Risk Management Policy, Guidelines, and Implementation Plan

TQR Public Company Limited

Table of Contents **Page**

Risk Management Policy, Guidelines, and Implementation Plan

1. Principles and Rationale

TQR Public Company Limited (the "Company") recognizes that risk management is an integral part of good corporate governance and a fundamental foundation that enables the Company to achieve its objectives. The identification and management of risks support better decision-making, help identify opportunities, and enable the Company to mitigate the impacts of significant events that may affect shareholders. Risk refers to the possibility of events that may occur and have an impact on the Company's objectives, and can be measured by the level of impact and the likelihood of occurrence.

2. Objectives

The Risk Management Policy (the "Policy") has the following objectives:

2.1 To establish a consistent operational framework for the Company's risk management process to be implemented throughout the organization.

2.2 To ensure that roles and responsibilities for controlling identified risks are appropriately defined.

3. Scope

This Policy shall apply to all operations, including all executives and employees of the Company, as well as its group companies, including persons and juristic entities under the Company's supervision.

4. Risk Management Policy

This Policy shall apply to all operations, including all executives and employees of the Company, as well as its group companies, including persons and juristic entities under the Company's supervision.

4.1 The Company conducts its business within acceptable risk levels in order to achieve its objectives and meet the expectations of stakeholders. Risk management is integrated into the annual business planning process, day-to-day management and decision-making, as well as project management processes.

4.2 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 defining appropriate measures to manage such risks.

4.3 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 risk occurrence and the potential impact if such events occur shall be assessed.
- Risks shall be managed in accordance with the established risk management criteria, taking into account the related costs and the benefits to be derived from such risk management.
- Risks shall be monitored to ensure that the Company's risks are appropriately managed.

- Risks that may affect the Company's business plans and strategies and are classified as high or very high risk levels shall be reported to the Executive Committee, the Audit Committee, and the Board of Directors for acknowledgment.

5. Roles and Responsibilities

5.1 The Board of Directors has overall responsibility for overseeing risk management within the Company.

5.2 The Audit Committee supports the Board of Directors in performing its risk management duties by reviewing and ensuring that the risk management system is appropriate and effective.

5.3 The Risk Management Committee is responsible for considering and reviewing the Company's risk management and internal control systems.

5.4 The qualifications, duties, and responsibilities of the Risk Management Committee shall be in accordance with the Company's Risk Management Committee Charter.

5.5 Executives of each department are responsible for supporting the operations of the Risk Management Committee and for identifying, analyzing, assessing, and prioritizing risks within their respective areas of responsibility, as well as defining appropriate measures to manage such risks.

5.6 All executives and employees are responsible for complying with the risk management measures prescribed by the Working Committee. Reporting the results of the implementation of risk management measures shall be considered part of job responsibilities, and all employees must communicate appropriately and in a timely manner with the Working Committee if any obstacles to the implementation of the prescribed risk management plan are identified.

6. Risk Management Process

The Company has established a policy to manage various risks that are expected to affect the Company, taking into account both internal and external factors, in order to manage risk categories and control risk levels to remain within appropriate and acceptable limits. The Company's management has established the enterprise risk management process as follows:

6.1 Objective Setting

The enterprise risk management process, including the identification of risk types, risk assessment approaches, and methods for defining risk mitigation measures, shall be aligned with enabling the organization to achieve its mission, mandate, objectives, and goals under the principle that the Company conducts its business in accordance with good corporate governance and in alignment with the organization's vision and values.

6.2 Determination of Risk Appetite

Risk appetite refers to the level of risk that management determines as the acceptable boundary for decision-making and the impact arising from such decisions, with the assurance that within such boundaries, the organization will be able to operate sustainably and achieve its established objectives.

may be defined in the form of statements or descriptions to ensure that executives and relevant persons have a common understanding. The level of risk acceptance should be consistent with the risk assessment criteria as specified in the section "**Risk Level Assessment and Acceptable Risk Levels.**"

6.3 Risk Identification

The risk management process shall include regular reviews and consideration of risk factors in all aspects, both internal and external, and shall cover strategic risks, financial risks, management risks, legal and compliance risks, information technology risks, operational risks, as well as corruption risks. The Company has classified the risk categories to be considered as follows:

Table 1: Basic Risk Categories

Main Risk Category	Sub-Risk Category	Definition
Strategic Risk	Strategic Risk	• Risk arising from the formulation of strategies that are not aligned with economic conditions and the competitive environment • Risk of deviation in the execution of strategic plans from those originally defined • Risk arising from significant external events, changes, and uncertainties that prevent the Company from protecting its business value, thereby affecting business growth and shareholder value
	Supply Chain Risk	• Risk arising from shortages of or inability to access necessary resources, such as the inability to obtain reinsurance in accordance with the terms of the cedent, etc.
Financial Risk	Financial Risk	• Risk of losses resulting from non-payment and/or delayed payment • Risk of losses resulting from receiving commissions lower than expected • Risk of losses resulting from liquidity problems of counterparties
Management Risk	Human Resource Risk	• Risk of losses resulting from a shortage of personnel with necessary knowledge and competencies • Risk arising from insufficient or inappropriate personnel development in response to changing business competition • Risk arising from dependence on key personnel
	Operational Risk	• Risk of losses resulting from operational errors • Risk arising from inefficient operations
	Reporting Risk	• Risk of losses resulting from incorrect decision-making or insufficient information for decision-making • of losses resulting from leakage of critical information
	Customer Satisfaction Risk	• Risk of losses resulting from substandard service quality that does not meet established standards • Risk of losses resulting from failure to comply with agreements with customers

Main Risk Category	Sub-Risk Category	Definition
Compliance Risk	Compliance Risk	• Risk of losses resulting from failure to fully comply with laws, notifications, and orders governing the organization's business operations • Risk arising from non-compliance with established regulations, guidelines, and operational procedures
Information Technology Risk	IT Risk	• Risk of losses resulting from unauthorized access to information systems, computer equipment, and critical data by both internal and external parties • Risk of losses resulting from inability to restore information systems within the required timeframe • Risk of losses resulting from cyberattacks, such as denial of access to information systems or data
Fraud Risk	Fraud Risk	• Risk of losses resulting from giving or receiving bribes • Risk of losses resulting from intentional manipulation or concealment of financial statements and reports
Other Risks	Disaster and Uncontrollable Risk	• Risk of losses resulting from criminal acts • Risk of losses resulting from other external factors such as natural disasters, political events, economic conditions, pandemics, and riots, etc.
	Reputational Risk	• Risk of damage to reputation and social acceptance

In order for the management of various types of risks to be carried out effectively, the organization must identify the causes that give rise to such risks. Risk identification and cause analysis may be conducted using various tools and working methods, such as:

- Joint meetings for discussion and exchange of ideas (brainstorming)
- Use of information from experts, external auditors, and internal auditors as supporting inputs, such as internal audit reports
- Opinion surveys
- Use of statistical data
- Analysis Use of problem analysis tools, such as Fishbone Diagrams or Five Whys Analysis

6.4 Risk Level Assessment and Acceptable Risk Levels

Risk level assessment shall be based on the likelihood of occurrence (Likelihood, L) and the impact if such risk occurs (Impact, I), using the following calculation:

Risk Level = Likelihood (L) × Impact (I)

The organization's risk levels can be classified into ranges according to risk scores as follows:

Risk Score Derived from Impact × Likelihood	Definition
Low Risk Level **1 - 4**	Low-level risk that the organization should acknowledge and monitor
Medium Risk Level **5 - 8**	A medium-level risk that the organization should closely monitor in order to be able to take timely action if such risk shows a tendency to increase
High Risk Level **9 - 12**	A high-level risk which, if it occurs, will have a significant impact on operations and the achievement of objectives. The organization must promptly establish measures to control and reduce the likelihood of occurrence and/or the impact of such risk.
Very High Risk Level **16**	A very high-level risk which, if it occurs, will severely impact operations and the achievement of objectives. The organization must immediately establish measures to control and reduce the likelihood of occurrence and/or the impact of such risk, and the progress of such measures must be closely monitored.

The risk levels acceptable to the Company are those classified as low and medium risk, with risk scores ranging from 1 to 8. Risks with a risk score of 9 or higher shall be considered risks that the Company is required to manage and address.

Figure 2: Acceptable Risk Levels (Blue Line Indicator)

According to the illustrated figure above, Risks 2, 3, and 4 are considered acceptable risk levels, with Risk 2 being a risk that the Company must closely monitor. Meanwhile, Risk 1 is considered a critical risk that the Company must promptly take action to reduce the likelihood of occurrence and/or the impact to an acceptable level.

Table 2-1: Impact Levels

Level	Description
4	<u>Performance results fall below acceptable levels:</u> • Loss of competitiveness to the extent that the Company may be unable to continue its business operations • Loss of assets, personnel, and resources amounting to indirect losses of THB 5,000,000 or more, or causing business operations to be disrupted for more than one (1) day • Material errors in information systems that are detected, such as incorrect financial statements, resulting in penalties imposed by government authorities • Financial losses of THB 5,000,000 or more • The Company is subject to criticism by mass media and social media for more than five (5) days or is questioned by government authorities • Loss of key customers resulting in revenue losses of THB 5,000,000 or more • The Company is subject to legal action to the extent that it is unable to continue its business operations
3	<u>Performance results fall below the established targets but remain within acceptable limits:</u> • Loss of competitiveness affecting market share and customers, resulting in growth being more than 10% lower than expected • Loss of assets and resources amounting to indirect losses of THB 500,000 – 5,000,000 or causing business operations to be disrupted for eight (8) hours • Material errors in information systems that can be corrected or explained • Financial losses of THB 500,000 – 5,000,000 • Loss of key customers resulting in revenue losses of THB 500,000 – 5,000,000 • The Company is subject to legal action resulting in business suspension for more than three (3) days or fines of THB 500,000 or more
2	<u>Performance results remain in line with the established objectives but should be closely monitored</u> • Loss of competitiveness affecting market share and customers, resulting in growth being 1–10% lower than expected • Loss of assets and resources amounting to indirect losses of THB 100,000 – 500,000, or causing business operations to be disrupted for four (4) hours • Material errors in information systems that are detected by internal personnel • Financial losses of THB 100,000 – 500,000 • Loss of key customers resulting in sales losses of THB 100,000 – 500,000 • The Company is subject to legal action resulting in business suspension for one (1) to three (3) days or fines of THB 100,000 – 500,000

Level	Description
1	<u>No impact on the achievement of operational objectives:</u> • Minor loss of competitiveness • Loss of assets and resources amounting to indirect losses of less than THB 100,000 • Minor errors in information systems • Financial losses of less than THB 100,000 • The Company receives complaints from residents in nearby areas or affected parties • Order cancellations and debt reductions granted to customers amounting to less than THB 100,000 • The Company is fined an amount not exceeding THB 100,000

Table 3: Frequency and Likelihood Levels

Frequency	Annual Frequency	Probability	Vulnerability
4	Frequent: Occurs weekly (revise to specify the number of occurrences per year)	Almost Certain: Likelihood of occurrence of 90% or higher	There are no risk mitigation measures in place to address or manage the issue.
3	Likely: Occurs monthly	Likely: Likelihood of occurrence between 65% and 90%	Risk mitigation measures exist, but they are insufficient or ineffective.
2	Possible: Occurs quarterly	Possible: Likelihood of occurrence between 35% and 65%	Risk mitigation measures are in place and are adequate and effective, with a reasonable level of reliability.
1	Unlikely: Occurs annually or less frequently	Unlikely: Likelihood of occurrence between 1% and 35%	Risk mitigation measures are in place and are adequate, effective, and highly reliable.

7. Meetings of the Risk Management Committee and Preparation of Risk Management Reports

The Risk Management Committee is responsible for convening meetings to monitor the results of risk management activities, as well as jointly reviewing the appropriateness of the risk management plan and the risk management process. Meetings shall be held on a quarterly basis, and the Risk Management Committee shall appoint a Risk Management Committee Secretary to record the meeting minutes.

In addition to meeting minutes, the Secretary and committee members are responsible for preparing risk management reports, which shall be presented by the Chairman of the Risk Management Committee to the Board of Directors for consideration and/or approval.

8. Review of the Risk Management Policy and Risk Management Process

The Risk Management Policy and the risk management process as specified in this Policy shall be reviewed and updated to ensure alignment with the business environment and the organization's risk profile. The review shall be conducted at least once a year. In the event of any material amendments, the Chief Executive Officer shall present such changes to the Risk Management Committee for consideration, and the Risk Management Committee shall then present them to the Board of Directors for acknowledgment and approval, with such review and approval to take place at least once a year.

This policy is reviewed and will be effective from November 10, 2025 onwards.

Note: Approved by the resolution of the Board of Directors' Meeting No. 7/2025 on November 10, 2025.