public Company Limited aims to conduct sustainable and continuous business, adding value to all stakeholders, including shareholders, customers, partners, employees, the government, and the general public. Recognizing the significance of risk management, which serves as a critical mechanism for planning and structuring the company, aligning with defined objectives, strategies, and operational effectiveness, the company has established a risk management policy based on the COSO Enterprise & Risk Management – Integrating with Strategy and Performance (2017) framework[1]. This framework facilitates the identification of comprehensive risks and ensures that risk management remains at an acceptable level. It involves active participation from the board of director, management, and all employees, who continually review policies and practices to maintain appropriateness.

2. Objectives

2.1 To incorporate risk management as an integral part of decision-making for defining strategies, plans, and various operations within the company.

2.2 To identify risks and establish risk management approaches that maintain an acceptable level of risk. This involves considering effective measures to reduce the likelihood and/or impact of potential risks, aiming to achieve organizational and business unit goals.

To communicate and foster an organizational culture where Board of Directors and Executives Committee are informed and aware of critical risk information, risk trends, and the overall risk landscape. This facilitates effective decision-making and efficient risk oversight.

[1] COSO Enterprise & Risk Management: The framework for **organizational risk management** emphasizes the connection between risk management and strategic planning to enhance an organization's value.

3. Scope

The risk management policy applies comprehensively to the company and subsidiaries.

4. Definition

Risk means uncertainties or events that are not certain, including factors that prevent current plans or operations from achieving their intended objectives or goals. These risks can have negative financial implications and/or impact the company's reputation and image.

Risk Factor mean the cause or source of risk and events that may prevent the achievement of objectives or goals. In each factor, the true cause of the various risk factors can be explained, leading to specific risks, and measures can be taken to manage and reduce the risk that may occur.

Risk Management mean the process performed by Boad of Director, Executives Committee and all employees to assist in strategy formulation and execution, the risk management process is designed to identify potential events that may impact the company and manage risks within acceptable level.

Risk Appetite mean the level of risk that is assessed risk management and got approval by the company's board of directors as acceptable for the organization. When a risk has been analyzed and evaluated to potentially have an impact beyond the acceptable risk level, the risk owner should develop a Risk Management Plan (Action Plan) and present and get the approval from the relevant committees acoordingly.

The sources of risk from two factors:

1) Internal Factors: These include an organization's objectives, policies, strategies, operational processes, organizational structure, organizational culture, and information technology, etc.
2) External Factors: These encompass state policies, economic/social political conditions, competition, epidemics, and natural disasters, etc.

Risk Assessment is the process of identifying the severity levels and prioritizing risk factors. It involves evaluating the likelihood of occurrence and the impact resulting from those risks.

5. Roles and Responsibilities

5.1 Board of Directors

- Independently oversee risk management and provide recommendations on significant risks.
- Establish risk management policies, consider critical risk factors, and monitor risk management strategies and performance outcomes.

5.2 Audit Committee

- Review and assess the company's risk management policies and compliance with risk management principles for both the company and its subsidiaries.
- Ensure that audits are conducted based on risk considerations (Risk-based Audit) and that the organization appropriately manages risks.

5.3 Executive Committee:

- Define risk management policies and consider critical risk factors that may occur. This includes risk management strategies, reviews, monitoring of performance outcomes and associate risk management with internal audit controls.

6. Types of Risk:

6.1 Strategic Risk: Risk from inappropriate strategic planning or various factors that are **not** aligned with policies, objectives, organizational structure, internal factors, and external environment. It results in the failure to achieve the goals and objectives set by the company. Strategic risks encompass risks from revenue fluctuations, price volatility of raw materials, and insufficient labor quantities. These factors impact the organization's competitive strategy and operational directions.

6.2 Financial Risk: pertains to the risks associated with financial policies and procedures, including management of finances and investments. These risks impact a company's operations and financial statements, encompassing deviations from predefined targets. They include risks related to liquidity, credit, investments, foreign exchange fluctuations, and interest rates. Additionally, contractual non-compliance by counterparties can also result in adverse consequences for the organization.

6.3 Operational Risk: result from operational processes, system functions, or external events that impact efficiency and effectiveness in operations. It encompasses risks stemming from operational process deficiencies, which can render various activities within an organization inefficient. This category also includes risks related to managing information technology and knowledge data to achieve predefined operational objectives.

6.4 Compliance Risk: as defined in the context you provided, refers to the risk arising from non-compliance with laws, regulations, directives, principles, and practices both within the company and from external. This encompasses situations where regulations are ambiguously defined, requiring discretion or interpretation. Such risks can lead to legal actions, complaints, and impact the company's operations. It covers risks related to adhering to regulations, compliance with agency-imposed rules, and legal aspects relevant to the company's operations.

6.5 Cyber Risk: pertains to risks associated with cybersecurity. It arises from changes in information technology, including digital transformation. These risks impact a

company's operations and encompass the technology systems used for critical business activities.

6.6 Organization Risk: refers to risks within an organization such as mergers & acquisitions, joint management of customer marketing, and human resource management, including legal termination of employment.

6.7 External Risk: These are risks originating from external factors that an organization cannot directly control. These factors include changes in the Consequences of war, economic conditions, transportation patterns, political landscape and natural disasters such as floods, fires, and various diseases.

6.8 Corruption risk: refers to the risk arising from any action taken to seek benefits unlawfully. This can include giving or receiving bribes, whether in the form of money, goods, political favors, charitable donations, hospitality expenses, or any other inappropriate consideration. Such actions may involve explicit agreements, promises, demands, or acceptance of money or other benefits that are not suitable for government officials, public agencies, private entities, or individuals acting in an official or unofficial capacity.

Procedure of risk management practice as follows;

1) Identify all risks that related to your business operations, financial, and relevant regulations and laws.
2) Analyze and evaluate the risk considering both opportunities and threats that may occur.
3) Set measures and action plan to manage risks by acceptance of the risks, implementing measures to reduce the likelihood or impact of the risk, avoiding the risk or sharing the risk with other parties.
4) Implement control measures of risks are follow the action plan appropriately at all levels of organization, including company groups, section, departments, and

processes. And it is ensure alignment with legal requirements, environmental, job complexity, Job description, scope, and operational processes.

5) Monitor and Review: continuously track and review the effectiveness of risk controls.