Information Security Management

Material Issue
GRC

Governance

GRI:3-3

The Fuji Oil Group's Sustainability Committee[*1] is an advisory body to the Board of Directors that is chaired by the President and CEO. It deliberates on and monitors the material ESG issue[*2] of Governance, Risk, and Compliance (GRC) from a multi-stakeholder perspective, and recommends the results to the Board. The Chief Financial Officer (CFO) oversees the progress of initiatives for Information Security Management, a priority action within this material issue.
In addition, an Information Officer and a Computer Security Incident Response Team (CSIRT) were established under the CFO at each Group company. The CSIRT also appointed an information management director and an information security manager for each Group company. We aim to systematically raise the information security level of all Group companies, with the advice of external experts.

*1 Governance, Strategy, Metrics and Targets, Risk Management > Governance
https://www.fujioilholdings.com/en/sustainability/sustainability_management/

*2 Governance, Strategy, Metrics and Targets, Risk Management > Strategy, metrics and targets
https://www.fujioilholdings.com/en/sustainability/sustainability_management/

Strategy

Our Group recognizes information security as a risk category directly tied to our business, and is working to strengthen our information security management.
Neglecting to address risk may lead to failures in business continuity and damage to corporate value, such as system destruction or confidential information leaks caused by cyber-attacks. Promoting measures against risk can be an opportunity to foster trust among stakeholders and increase corporate value.
Our Group formulated the Information Management and Information Security Regulations (revised in FY2022) and trains employees on a continual basis to ensure that they understand and follow these regulations.
We also establish appropriate operational processes and rules for information systems to ensure and maintain the confidentiality, integrity and availability of internal and external information assets, while on a technical level we are taking multilayered measures to prevent unauthorized access from outside the Group's information systems and to protect against computer viruses. These efforts help us fulfil our corporate social responsibilities by continuing to provide reliable products and services, and properly managing all critical information we receive from customers, business partners and various stakeholders involved in our business operations.
As digital technology and data use become increasingly vital to our operations, we will work to ensure information security, and promote the digital transformation (DX) of our Group to further strengthen our competitiveness.

Risk Management

Education

Since FY2018, we have been conducting IT security training for our Group employees to raise awareness, mainly by e-learning. The completion rate in FY2023 was 96.3%.[*] We will work to develop the content of the training and encourage participation with the aim of achieving 100% participation in the future.

* Targeted at officers, executive officers and employees of our Group who have a company email address and use a computer in their day-to-day operations.

Internal security audit

Since FY2020, we have been conducting internal security audits within our Group in order to assess the state of compliance with security requirements together with explicit evidence, and to set up a PDCA cycle for correction. In FY2024, we will update the evaluation items covered by the audit to include OT* security measures and cloud services used by business divisions, as we will conduct more effective internal audits and self-assessments.

Results are reviewed for each company subject to internal audits, and for any non-compliant items, an improvement plan is created with the company's information security manager (usually the IT manager), and summarized as a final report on the results. Afterwards, upon approval of the information management director (usually an officer), the measures for improvement are properly carried out.

* Operational technology (OT) comprises the systems and their associated technologies which control and operate control devices in factories and other facilities.

Metrics and targets

GRI:418-1

○ At least 90% complete △ At least 60% complete ✕ Less than 60% complete

FY2023 Goals	FY2023 Results	Self-assessment
Prevent serious security incidents across the entire Group	No major incidents that impacted business continuity occurred	○
Continue conducting measure evaluations by CSIRT, which include internal security audits (FY2023 plan: IT evaluation for six companies, OT evaluation for four companies)	Conducted internal IT security audits at a total of six companies according to plan, and OT security assessments at a total of six companies, exceeding what was planned	○

Analysis

COBIT* Level 4 requires the ability to demonstrate implementation of activities that ensure IT security, to measure the status of information asset protection and IT security assurance compliance, and to be ready to implement improvements when necessary. To meet these requirements for maturity of IT governance, we introduced an evaluation system by the CSIRT, including internal security audits. In FY2023,we conducted checks for 12 Group companies. Furthermore, from FY2023 we have included specific details on security response, such as protection, detection and recovery, in the evaluation. This system ensures a robust PDCA process for information security management.

* COBIT: A framework to measure the maturity of IT governance, evaluated on a scale of 0 to 5. Level 5 indicates the process is "optimized." Our Group is understood to be at Level 4, "managed."

Next steps

We will continue providing support for both IT and OT security measures in order to raise awareness of the Group's Information Security Regulations; and ensure compliance in all our companies. In FY2024 the Group will introduce further unified technical measures, such as network equipment vulnerability management and detection of suspicious behavior on PCs and servers.

- Continue conducting measure evaluations by CSIRT, which include internal security audits (FY2024 plan: IT evaluation for 12 companies, OT evaluation for six companies)
- Introduce technical measures (FY2024 plan: The entire Group except for very small sites and sites with low investment ratio)
- Conduct education through global e-learning to raise employees' security awareness