Risk Management Policy

Effective from 19 May 2025

Risk Management Policy

Principles and Rationale

Precise Corporation Public Company Limited and its subsidiaries (the "Company") recognize the importance of enterprise risk management as part of good corporate governance. Effective risk management helps enhance the organization's **resilience** and **agility** in responding to continual changes, whether arising from:

- **External factors** such as politics, economic conditions, or technological innovation.
- **Internal factors** such as organizational structure, work processes, or personnel readiness.

Effective enterprise risk management enables the Company to continue its business operations, minimize the negative impacts of risks, and identify opportunities for growth and competitiveness, to achieve its operational objectives and grow sustainably.

The Company has therefore adopted the Enterprise Risk Management framework in accordance with COSO-ERM 2017, and internal control standards as set out by The Committee of Sponsoring Organizations of the Treadway Commission (COSO) as tools for enhancing the effectiveness and efficiency of the Company's risk management.

Objectives

1) To establish a framework and guidelines for enterprise risk management.
2) To ensure that responsibilities for controlling identified risks are appropriately assigned at the levels of the Board of Directors, management, and employees.

Scope

This Policy applies to all operations of the Company and its subsidiaries and covers all levels of personnel and related parties, including directors, executives, and employees.

Definitions

- **Risk**

  Means an event or situation of uncertainty that may occur and affect achievement of objectives and targets.

- **Enterprise Risk Management (ERM)**

  Means the establishment of policies, structures, processes, and methods that enable the Board of Directors, management, and employees to perform their duties at both the strategic and operational levels in a way that allows the organization to identify potential events, assess their impact on the organization, and determine how

to manage such risks within an acceptable level. This is to provide reasonable assurance that operations will achieve the defined objectives or targets.

- **Likelihood**

  Means the chance or probability that an event will occur.

- **Impact**

  Means the consequence or effect of a risk. A single risk may have multiple potential impacts, both financial and non-financial. Risk impacts may be positive or negative on the organization's strategies or business objectives.

- **Risk Appetite**

  Means the overall level of risk that the organization is willing to accept when a risk event occurs. It is a key factor in evaluating strategic choices for doing business and in setting strategies to achieve the defined objectives or targets.

Risk Management Process

The Company prescribes a five-step risk management process, as follows:

1) Setting Objectives

Each business line and unit at all levels must define operational objectives or targets that align with the Company's vision, mission, strategies, and overall goals. Objectives must be clear, measurable, and capable of being evaluated.

2) Risk Identification

This is the process of identifying risk events or uncertainties that may occur and affect the achievement of business objectives. The Company requires risk management at least at 2 levels

(1) Corporate level
(2) Unit / Process / Project level (as appropriate)

Risks are categorized into 5 main types

(1) **Strategic Risk**

Risk arising from formulation of strategies or management policies that may prevent the organization from achieving its objectives or creating value.

Examples

- Policies that are not aligned with stakeholder needs.
- An organizational structure that drives frequent strategic changes.
- Operational plans that are unsuitable or inconsistent with changing factors and environments, such as economic volatility, competitive intensity, or changes in business partners, etc.

(2) **Financial Risk**

Risk arises from factors that affect the Company's financial position.

Examples

- Investment plans are not sufficiently clear to support financial forecasting.
- Liquidity issues.
- Exchange rate and interest rate fluctuations.
- Lack of new revenue sources, etc.

(3) **Operational Risk**

Risks arising from inadequate or failed internal processes, people, and systems, or from external events.

Examples

- Project delays.
- Use of tools or equipment with inadequate efficiency.
- Errors in contract management and monitoring.

- Low employee motivation.
- Complaints from surrounding communities, etc.

(4) **Compliance Risk**

Risk arising from failure to comply with laws, rules, regulations, or standards relevant to operations, or from laws and regulations that are inappropriate and hinder operations. It may also arise when internal policies and procedures cannot be practically followed.

Examples

- Confusion in selecting which law or regulation to apply when multiple laws or regulations may be referenced in each case.
- Conducting operations contrary to relevant laws or regulations due to lack of due care which may result in non-compliance with external regulatory requirements or with the organization's internal regulations.

(5) **Information System and Information Technology Risk**

Risk arising from the potential occurrence of expected or unexpected events related to the use of information technology that affect the Company's systems. This type of risk is divided into 3 subcategories:

- Hardware Risk
  Refers to risks arising from failures or malfunctions of equipment or network devices, including deterioration due to aging or normal wear and tears.

- Software Risk
  Refers to risks arising from software system failures, such as using programs that are not updated to current versions, which may leave vulnerabilities caused by software bugs.

- Information Risk

  Refers to risks where users within the organization gain access to information systems or data beyond their authorized access level, or where malicious individuals (hackers) steal data or cause damage to computer systems and information assets.

In addition, because the Company places great importance on risk management to ensure sustainable business growth, the risk management process must not be limited solely to achieving economic objectives or targets. All relevant parties must consider risks in multiple dimensions, including environmental, social/community,

and governance aspects, which also encompass risks of corruption and human rights violations in the Company's work processes

3) Risk Assessment

Risk assessment is the evaluation of the materiality of each risk by considering:

- **Likelihood** that the event may occur; and
- **Impact** of the risk.

Those concerned are responsible for assessing the risks of each identified issue. The criteria used for risk assessment should reflect the Company's values, objectives, and resources. The Company uses a **Risk Matrix** as a tool for assessment, as illustrated below:

Risk Matrix

Impact \ Likelihood	1 Low	2 Medium	3 High	4 Very hight
4 Very hight	High	High	Very hight	Very hight
3 High	Medium	Medium	High	Very hight
2 Medium	Low	Medium	Medium	High
1 Low	Low	Low	Medium	High

Level	Represented By	Meaning
Very High		A level of risk that is unacceptable. Immediate and urgent risk management actions are required to bring the risk down to an acceptable level.
High		The level of risk is unacceptable. Risk management actions must be taken to ensure the risk remains at an acceptable level going forward.
Medium		A level of risk that is acceptable, but ongoing and regular control measures are required to prevent the risk from shifting to an unacceptable level.
Low		A level of risk that is acceptable without the need for additional control or risk management measures. However, regular monitoring is still necessary.

Note: *The Company prescribes a special criterion for risk consideration: If any risk receives an Impact score of 4, regardless of the Likelihood score and even if, according to the Risk Matrix, the overall risk level is not classified as unacceptable, the responsible unit or the risk owner must still implement measures to reduce the Impact of that risk to a score of less than 4.*

4) Risk Management

Risk management is the response to risk through the determination of risk treatment measures so that risks can be managed to an acceptable level (Risk Appetite).

In defining risk treatment measures, the Company will:

- Consider the costs and benefits of the proposed actions.
- Assess whether existing risk management measures are sufficient in terms of: Effectiveness in reducing Likelihood; and Effectiveness in reducing Impact of various risks.

If any risk is not yet being managed or existing measures are not sufficient to keep it within an acceptable level (Risk Appetite), additional risk treatment measures must be defined. Such measures must be capable of reducing the Likelihood and/or Impact of the relevant risk in a manner appropriate to that specific risk.

5) Monitoring and Reporting

Monitoring and reporting of risk management results shall be carried out to senior management, the Risk Management Committee, or the Board of Directors (as the case may be), to provide reasonable assurance that the prescribed risk treatment measures are being implemented effectively and appropriately, or to determine whether they need to be adjusted.

The Company requires that risk management results be monitored and reported to the Board of Directors at least twice a year, to track the status of organizational risks and determine:

- Which risks are within acceptable levels.
- Which risks are still in progress (under treatment); and
- Whether any new risks have emerged.

Duties and Responsibilities

1. The Board of Directors is responsible for approving the Risk Management Policy and overseeing risk management for the organization.
2. The Risk Management Committee is responsible for:
    - Reviewing the Risk Management Policy before proposing it to the Board of Directors for approval.
    - Overseeing and supporting the Company to ensure that risk management processes are continuously implemented throughout the organization.
    - Monitoring that management develops and implements risk management plans and providing comments and recommendations for improvement so that risks are managed appropriately.
3. The Audit Committee supports the Board of Directors in performing its risk management duties by reviewing, with a view to obtaining reasonable assurance, that the Company's risk management system is appropriate, effective, and efficient.
4. Senior management plays a key role in implementing the risk management process within the organization by:
    - Building an organizational culture emphasizes the importance of risk management.
    - Monitoring performance and allocating resources so that the Company's risk management is carried out effectively, efficiently, and continuously.
    - Regularly reporting risk management results to the Risk Management Committee and the Board of Directors to ensure that the Company can manage risks and achieve its business objectives sustainably.
5. The Risk and Compliance Management Working Group is responsible for monitoring and supporting the risk management of senior management and the Board of Directors by:
    - Reviewing the Company's Risk Management Policy and proposing enhancements to risk management processes and criteria for consideration by the Risk Management Committee, before submission to the Board of Directors for approval.
    - Reviewing key risk and treatment plans as assessed by the Company or the relevant risk owners.

- Communicating the Company's prescribed risk management processes and criteria to ensure consistent implementation across the organization.
- Monitoring and supporting continuous implementation of risk management.

6. All executives and employees at every level are responsible for complying with this Policy.

7. Internal Audit is responsible for:
   - Reviewing the effectiveness and efficiency of risk management and internal controls through the annual internal audit plan, which focuses on auditing key business processes based on risk (Risk-Based Auditing).
   - Following up on corrective actions for deficiencies identified and reporting them to the Audit Committee.