

Risk Management Scope, Organization Structure and Operation Status:

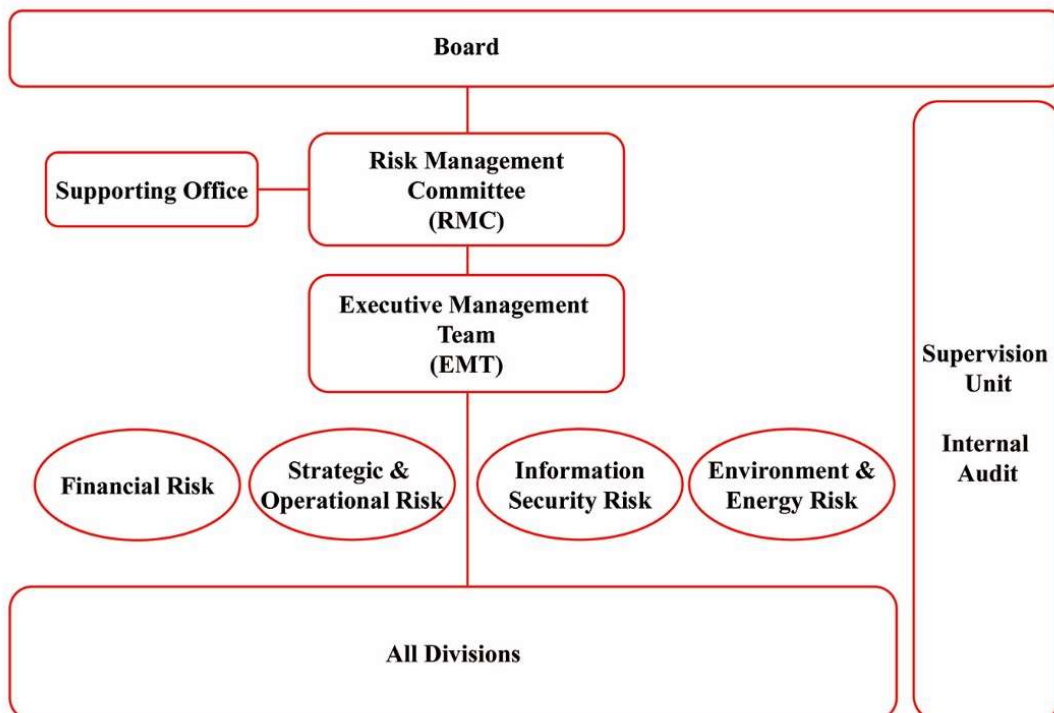
Risk Management Policy and Scope

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.

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.

Organization Structure and Responsibilities

FET Risk Governance Organization



Organization		Responsibility
Highest decision-making and supervision	Board of Directors and Internal Audit	Board of Directors : <ul style="list-style-type: none"> • Approve risk management policies and framework. • Supervise the effective operation of the risk management mechanism. Internal Audit : <ul style="list-style-type: none"> • Perform audit • Report audit results to the Board of Directors.
Third-layer management	Risk Management Committee	<ul style="list-style-type: none"> • Review risk policies and framework, risk appetite, or tolerance level. • Review management reports on major risk issues. • Timely report to the Board.
Second-layer management	Executive Management Team (EMT)	<ul style="list-style-type: none"> • Develop risk policies and framework; set risk tolerance and goals. • Implement Board of Directors decisions, allocate resources effectively, and manage the overall risks. • Establish risk management culture.
First-layer management	All Divisions	<ul style="list-style-type: none"> • 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.

2022 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 2022, 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 22 and August 02 respectively, reporting and reviewing high-risk issues of cyberattacks, energy supply and regulatory compliance risks, including major threat analysis, risk response countermeasures and implementation

status. The Company has also reported to the 7th meeting of the 9th term board of directors on November 11, 2022 about the status of risk management and supervision.

Furthermore, to strengthen the employees' information security and privacy risk awareness, the Company has conducted two training courses in 2022, including "Personal Data Protection Act (PDPA) case analysis" with totally 5,369 participants, and "Information Security Protection Fundamentals" with totally 5,300 participants. (The number includes both full-time and contract staffs.)