

Risk Management

Basic Policies

Based on the Fuji Electric Risk Management Rules, the Company manages risks in a coordinated, systematic manner. We practice appropriate management and counter various risks that could

Risk Management System

The Company’s business divisions and affiliated companies are responsible for managing risks related to their business activities as a part of their business duties, developing appropriate risk management systems, and implementing risk countermeasures. However, amid an increasingly complex operating environment shaped by climate change, large-scale disasters affecting broad areas, geopolitical risks, and responses to economic security concerns, we will strengthen risk management for common risks across the Company.

Significant risks, such as those related to business plans and large-scale investments, are reported at the Executive Committee as appropriate to facilitate the sharing of information. We also have manuals in place to ensure that risks are steadily managed. We provide training in handling each type of risk and inform the whole Company about our efforts to manage risks through company magazines and other appropriate means.

The internal auditing divisions conduct regular audits to check whether each business division and affiliated company identifies and evaluates risks based on the Fuji Electric Risk Management Rules, defines countermeasure policies, and properly builds and operates management systems. In fiscal 2025, we conducted internal audits at 46 bases.

In fiscal 2026, we will establish a new Risk Management Office within the Corporate Management Planning Headquarters, which oversees risk management across the Company. As part of the internal control system, the Office will systematically identify and evaluate risks that could have a significant impact on management, including company-wide BCP*, security, and economic security, and will work to collect information in cooperation with relevant parties, establish systems, and deploy countermeasures.

*Business Continuity Plan

Emergency Response

If an emergency arises due to a large-scale disaster, accident or any other serious cause, we need to act to prevent the situation from becoming any worse and resolve the situation as soon as

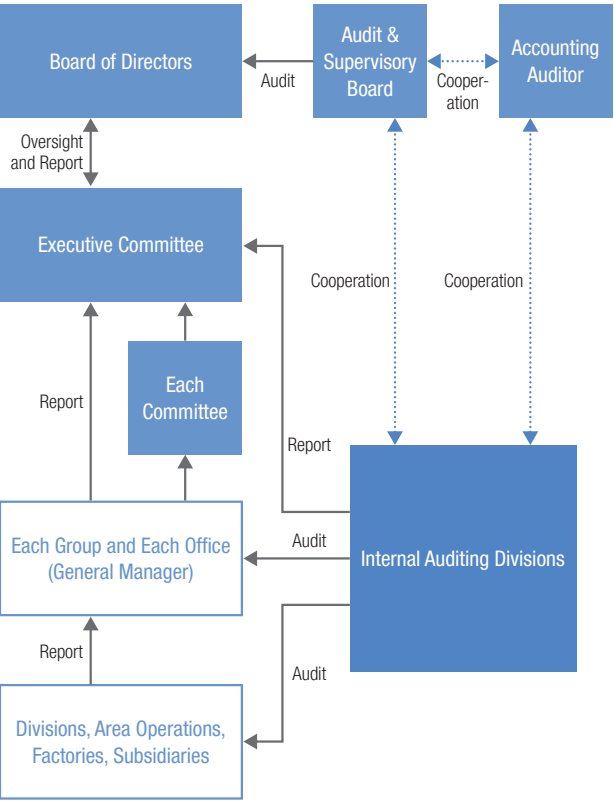
Risk Management Process

When annual budgets are formulated, the Company’s business divisions and affiliated companies gain an understanding of and evaluate risks related to their business activities.

They consider policies and countermeasures in response to each risk (aversion, mitigation, relocation, retention, etc.) based on the impact on management and the frequency of occurrence, and implement these policies and countermeasures by appointing a person in charge of execution in each division or other unit.

We conduct an interim follow-up after the end of the second quarter, followed by an annual evaluation of risk countermeasures and the formulation of countermeasures for the next fiscal year.

affect Fuji Electric’s management in order to prevent risks from materializing (crisis situations), thereby minimizing the impact on management in the event that risks do materialize.

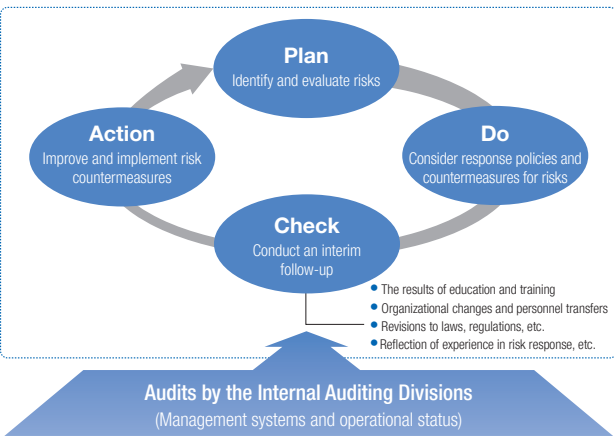


For the list of major risks, please refer to our website. https://www.fujielectric.com/csr/governance/risk_management/risk/governance_risk_factors.html



possible. Hence, we have guidelines in place on preparations for possible emergencies, an emergency contact network, and setting up an emergency task force.

Annual Risk Management Process



Responding to Natural Disasters and Accidents (BCP Efforts)

In order to resume and continue the important businesses within the required time, even when unforeseen situations such as large-scale disasters and accidents occur, we have formulated business continuity plans (BCPs) and are making efforts company-wide for continuous improvement, based on the Fuji Electric Business Continuity Management (BCM) Rules.

In addition to formulating BCPs at the head office, factories, and area operations, which serve as contact points with customers, we have comprehensively formulated BCPs for functions that are essential for business continuity, such as measures for early recovery and minimizing damage to IT systems, response to natural disaster risks in the procurement field, and multi-sourcing. Furthermore, we implement education and training based on the formulated BCPs and regularly evaluate the effectiveness of the BCPs and their management system once every six months at the “Company-wide BCM Promotion Meeting.” For BCPs formulated at factories and area operations, the Crisis Management Secretariat checks, assesses, and verifies whether the assumed scale of disasters and damage reflects the latest risks, as well as the appropriateness of target recovery times and strategies for business continuity. Through these efforts, we work to improve BCPs and strengthen our business continuity capabilities.

Furthermore, to ensure reliable execution of emergency response and business continuity measures, we hold “Business Continuity Seminars” for business manager-level employees and “Disaster Response Headquarters Drills” at each base on an ongoing basis. Four times a year, we also conduct drills that simulate a situation in which the head office’s disaster response headquarters is non-functional due to a large-scale earthquake.

In recognition of these proactive business continuity initiatives, we have obtained and renewed the “Resilience Certification” as an organization that contributes to national resilience.

Strengthening Security Measures

To address the threat of cyberattacks, we are continuously strengthening cybersecurity and governance, including information management and operational structures.

Efforts to Maintain and Strengthen Information Security

To properly manage as confidential information all asset value such as management, commercial and technical information and personal information held by Fuji Electric, the Company has redeveloped and rolled out policies and regulations related to information security based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Furthermore, we have also established management systems at Fuji Electric as well as Group companies in Japan and overseas, and we provide regular training to all of our employees, manage access to operating sites and offices, implement Internet device and computer security measures, and conduct annual inspections regarding the status of efforts taken by each workplace.

In addition, to respond to increasingly diversified and sophisticated cyber-security threats, we endeavor to strengthen our computer security incident response team and security operation center (CSIRT/SOC), our monitoring of signs and

information related to new cyberattacks, and our information-system defense and attack monitoring functions.

At our bases as well, we strive to improve our information security countermeasures based on the requirements of our business partners, related industry organization guidelines, market trends, and other factors, and in businesses for which public certification of information security management is required, two departments and two subsidiaries of Fuji Electric Co., Ltd. have acquired information security management system (ISMS) certification. Furthermore, concerning personal information protection, Fuji Electric Co., Ltd. and two of its subsidiaries have acquired the Privacy Mark certification.

Strengthening Product and Factory Security

Product security must be strengthened to comply with laws and regulations such as the EU Cyber Resilience Act (CRA). With digitalization, products and systems such as drive control systems, control equipment, and monitoring and control systems are increasingly connected to networks. Technologies (embedded security) and support that maintain a secure state throughout the entire product life cycle (design, development, shipment, operation, etc.) are becoming increasingly important.

To improve the quality and ensure a stable supply of our products and services, we have been promoting certification under the international standard for control system security, IEC*1 62443-4-1, since fiscal 2023. In April 2026, in addition to the five bases that had already obtained certification (the Tokyo Factory, Suzuka Factory, Kobe Factory, Hakko Electronics Co., Ltd., and Fuji Electric FA Components & Systems Co., Ltd.), the Tsukuba Factory also obtained certification. The Tokyo Factory also had its certification renewed in recognition of its continued operation of the “secure product development process.”

In fiscal 2026, we will establish a new Security Committee and launch organizations with functions for new product security incident response (PSIRT*2) and factory security incident response (FSIRT*3), in addition to the existing function for information security incident response (CSIRT*4). These organizations will coordinate their activities across organizational boundaries to appropriately address diverse cyber threats and minimize risks. Through these initiatives, we are working to improve the quality and ensure the stable supply of products and services delivered to customers.

*1 IEC: International Electrotechnical Commission
*2 PSIRT: Product Security Incident Response Team
*3 FSIRT: Factory Security Incident Response Team
*4 CSIRT: Computer Security Incident Response Team

Initiatives to Strengthen Project Management

We are committed to reducing the risks of incurring losses by strengthening project management in order to further enhance our corporate value through profit-oriented management.

To facilitate early identification of loss risks and predictive maintenance, we analyze the causes of major losses that have occurred and share them with relevant divisions within the company. We also implement measures to prevent recurrence and monitor such implementation.

In particular, we will continue efforts to enhance training at our overseas bases, leading to further strengthening of project management and an even greater reduction in the risk of losses.