Risk Management Policy, Organization Structure and Operation Status

Risk Management Policy and Scope

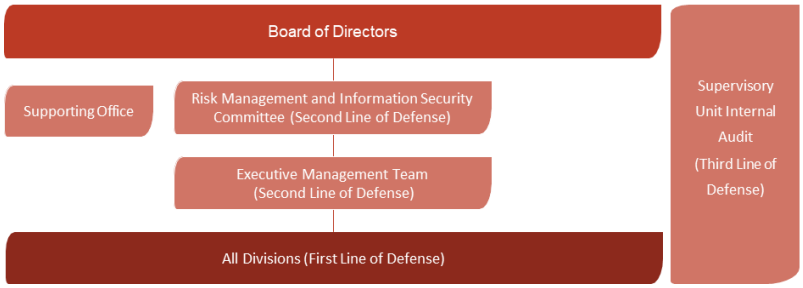
To implement corporate risk management, FET refers to the international standard "ISO 31000 Risk Management - Principles and Guidelines" and follows the P-D-C-A (Plan-Do-Check-Act) model to formulate the "Risk Management Policy", which was approved by the Board of Directors on November 5, 2018, and serves as the guiding principle for all divisions. The policy covers management objectives, organizational structure and responsibilities, and risk management procedures to effectively identify, measure, monitor, and control various risks, ensuring risks are kept within acceptable levels. Furthermore, FET reviews with the Board of Directors on February 15, 2023, continuously enhances the Policy and the operation of risk management mechanisms in accordance with "Corporate Risk Management Best Practice Principles for TWSE/GTSM Listed Companies" announced by the Taiwan Stock Exchange and passes the amendment of the Charter of the Risk Management Committee. The Risk Management Committee ("the Committee") was established since November 2018 and is a board-level functional committee. Its members are appointed by the Board of Directors, with more than half of them being Independent Directors. To emphasize the importance of information security, the Board of Directors approved to rename to the Risk Management and Information Security Committee ("the Committee") on May 3, 2024. This also demonstrates FET's ongoing commitment to information security and customer privacy protection.

FET categorizes and implements risk management in the following areas: Financial Risk, Strategic and Operational Risk, Information Security Risk, and Environment and Energy Risk. To achieve comprehensive risk management, the Company has established a multi-level risk management framework that includes all divisions, Executive Management Team, Risk Management and Information Security Committee, 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

All divisions serve as the first line of defense for FET's risk management. They are responsible for identifying, assessing, managing, and reporting daily risks within their respective units, as well as implementing necessary countermeasures. The Executive Management Team ("EMT") and the Risk Management and Information Security Committee ("the Committee") serve as the second line of defense. They are responsible for reviewing and formulating risk management policies, establishing risk appetite or tolerance, and overseeing the review of significant risk management situations. Internal Audit serves as the third line of defense and is responsible for conducting independent reviews of compliance and the effectiveness of risk management mechanisms.

Risk Management Organization Structure



Risk Management Scope

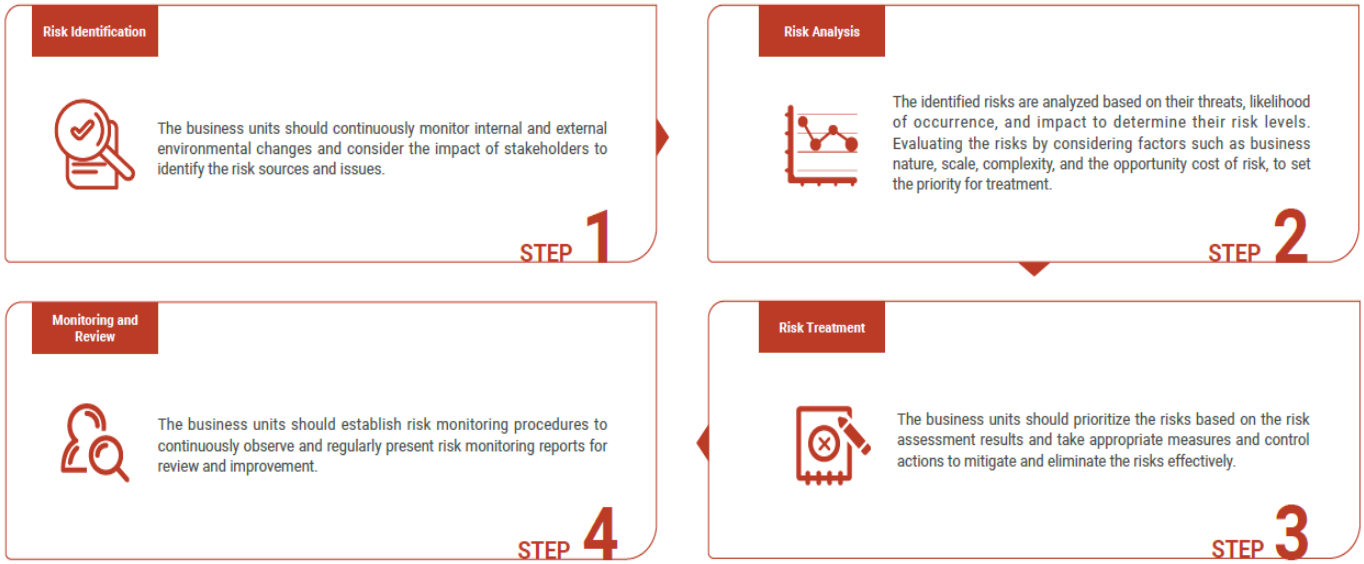
The responsibilities of each level are outlined as follows:

Organization	Responsibilities
Board of Directors **Highest decision-making unit**	• Approve risk management policies and framework. • Ensure the consistency of the operational strategy direction and the Policy. • Supervise the effective operation of the overall risk management mechanism.
Internal Audit **Supervisory Unit** **(Third Line of Defense)**	• Perform Audit. • Report audit results to the Board of Directors.
Risk Management and Information Security Committee **(Second Line of Defense)**	• Review policies & framework, risk appetite or tolerance level • Review major risk issues and management report • Review information security and privacy protection strategies, major plans and management effectiveness • Periodically report to the Board
Executive Management Team **(Second Line of Defense)**	• 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. • 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 **(First Line of Defense)**	• 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.

The Board of Directors is the highest decision-making body for risk management. They are responsible for approving the company's risk management policies and framework and overseeing the effective operation of mechanisms. The Committee reviews the risk appetite, risk tolerance, and management of significant risk issues, and reports on the operation of risk management to the Board of Directors at least once a year.

Risk Management Process

FET's risk management process is primarily based on the international standard "ISO 31000 Risk Management - Principles and Guidelines" and the P-D-C-A framework. These procedures encompass risk identification, analysis, treatment, monitoring, and review.



In addition, FET has established risk appetite for various risk categories and conducts regular reviews and reports to the EMT and the Committee. Once approved, it serves as a reference for all divisions in assessing and responding to risks.

► FET's Four Risk Appetite Categories:

1. Financial Risk

FET is cautious for financial exposure or loss. We aim to have the right balance among prudent financial policies, sufficient business investments, and various stakeholders' interests, to optimize a high level of return in pursuing strategic objectives.

2. Strategic & Operational Risk

FET is willing to accept reasonable risks for innovative technology solutions to meet user demands in the rapid-changing business environment. Whilst, FET is committed to comply with relevant laws and provide high quality services to our customers. We implement strict policies to minimize the risks on business continuity to maintain market competitiveness and esteemed reputation.

3. Information Security and Privacy Risks

FET has no appetite (zero tolerance) for unauthorized access to systems and confidential data. We implement strong management and technical control measures to mitigate risks and keep information and communication infrastructures and customer data secured.

4. Environmental and Energy Risks

FET minimizes environmental hazards and energy supply risks through innovative technology and Environmental Sustainable Development. We enhance facility resilience with backup planning and diverse renewable energy sources to reduce operational risks.

2025 Risk management operations and report to the Board

All divisions conduct regular assessments to evaluate the significant impact on customers, investors, and other

stakeholders in terms of economic, environmental, and social aspects of corporate governance. Risks are identified and assessed based on the operational impact and likelihood. The review of the company's risk exposure is carried out at least twice a year, including the assessment initiated by the Supporting Office of RMSC and regular risk assessments that adhere to international standards. Each unit should develop a risk management plan and implement necessary countermeasures based on their risk appetite, the results of risk assessment, and the priority order.

Additionally, each department must consistently monitor and evaluate the level of exposure in their daily operations and submit regular (weekly or monthly) monitoring reports. The responsible units should review and improve their practices based on the monitoring and audit results, as well as any risk events that have occurred to ensure the ongoing effectiveness of risk governance. If significant exposure situations are identified that pose a threat to financial, operational, or legal compliance, immediate action should be taken and reported to the relevant supervisors and the emergency response team(*Note). For major risk issues, in addition to regularly reporting the risk status to the EMT and strengthening control plans, the responsible units should also submitted these issues to the Committee for review. The Committee has held two meetings on May 06 and Aug. 05, 2025. On Nov. 06, 2025, the Committee further reported to the Board of Directors regarding the supervision of risk management.

(*Note) The operation of the emergency response team is divided into two levels based on the severity of the incidents. Different levels of supervisors oversee the response, coordinating with relevant units to manage the emergency. The response team also keeps overseeing the impact on internal and external stakeholders, communicating as necessary to minimize risks and potential impacts on customers and the company.

In 2025, the Supporting Office coordinated the identification and evaluation of execution risks for all divisions and submitted them to the Executive Management Team for approval. Major risk issues were selected for review by the EMT meeting and the Committee. The content includes primary threat analysis, risk response strategies, and implementation status. The issues include the following:

Risk Topics	Impact Analysis	Response Strategy
Cyberattack risk	The threat of cyberattacks continues to intensify, with global ransomware attack incidents surged by 87% since Feb. 2025.	FET deploys a layered security mechanism with defense-in-depth, implementing various technical protection measures and management activities to reduce the risk of attacks. Furthermore, it enhances employees' security awareness and familiarity through drills, and to improve the incidents response measures.
Climate change and disaster risk	The climate change and natural disaster risk trends indicate that typhoons are becoming less frequent but stronger, floods and droughts are becoming more unevenly distributed, and prolonged periods of high temperatures are significant. Through assessment, it shows that compound natural disasters have the highest impact on the business continuity of telecommunications networks, mainly affecting the communication network switching facilities and base stations.	FET continuously to strengthen and ensure the power backup capabilities for network switching facilities and base stations, as well as the backup routes for transmissions, regularly analyze disaster potential trends, and conduct drills to enhance the resilience of important facilities against disasters.

Emerging Risks

In response to domestic and international situations, FET continues to identify emerging risks in the environmental, social, and governance aspects, assess the impact on operations, and formulate strategic measures to reduce the impact on the company. Annual identification of emerging risks and the corresponding measures are as follows:

Key Emerging Risks	Risk Area	Potential Impact Analysis	Adaptation and Mitigation Measures
Geo-politics	**Geo-political Aspects**	According to the latest Global Risk Survey released by Oxford Economics on August 2, 2023, a survey of more than 100 international companies showed that the views of the international business community on major threats to the global economy have undergone significant changes, including the Taiwan Strait, North and South Korea, etc. Geopolitical tension is considered to be the top risk in the next five years. If these tensions escalate, they could potentially give rise to the third major risk - deglobalization risk. FET is a critical infrastructure provider in charge of important facilities such as base stations, mobile communication networks, and server rooms, in the face of unstable geopolitical conflicts, the potential impact assessments are as follows: Infrastructure attacks and cybersecurity threats: Geopolitical tensions may endanger the normal operation of mobile communication networks; for example, in recent years, the possibility of national-level cyberattacks triggered by technology has continued to exist, and the threat to critical infrastructure has increased significantly. This situation may lead to interruption of telecommunications services and disruption of business or personal communication links. Supply chain disruptions: In the face of global geopolitical tensions, if the supply chain in some regions is interrupted due to geopolitical factors, it may cause delays in the timely supply of critical components for communication infrastructure or key networking equipment, leading to service disruptions or downgrades	• Redundancy, Backup, and Recovery Plans: Develop effective redundancy and backup mechanisms, establish disaster recovery site backup solutions, increase spare equipment components, and conduct regular drills to ensure the continuity of critical operations and the ability to respond quickly and restore normal service in emergencies. • Enhance the resilience of the Supply Chain: Establish diversified sources for the supply chain to reduce reliance on specific regions or suppliers.
Energy Shortage	**Environ-mental Aspects**	Energy shortages may impact FET's operations in terms of both primary power supply and water resources, which could result in the following potential risks: (Electricity and water costs account for about 10% of FET operating expenses) Unstable power supply or water shortage: This may lead to disruptions or decreased quality of communication services, potentially causing customer-related compensations and other issues. Increased operating costs: Due to the demands of government energy transformation, the proportion of high-cost renewable energy continues to increase, international fossil fuel prices continue to rise, renewable energy supply is unstable due to weather or disasters, or energy shortages caused by government energy transformation failures, etc., the company may need to pay higher electricity bills in the future (it is estimated that the next three to five years may increase by 20% to 30%), or need to increase operating costs for backup solution due to energy shortages. Impaired service quality and satisfaction: Malfunctioning base stations and equipment can result in poor call quality, and slower or unstable network	FET regularly assesses its energy usage, formulates comprehensive long-term energy strategies, sets energy management objectives, and implements multifaceted measures to address and control energy-related challenges, including: • Carbon Reduction Targets: FET has already achieved the Science Based Target, aiming to reduce greenhouse gas emissions from Scope 1+2 and Scope 3 by 42% compared to 2021 levels by 2030. • Technological Innovation and Digital Transformation: Optimizing energy management control systems, adopting high-efficiency power conversion equipment, and replacing outdated equipment to improve energy efficiency and reduce energy costs and greenhouse gas emissions. • Backup Power Systems and Expansion of Water Storage Capacity: Regularly assessing backup capacity, establishing emergency support suppliers, and periodically replacing outdated backup equipment to meet future

		speeds, impacting customer experience and satisfaction, and potentially damaging the company's reputation.	energy demands. • Implementation of Energy Storage Systems: Strengthening the application of energy storage technology to effectively utilize intermittent energy sources and provide temporary energy support during energy shortages, ensuring stable energy supply. • Diversification of Energy Sources: Establishing a diversified energy supply structure to reduce the risk of dependence on a single energy source.

Sensitivity Analysis and Stress Testing

FET conducts sensitivity analysis and stress testing on financial risks as well as non-financial risks, such as operational risks, information security risks, and environmental and energy risks. The responsible units are tasked with identifying and analyzing potential threats and weaknesses. They conduct regular sensitivity analyses or stress tests each year for various risks. They implement control measures and continuously monitor and improve to ensure the effectiveness of risk management.

Financial Risk	FET's financial unit conducts an annual financial risk identification to assess the impact of the evaluation results on the company's earnings per share (EPS). Subsequently, adjustments are made to the hedging and financial risk management strategies to ensure that the company's exposure remains within a controllable range.

Non-financial Risks	FET has adhered to the recommendations of the Task Force on Climate-related Financial Disclosures (TCFD) in order to thoroughly evaluate and analyze the potential effects of climate change and energy risks. FET conducts disaster prevention drills every six months for its main generators, which include simulating typhoons, floods, and other natural disasters. To simulate potential power outages caused by typhoons, it is necessary to perform load tests and stress tests (no-load test should be conducted twice a month, and load test once every six months) on the emergency generators at the main server rooms. Additionally, contracts should be signed with external fuel suppliers and drills should be conducted.

FET regularly conducts risk identification, analysis, and assessment to address information security and privacy risks. FET also develops Business Continuity Plans (BCPs) and conducts simulations of scenarios such as natural disasters and cyberattacks in collaboration with relevant units. Additionally, FET plans and carries out multiple tests and drills for network services and core communication systems each year to ensure uninterrupted operation. Continuous review and improvement efforts are undertaken to maintain the seamless operation of critical services.

Supervision and Management

FET pays attention to both internal and external risks and continuously reviews and enhances its risk management mechanisms through internal and external audits. Externally, we have implemented international standard validations in various areas, including ISO 27001 for information security management, BS 10012 for personal information management, ISO 20000 for service management systems, ISO 50001 for energy management, ISO 14001 for environmental management, and ISO 14064-1 for greenhouse gas inventories, etc. Each year, the responsible unit initiates risk identification, analysis, assessment, risk treatment, and corrective and preventive actions. Furthermore, FET has conducted ISO31000 risk management audit by external third-party institute to ensure completeness and effectiveness, driving continuous improvement and optimization on risk management mechanisms.

Internally, the Internal Audit Division serves as the supervisory unit, regularly reviewing the operations of risk management in the audit plan and reporting the findings to the Board of Directors. Through the implementation of multiple lines of defense, including all divisions, Executive Management Team, Risk Management and Information Security Committee, Board of Directors, and Internal Audit, the company is able to effectively manage risks, oversee

operations, and respond to risks in a flexible manner. This ensures timely risk control, prompt response, and effective management to achieve the company's strategic objectives.

Promotion of Risk Culture and Awareness

FET's directors participate annually in external training courses and seminars to stay informed about the latest overall risks, potential opportunities, and challenges. For details, please refer to the official website-director training.

In addition, Risk management relies on the joint efforts of all employees. According to FET Risk Management Policy, to enhance the staffs' risk management capabilities, and internalize the corporate culture, the relevant units need to regularly promote or arrange trainings. In 2025, FET communicates risk management objectives, policies, risk management processes and principles to all employees through training courses, promotional messages, corporate intranet/websites. The company-wide trainings including "Integrity Management, Professional Ethics, Anti-Corruption, Anti-Bribery, and Insider Trading Awareness", "Workplace Health and Safety", and "Defense Techniques against Social Engineering Attacks", etc., to constantly enhance the corporate risk culture. design innovative forms of activities, including computer login pop-up screen design, etc., to increase the attention and promote risk awareness throughout the company.

FET also requires the establishment of necessary risk management mechanisms in the operations of each unit. For instance, when developing products and service systems, we strictly follow the principle of Security by Design. We integrate security controls at every stage of the system development life cycle and conduct mandatory security testing in accordance with the requirements of regulations and standards before launching. This enhances the security and resilience of the services we offer to customers, guaranteeing top-notch service quality.

As for financial incentives of risk management, FET sets performance Key Performance Indicators (KPIs) for all employees based on their positions and annual goals to motivate them. Risk management and agile response at work are also one of the evaluation indicators. Combined with the company's performance appraisal system, employees with excellent performance will be commended and rewarded, such as Performance bonuses and special incentives are provided to encourage and shape the management responsibility and risk awareness of all staffs. Including but not limited to the following:

- Store and customer service risk management rewards: Provide rewards based on indicators such as customer service quality, operational accuracy, customer satisfaction, and social responsibility care.
- Information security and emergency response management rewards: Provide rewards for emergency response to risk situations to reduce the impact on customers and the company.
- Business and operational innovation risk management rewards: evaluate and provide rewards for risk control of business innovation and operational operations.