RISK MANAGEMENT POLICY

TQR PUBLIC COMPANY LIMITED

FISCAL YEAR: 2024

Effective Date: October 3, 2024

Note: This policy is for internal use only.

Contents

1. Principles and Rationale

TQR Public Company Limited (“the Company”) recognizes that risk management is a key component of good corporate governance. It serves as a foundation to achieve corporate objectives, improve decision-making, identify opportunities, and mitigate potential impacts on stakeholders. Risk is defined as the likelihood of an event occurring that may affect the Company's objectives, measured by its impact and probability.

2. Objectives

This policy aims to:

1. Establish a consistent framework for the Company’s risk management processes applicable across the organization.

2. Ensure clear assignment of responsibilities for risk oversight.

3. Scope

This policy applies to all operations, including executives, employees, subsidiaries, and individuals/entities under the Company’s supervision.

4. Risk Management Policy

1. The Company conducts its business within an acceptable risk tolerance to achieve objectives and meet stakeholder expectations. Risk management is integrated into the annual business planning process, day-to-day operations, and project management.

2. All executives and employees are risk owners, responsible for identifying, evaluating, and managing risks in their areas of responsibility.

3. Critical risks must be managed as follows:

    - Identify risks promptly.

- Assess the likelihood and impact of each risk.
- Manage risks according to the Company's established principles, considering costs and benefits.
- Monitor risks to ensure effective management.
- Report high and very high risks affecting strategic or business plans to the Risk Management Committee, Audit Committee, and Board of Directors.

5. Roles and Responsibilities

1. The Board of Directors is collectively responsible for overseeing risk management within the company.
2. The Audit Committee supports the Board of Directors in performing its duties related to risk management by reviewing and ensuring that the risk management system is appropriate and effective.
3. The Risk Management Committee is responsible for considering and reviewing the company's risk management and internal control systems.
4. The Risk Management Committee's qualifications and responsibilities are in accordance with the company's Risk Management Committee Charter.
5. Each department's executives are responsible for supporting the work of the Risk Management Committee and are tasked with identifying, analyzing, assessing, and prioritizing the risks within their respective departments, as well as determining appropriate measures to manage those risks.

6. All executives and employees are responsible for complying with the risk management measures established by the working group. Reporting the results of actions taken according to the risk management measures is considered part of their duties. All employees must communicate appropriately and promptly with the working group if they encounter obstacles in implementing the designated risk management plan.

6. Risk Management Process

The Company addresses risks impacting its operations by considering internal and external factors. The organizational risk management process includes:

6.1 Objective Setting

Align risk identification and management measures with the Company's mission, vision, and values under good corporate governance principles.

6.2 Determining Risk Appetite

Define acceptable risk levels to ensure sustainable operations and achievement of objectives.

6.3 Risk Identification

- The risk management process requires regular reviews and assessments of risk factors, encompassing both internal and external elements. These factors include strategic risks, financial risks, management risks, compliance risks, IT risks, operational risks, and corruption risks. The Company categorizes risks into key groups as detailed below:

Table 1: Key Risk Groups

Main Risk Group	Sub-Risk Group	Definition
Strategic Risk	Strategic Risk	- Risk from strategies misaligned with economic and competitive conditions.

Main Risk Group	Sub-Risk Group	Definition
		- Risk of deviation from established strategic plans.
		- Risk from external events, changes, or significant uncertainties affecting the Company's value and growth.
	Supply Chain Risk	- Risk from shortages or inaccessibility of essential resources (e.g., inability to secure reinsurance terms).
Financial Risk	Financial Risk	- Risk of damages from delayed payments or non-receipt of payments.
		- Risk from receiving lower-than-expected commissions.
		- Risk from counterparties' liquidity shortages.
Management Risk	Human Resource Risk	- Risk from a lack of skilled personnel.
		- Risk from inadequate staff development for changing business conditions.
		- Risk from over-reliance on key personnel.
	Operational Risk	- Risk from operational errors.
		- Risk from inefficient operations.
	Reporting Risk	- Risk of poor decisions due to missing or inadequate information.
		- Risk of sensitive data leakage.
	Customer Satisfaction Risk	- Risk from substandard service quality.
		- Risk from failure to meet customer agreements.

Main Risk Group	Sub-Risk Group	Definition
Compliance Risk	Compliance Risk	- Risk from non-compliance with laws, regulations, or business operation mandates.
		- Risk from deviations in operational procedures or guidelines.
IT Risk	IT Risk	- Risk from unauthorized access to IT systems or sensitive data.
		- Risk from inability to recover IT systems within required timeframes.
		- Risk from cyberattacks (e.g., denial of access to systems or data).
Corruption Risk	Fraud Risk	- Risk from bribery activities.
		- Risk from intentional financial statement manipulation.
Other Risks	Disaster and Uncontrollable Risk	- Risk from crime or external factors such as natural disasters, political unrest, economic downturns, pandemics, or riots.
	Reputational Risk	- Risk of damage to the Company's reputation and social acceptance.

Risk Management Tools and Practices

Effective risk management requires identifying the root causes of risks using the following tools and methods:

- Collaborative brainstorming sessions.
- Expert insights or audit reports (internal or external).
- Surveys and statistical data.
- Analytical tools like Fish-Bone Diagrams or Five Whys Analysis.

6.4 Risk Assessment and Acceptable Risk Levels

Risk assessment considers the likelihood (L) and impact (I) of each risk type using the formula:

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

Table: Risk Level Categories

Risk Score Range	Risk Level	Description
1–4	Low Risk	Risks requiring awareness and monitoring.
5–8	Medium Risk	Risks requiring close monitoring for timely mitigation.
9–12	High Risk	Significant risks needing immediate control measures.
16	Very High Risk	Critical risks requiring immediate control and close progress monitoring.

Acceptable Risk Levels

The Company considers risk levels of 1 to 8 (low and medium risks) as acceptable, while risks scoring 9 or above require immediate management.

Figure 2 illustrates the acceptable risk level (blue line).

Table 2-1 illustrates the impact levels.

Level	Description
4	**<u>Performance falls below the acceptable level of objectives:</u>** • **Loss of competitiveness to the extent that business operations may cease.** • **Loss of assets, personnel, and resources valued indirectly at 5,000,000 THB or more, or operational downtime exceeding 1 day.** • **Significant errors in information systems, such as incorrect financial statements, detected and adjusted by government agencies.** • **Damage of 5,000,000 THB or more.** • **Criticism by media and social media for over 5 days or inquiries from government agencies.** • **Loss of key customers accounting for revenues of 5,000,000 THB or more.** • **Legal action preventing the company from continuing business operations.**
3	**<u>Performance falls below target objectives but remains within acceptable criteria:</u>** • Performance falls below the acceptable level of objectives: • Loss of competitiveness to the extent that business operations may cease. • Loss of assets, personnel, and resources valued indirectly at 5,000,000 THB or more, or operational downtime exceeding 1 day. • Significant errors in information systems, such as incorrect financial statements, detected and adjusted by government agencies. • Damage of 5,000,000 THB or more.

Level	Description
	• Criticism by media and social media for over 5 days or inquiries from government agencies. • Loss of key customers accounting for revenues of 5,000,000 THB or more. • Legal action preventing the company from continuing business operations.
2	**Performance meets target objectives but requires monitoring:** • Performance falls below the acceptable level of objectives: • Loss of competitiveness to the extent that business operations may cease. • Loss of assets, personnel, and resources valued indirectly at 5,000,000 THB or more, or operational downtime exceeding 1 day. • Significant errors in information systems, such as incorrect financial statements, detected and adjusted by government agencies. • Damage of 5,000,000 THB or more. • Criticism by media and social media for over 5 days or inquiries from government agencies. • Loss of key customers accounting for revenues of 5,000,000 THB or more. • Legal action preventing the company from continuing business operations.
1	**No impact on achieving objectives:** • Performance falls below the acceptable level of objectives: • Loss of competitiveness to the extent that business operations may cease. • Loss of assets, personnel, and resources valued indirectly at 5,000,000 THB or more, or operational downtime exceeding 1 day. • Significant errors in information systems, such as incorrect financial statements, detected and adjusted by government agencies.

Level	Description
	• Damage of 5,000,000 THB or more. • Criticism by media and social media for over 5 days or inquiries from government agencies. • Loss of key customers accounting for revenues of 5,000,000 THB or more. • Legal action preventing the company from continuing business operations.

Table 3: Frequency and Probability Levels

Frequency	Annual Frequency	Probability	Vulnerability
4	Frequent: Occurs weekly (adjust annually)	Almost Certain: Probability ≥ 90%	No risk prevention or resolution measures in place.
3	Likely: Occurs monthly	Likely: Probability 65% - 90%	Risk prevention measures are in place but insufficient or ineffective.
2	Possible: Occurs quarterly	Possible: Probability 35% - 65%	Sufficient and effective risk prevention measures, reliable to some extent.
1	Unlikely: Occurs yearly or less	Unlikely: Probability 1% - 35%	Sufficient and highly effective risk prevention measures, highly reliable.

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

The Risk Management Committee is responsible for holding meetings to monitor the outcomes of risk management, including jointly reviewing the suitability of the risk management plan and process. Meetings are to be held quarterly, and the Risk Management Committee shall appoint a secretary to the committee to record meeting minutes.

In addition to the meeting minutes, the secretary and committee members are responsible for preparing risk management reports. The Chairperson of the Risk Management Committee shall present these reports to the Board of Directors for consideration, approval, and/or endorsement.

8. Review of Risk Management Policy and Processes

The risk management policy and processes outlined in this document should be reviewed and updated to align with the business environment and the organization's risks. This review should be conducted at least once a year. In the case of significant amendments, the Chief Executive Officer is responsible for presenting the proposed changes to the Risk Management Committee for review. The Risk Management Committee shall then present these changes to the Board of Directors for acknowledgment and approval for implementation.

Signed by:

Mr. Chanaphan Piriyaphan

Chief Executive Officer

Policy Review and Enforcement This policy has been reviewed and is effective from October 3, 2024.

Note: Approved by resolution of the Board of Directors Meeting No. 5/2024 on October 3, 2024.