Risk Management Scope, Organization Structure and Operation Status:

Risk Management Policy and Scope

In order to implement enterprise risk management, the Company refers to the framework of the international standard "ISO 31000 Risk Management – Principles and Guidelines" and follows the P-D-C-A model to formulate the “Risk Management Policy"(“The Policy”), which is approved by the Board of Directors on Nov 05, 2018 as the guiding principle for all divisions. The contents of the Policy covers management objectives, organizational structure and responsibilities, risk management procedures and related mechanisms to effectively identify, measure, monitor and control various risks, and manage the risks within an acceptable level. The Company has also reviewed in the Board of Directors on Feb 15, 2023 according to "the Corporate Risk Management Best Practice Principles for TWSE/GTSM Listed Companies" announced by Taiwan Stock Exchange, to continuously review and optimize the operation of the risk management mechanism.

To achieve the objectives of safeguard company assets, reduce impact on business, maximize business gains, and ensure the sustainability of the company, the Company implement risk management from a more comprehensive perspective that encompasses scopes including financial risk, strategic and operational risk, information security risk, and environment and energy risk. Besides, the Company also establish a multi-layer risk management structure. Through the design and operation of multi-layer organizations and management mechanisms, including: (1) all divisions; (2) the Executive Management Team (EMT); (3) the RMC; and (4) the Board of Directors and Internal Audit, featuring the flexibility of risk management, supervision, as well as risk response, to better control risks in a rapid-changing business environment while achieving the Company’s strategic goals.

Risk Management Process

The risk management processes include risk identification, analysis and evaluation, risk treatment, monitoring and review

Risk Identification：The business units should continuously pay attention to internal and external environment changes and consider the impact on stakeholders to identify the risk sources and issues.

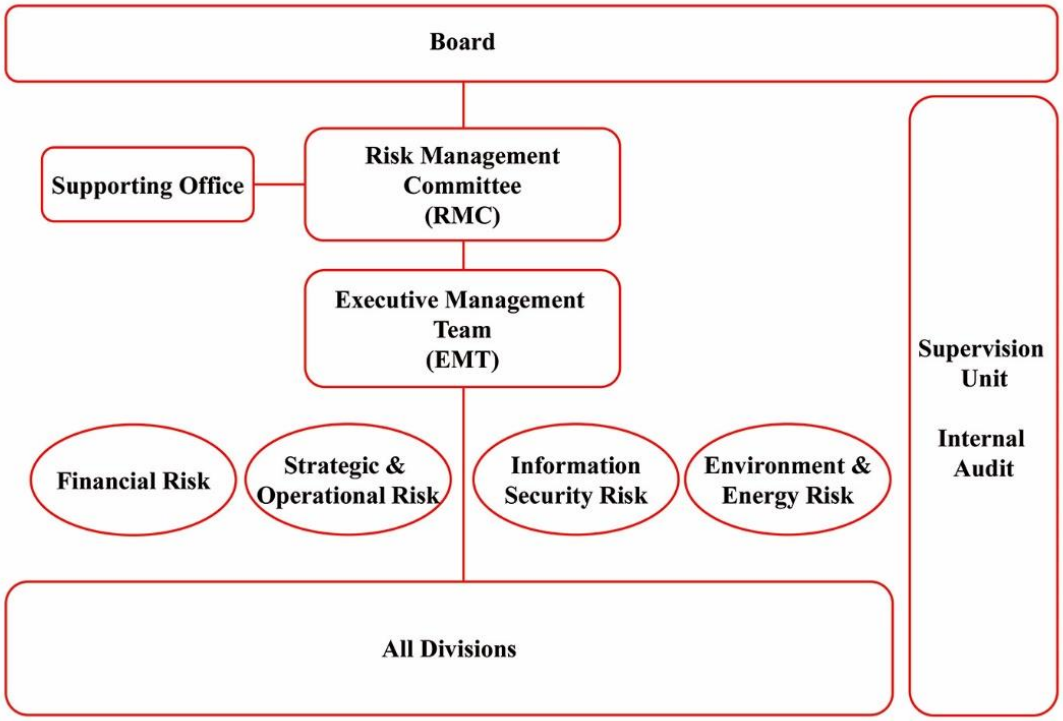
Analysis and Evaluation：The identified risks are analyzed in terms of threat, likelihood and impact. Based on the analysis results, consider the business nature, scale, complexity, opportunity cost, etc. to determine the acceptable level of risk.

Risk Treatment：The business units should determine the priority according to the risk assessment results, and take appropriate countermeasures and actions to control and eliminate the risks.

Monitoring and Review：The business unit should establish risk monitoring procedures, continuously observes and regularly submits risk monitoring reports for review and improvement.

Organization Structure and Responsibilities

FET Risk Governance Organization



Organization	Responsibility
Board of Directors and Internal Audit (Highest decision-making and supervision)	• Board of Directors： • Approve risk management policies and framework. • Ensure the consistency of the operational strategy direction and the Policy. • Supervise the effective operation of the risk management mechanism. • Internal Audit： • Perform audit • Report audit results to the Board of Directors.
Risk Management Committee	• Review risk policies and framework, risk appetite, or tolerance level. • Review management reports on major risk issues. • Periodically report to the Board.
Executive Management Team (EMT)	• Develop risk policies and framework; set risk tolerance and goals. • Implement the Board's and the Committee's decisions. • Allocate resources and manage the overall risks. • Approve the priority of risk control and risk level. • Establish risk management culture.
Supporting Office (risk management promotion and execution unit)	• Assist the Committee operations. • Assist in the formulation, promotion and training of the Policy.

Organization	Responsibility
	• Regularly review the Company's risk category, coordinate the risk assessment results and report for approval. • Assist in supervising the implementation of business units' risk management activities and cross-unit coordination and communication. • Periodically compile and report the implementation status of the Company's risk management.
All Divisions	• Responsible for the identification, evaluation, management, and reporting of daily risks and taking necessary countermeasures. • Monitor risk situations, ensure the effective implementation of control procedures, and make timely reports of risk information to comply with relevant laws, regulations, and corporate policies. • Facilitate and promote relevant policies and regulations.

In addition to the above organizations, if there's risk event occurred, the relevant units shall immediately set up contingency management teams to respond promptly to various risk conditions and communicate with relevant internal and external stakeholders, to ensure compliance with laws and regulations and to minimize potential losses and impacts.

2023 Risk Management Operation Status and Board Report

All divisions of the Company regularly conduct risk assessments based on the materiality principle every year, with consideration of economic, environmental and social aspects of corporate governance issues that may have significant impact on customers, investors and other stakeholders, and develop risk management strategies and plans. For high-risk issues, in addition to regularly reporting risk status, strengthening management and control plan to the Executive Management Team (EMT), the responsibility units also report to the Risk Management Committee (RMC) for supervision and review. The RMC reports to the Board at least once a year.

In 2023, the supporting office has held three meetings to consolidate all divisions' risks assessment results and risk matrix, reported to and get approved by the Executive Management Team (EMT). In addition, the Risk Management Committee (RMC) has held two meetings on February 14 and August 08 respectively, reporting and reviewing high-risk issues of cyberattacks, and system outage risk, including major threat analysis, risk response countermeasures and implementation status. The Company has also reported to the 11th meeting of the 9th term board of directors on November 03, 2023 about the status of risk management and supervision.

Furthermore, to strengthen the employees' information security and privacy risk awareness, the Company has conducted three training courses for all employees in 2023, including "The preventive actions of social engineering attacks", "Case study with Personal Data Protection Act (PDPA)", and "Mobile device security and APP analysis", and the passing rates all achieved 100%. (All trainings include both full-time and contract staffs.)