HARN ENGINEERING SOLUTIONS PUBLIC COMPANY LIMITED

RISK MANAGEMENT POLICY

Approved by the resolution of the Board of Directors at Meeting No. 2/2021 held on 25 March 2021.

with effect from 26 April 2021 onwards.

and reviewed by the Board of Directors at Meeting No. 2/2025 held on 24 March 2025.

Risk Management Policy

At present, the Company's business operations are exposed to increasingly complex and severe risks arising from changes in both the internal and external business environments. To achieve sustainable long-term growth, the Company must establish a sound risk management foundation sufficient to prevent and mitigate the impacts of risks arising from various uncertainties, including corruption risks. Accordingly, to ensure that all departments across the Company adopt a consistent approach to risk management, the Risk Management Committee has established the Risk Management Policy of Harn Engineering Solutions Public Company Limited to serve as the risk management framework for operational practices by all employees.

Objectives

To address operational obstacles and to prevent or reduce the likelihood of undesirable events and their potential impacts that may cause the Company's operations to fail to achieve its objectives and goals. This Policy also aims to promote good corporate governance and ensure that business is conducted in a fair, honest, and transparent manner.

Scope

To ensure continuity of operations and the achievement of the Company's objectives, all departments shall implement risk management, with risk management being integrated as a routine process in the daily work of all employees. The objective is to embed risk management as an integral part of the Company's organizational culture.

Definition

Risk means an event (in the future) that may arise under changing circumstances, uncertainty, emergencies, or abnormal situations, which may affect, cause damage or failure, or reduce the likelihood of achieving the Company's goals and objectives at the corporate, functional, departmental, or individual level.

Risk Management

Risk management means the process of managing risks in the Company's operations in alignment with its established objectives, through the establishment of systematic frameworks and procedures for risk-related practices. This is to ensure that risks affecting the Company are managed such that the level and magnitude of impact remain within the Company's acceptable risk appetite, including systematic assessment, control, and monitoring, with primary consideration given to the achievement of the Company's objectives.

Risk Management Policy

1. The Company shall conduct its business within an acceptable level of risk in order to achieve its objectives and meet the expectations of stakeholders. Risk management shall be integrated as part of the annual business planning, management processes, day-to-day decision-making, and project management processes.
2. All executives and employees of the Company are risk owners and are responsible for identifying and assessing risks within their respective areas of responsibility, as well as determining appropriate measures to manage such risks.
3. All risks that may affect the achievement of the Company's objectives shall be managed as follows:
    - Risks shall be identified in a timely manner.
    - The likelihood of occurrence and potential impacts shall be assessed.
    - Risks shall be managed in accordance with the established risk management criteria, taking into account related costs and expected benefits.
    - Monitoring shall be undertaken to ensure that the Company's risks are appropriately managed.
4. All risks that may impact the Company's business plans and strategies and are assessed at high and very high levels shall be reported to the Executive Committee, the Audit Committee, and the Board of Directors.

Benefits of Risk Management

1. The Company's performance can be achieved in accordance with its established goals and objectives, promoting continuous and sustainable business growth to create added value for the Company and its stakeholders, and supporting good corporate governance.
2. To promote employees' knowledge, understanding, and awareness of the importance of risk management, thereby fostering prudence in operations and reducing the likelihood of operational losses.

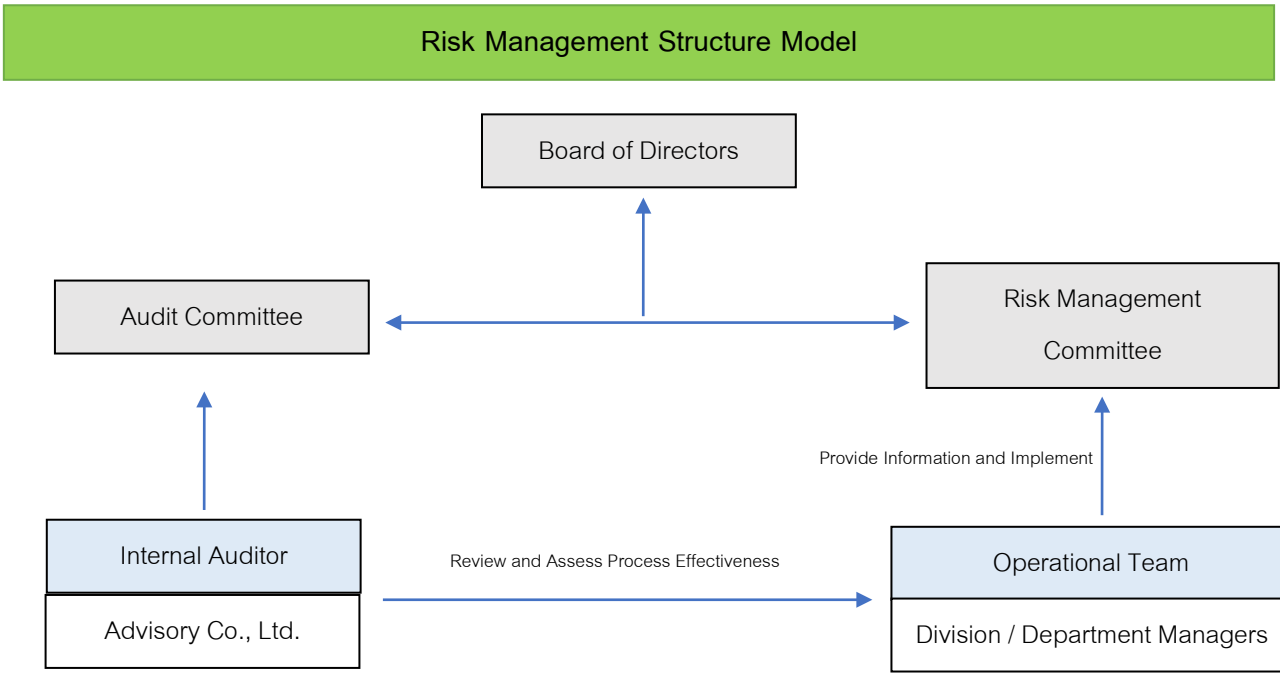
3. In preparing project plans, the Company can utilize risk analysis results as part of the decision-making process on whether to undertake projects that may impact the Company.
4. To enhance the completeness and feasibility of the Company's objectives and strategies and ensure alignment with the acceptable level of risk.
5. To promote preparedness and establish approaches for resolving issues that may arise and affect the Company's performance.
6. To provide management with information to support more accurate and timely decision-making.
7. To enable appropriate allocation of resources, taking into account investment efficiency and value.
8. To encourage employee participation and integration with other organizational systems in driving the Company toward the achievement of its objectives.

Risk Management Structure

The structure is divided into two levels:

1. Corporate Level – The Risk Management Committee, chaired by the Chairman of the Risk Management Committee, with duties and responsibilities in accordance with the Company's established practices.
2. Departmental Level – Division/department managers and all employees perform risk management activities under the supervision of the Risk Management Committee through respective line directors.

Risk Management Structure of Harn Engineering Solutions Public Company Limited



Duties and Responsibilities of the Committees in Risk Management

1. Duties and Responsibilities of the Risk Management Committee

1.1 To establish the Company's overall risk management policy and structure covering key risk categories, such as financial risk, investment risk, and reputational risk, for submission to the Board of Directors for approval, in alignment with the risk management guidelines of the Stock Exchange of Thailand and the Institute of Internal Auditors of Thailand.

1.2 To determine the Company's risk management strategy and guidelines in accordance with the risk management policy, enabling the assessment, monitoring, and control of each type of risk within acceptable levels, with participation from all departments in risk management and control.

1.3 To oversee and monitor compliance with the risk management policy under the framework and policies approved by the Board of Directors.

1.4 To establish risk measurement criteria and the Company's acceptable risk appetite.

1.5 To prescribe appropriate risk management measures in response to prevailing circumstances.

1.6 To assess risks at the corporate level and determine risk management approaches to maintain such risks within acceptable levels, and to supervise the implementation of risk management in accordance with the prescribed approaches.

1.7 To consider and assess transactions with corruption risk exposure and to determine control measures and risk management approaches, including reviewing all information in the self-assessment on anti-corruption measures.

1.8 To review and improve the risk management policy to ensure sufficient effectiveness and efficiency in risk control.

1.9 To have the authority to summon relevant persons for clarification or to appoint and assign roles so that personnel at all levels have appropriate risk management responsibilities, and to require reporting to the Risk Management Committee to ensure the achievement of risk management objectives.

1.10 To regularly report to the Board of Directors on the Company's risk management, operations, and risk status, including changes and required improvements to align with established policies and strategies.

1.11 To prepare the annual Enterprise Risk Management Manual.

1.12 To establish an integrated risk management system linked with information systems.

2. **Duties and Responsibilities of the Operational Team**

The Operational Team refers to division/department managers and all employees within the organization, with the following duties and responsibilities:

2.1 To adopt the risk management guidelines and prepare risk mitigation plans for activities within their respective areas, including corruption risks arising from their operational processes.

2.2 To implement and report the results of actions in accordance with the guidelines specified by the Risk Management Committee in the Annual Risk & Control Self-Assessment (RCSA).

2.3 To evaluate and prepare the Risk Control Progress of each division/department and submit it to the Secretary of the Risk Management Committee within the prescribed timeframe, under the supervision of the Risk Management Committee.

2.4 To perform other duties as assigned by the Risk Management Committee.

3. **Duties and Responsibilities of the Audit Committee**

3.1 To review the adequacy and effectiveness of the internal control system and internal audit system, including ensuring that the Company has appropriate and effective risk management systems for both general operational risks and corruption risks, sufficient to support the internal control framework.

3.2 To consider and provide opinions on the monitoring of compliance with anti-corruption measures.

3.3 To independently monitor risk management.

3.4 To communicate with the Risk Management Committee to ensure understanding of significant risks and their linkage with internal controls.

4. **Duties and Responsibilities of the Internal Audit Function**

4.1 To review and assess the effectiveness of the risk management process, ensuring that the Company has appropriate and effective risk management systems sufficient to support the internal control system, particularly with respect to corruption risks.

Risk Management Process

The Company has adopted the Enterprise Risk Management (ERM) framework in accordance with the guidelines of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as the approach to risk management. The key steps are as follows:

1. Objective Setting
2. Risk Identification
3. Risk Assessment

4. Risk Response
5. Control Activities
6. Monitoring

Based on the COSO risk management process described above, the Company has added two additional components to enhance the effectiveness of the six-step risk management process and increase the likelihood of achieving risk management objectives, namely:

7. Internal Environment

The Company shall establish a supportive environment and atmosphere that form a fundamental basis for effective risk management. Such environment influences the determination of strategies and objectives, the formulation of activities, and the identification and management of risks. The internal environment comprises various factors, including risk management philosophy, beliefs, culture, and ethics; the establishment of an appropriate organizational structure; and the selection of personnel who are knowledgeable, competent, and honest, together with their development to suit assigned responsibilities.

8. Information & Communication

The Company shall establish an effective communication system regarding the risk management policy for all employees to ensure understanding of their roles and involvement in risk management, including awareness of risk levels relevant to their respective divisions/departments. The Company shall also provide channels for receiving organizational information from both external and internal sources to enable personnel to respond to events promptly and effectively, and shall ensure appropriate recording and communication in terms of both format and timeliness.

Step 1: Objective Setting

The organization should ensure that the established objectives are aligned with its strategic goals and acceptable level of risk. Generally, objectives and strategies should be documented in writing and may be considered in the following aspects:

- Vision, mission, goals, and strategic objectives
- Operations, relating to efficiency and performance
- Reporting, relating to both internal and external reporting
- Compliance, relating to adherence to applicable laws, rules, and regulations

Step 2: Risk Identification

Risk identification is the process of identifying risks by determining events that may occur and cause departments or the organization to fail to achieve their objectives. Risk refers to an event (in the future) that may arise under changing circumstances, uncertainty, emergencies, or abnormal situations, which may affect, cause damage or failure, or reduce the likelihood of achieving the Company's goals and objectives at the corporate, functional, departmental, or individual level. The risk identification process comprises the following steps:

1. Consider activities, projects, and related work processes of the Company that may prevent the achievement of objectives and goals.
2. Identify risks and their causes by considering both internal and external sources of risk that may cause each activity or work process to fail to achieve its objectives and goals.

2.1 Methods for Identifying Key Risks

- Workflow and documentation analysis or process analysis
- Brainstorming
- Workshops
- Collection of historical loss event data
- Others

2.2 Sources of Risk from Internal Factors may include:

- The Company's objectives
- Policies, operational strategies, and work processes
- Organizational structure and management systems
- Accounting and financial information
- Corruption (fraud, asset misappropriation, and financial statement manipulation)
- Others

2.3 Sources of Risk from External Factors may include:

- Government policies
- Economic conditions
- Competition (business competitors)
- Laws and regulations
- Natural events
- Corruption (public officials or any other persons in the public or private sectors)
- Others

3. Risk Classification may be classified into four categories:

3.1 Strategic Risk (S), Refers to risks arising from inappropriate formulation or execution of strategic plans, including misalignment among policies, objectives, strategies, organizational structure, and competitive conditions.

3.2 Operational Risk (O), Refers to risks arising from all stages of operations, covering factors related to processes, technology/equipment, and personnel, including corruption resulting from the performance or omission of duties or abuse of authority in any form, fraud, concealment or falsification of evidence to obtain undue benefits, or asset misappropriation, which affect the efficiency of work processes.

3.3 Financial Risk (F), Refers to risks relating to financial management, which may arise from internal factors such as liquidity, credit, and investment management, or from external factors such as changes in interest rates, exchange rates, or counterparty default. Such risks may affect the Company's revenues, expenses, and profit or loss, including financial statement manipulation through omission or intentional misstatement in reporting the Company's financial position.

3.4 External Risk (E), Refers to risks arising from external factors that are beyond prediction or control, such as applicable laws and regulations, corruption involving any act of offering, promising, soliciting, demanding, giving, or receiving cash, cash equivalents, assets, or any other benefits, including bribery in any form, to public officials or any other persons in the public or private sectors, whether directly or indirectly, in order to induce such persons to perform or omit their duties to obtain or retain improper business benefits. This also includes events caused by natural disasters or individuals that may affect the Company's reputation, image, and normal business operations.

Step 3: Risk Assessment

Risk assessment is the process of measuring the severity level of risks identified in Step 2. The assessment comprises the following steps:

1. Consider risks arising from operations prior to the implementation of risk control measures identified in Step 2, by evaluating the severity and likelihood of occurrence before controls are applied (Inherent Risk).

2. Assess risks by analyzing the likelihood of occurrence and the level of impact in accordance with the Company's criteria for determining likelihood and impact levels. Such assessment may be conducted

using both qualitative and quantitative approaches, with the Company defining five levels of assessment criteria.

Assessment of Risk Likelihood and Impact Levels

Events Occurring Within 12 Months	Likelihood Level (Frequency)				
	1 Very Low	2 Low	3 Medium	4 High	5 Very High
Number of Occurrences	0–1 times	2 times	3–4 times	5–7 times	8 times or more
Estimated Occurrence (%)	0–5% within 12 months	>5–25% within 12 months	>25–50% within 12 months	>50–90% within 12 months	>90% within 12 months

Impact	Impact Severity Level				
	1 Very Low	2 Low	3 Medium	4 High	5 Very High
Financial Impact 1. % decrease in the Company's revenue (compared to prior year)	Same as / Higher than	≤ 1%	> 1–5%	> 5–10%	> 10%
2. % increase in the Company's expenses (compared to prior year)	Same as / Higher than	≤ 1–5%	> 5–10%	> 10–15%	> 15%
3. Decrease in EBITDA compared to prior year	Same	≤ 1%	> 1–2%	> 2–3%	> 3%
4. Budget overrun amount	Same	≤ 1–5%	> 5–10%	> 10–15%	> 15%
5. Value of damage (THB)	≤ 10,000 THB	10,001–100,000 THB	100,001–1,000,000 THB	THB 1–5 million	> THB 5 million
Non-Financial Impact 6. Regulatory impact	Verbal warning / Written warning	Written warning (no correction)	Litigation / Fine	Court judgment	Court judgment prohibiting business operations
7. Safety impact - Impact on individuals	Minor injury	Injury requiring medical treatment (no lost time)	Injury requiring medical treatment (lost time < 3 days)	Severe injury (lost time > 3 days)	Disability or fatality
- Environmental impact	No environmental impact	Immediately rectifiable	Rectifiable within a short period	Requires extended period for rectification	Requires significant resources and time for rectification
8. Corporate image impact	Negative news 1–3 days, rectifiable	Negative news 1–3 days, not rectifiable	Negative news 4–15 days, rectifiable	Negative news 4–15 days, not rectifiable	Negative news > 15 days, not rectifiable
9. Stakeholder confidence impact (e.g., customers, employees, shareholders, partners, creditors, media, financial institutions, community/society) (If financial impact can be assessed under items 4 or 5, it shall be classified under financial impact.)	Dissatisfied	Minor impact on business operations / customer complaints	Loss of confidence affecting operations / frequent complaints and claims for compensation	Adjustment / claim for compensation / product recall / consistent decline in sales performance	Potential product boycott / customer lawsuits / business closure

3. The risk levels identified in item 2 shall be used to assess impacts and prioritize control measures as follows:

Risk Assessment

Risk Level		Current Impact (Highest Identified)				
		1	2	3	4	5
Current Frequency	1	2 Low	3 Low	4 Low	5 Medium	6 Medium
	2	3 Low	4 Low	5 Medium	6 Medium	7 High
	3	4 Low	5 Medium	6 Medium	7 High	8 High
	4	5 Medium	6 Medium	7 High	8 High	9 High
	5	6 Medium	7 High	8 High	9 High	10 High

Control Level	
Green	(0–4) Controlled at a satisfactory level; no additional improvement required.
Yellow	(5–6) Controlled at a certain level but not satisfactory; continuous monitoring required.
Red	(7–10) Not controlled; additional controls shall be proposed.

Criteria for Color Determination
(Current Frequency + Current Impact) (Select the highest impact item)

Risk assessment shall be conducted both prior to the preparation of the risk management plan and after the implementation of such plan, in order to determine the effectiveness and efficiency of the risk management plan and whether it should be reviewed or improved.

Step 4: Risk Response

Once risks have been identified and assessed for significance, management shall evaluate feasible risk management approaches. In considering alternative actions, management shall take into account the acceptable level of risk and the costs incurred compared with the expected benefits to ensure effective risk management.

Management may select one or a combination of risk response methods to reduce the likelihood and/or impact of events to a level within the organization's risk tolerance.

Risk response principles include:

- Avoid – eliminate the likelihood of occurrence to zero
- Take – accept the risk
- Treat – reduce the likelihood and/or mitigate the impact
- Share – share the risk with other parties
- Transfer – transfer the risk to other parties

Step 5: Control Activities

Control activities are policies and operational procedures established to ensure that risks are appropriately managed. Control activities may vary depending on the internal environment, nature of business, organizational structure, and culture. A key aspect of control activities is the assignment of responsible personnel within the organization to evaluate the effectiveness of existing risk management measures and to determine additional actions necessary to enhance effectiveness. In addition, risk mitigation actions shall have clearly defined completion timelines.

Step 6: Monitoring

To ensure that risk management is appropriate and of high quality and has been applied at all organizational levels, all risks that significantly affect the achievement of organizational objectives shall be reported to responsible management. Risk management monitoring may be conducted in two forms: ongoing monitoring and periodic monitoring. Ongoing monitoring is performed regularly to enable timely response to changes and forms part of routine operations. Periodic monitoring is conducted after events occur. Continuous monitoring enables prompt resolution of issues. The organization should also prepare risk reports to ensure effective and efficient monitoring of risk management, comprising the following contents:

- Summary report of risk factors and risk levels
- Existing controls and risk management approaches
- Responsible unit/person and residual risk level after controls
- Top five highest risks

- Events with low likelihood but significant impact on employee or public safety, legal violations, material asset damage or impairment, reputational damage, or improper preparation of financial statements and reports
- Reporting to senior management or the Board of Directors

- Sign -

(Dr. Thirachai Pornsinsirirak)

Chairman of the Risk Management Committee