Information Security Management

Material Issue
Information Security

Governance Strategy Risk management Metrics and targets

Governance

GRI: 3-3

The Fuji Oil Group has established the Sustainability Committee[*1] as an advisory body to the Board of Directors that is chaired by the President and CEO. From a multi-stakeholder perspective, the committee deliberates on and monitors Information Security Management,[*2] a priority action to address material ESG issues, and makes recommendations to the Board. The Group implements related initiatives under the oversight of the Head of Finance and Accounting Headquarters, the Chief Financial Officer (CFO) and Senior Executive Officer.
In addition, we have established an Information Officer and a Computer Security Incident Response Team (CSIRT) under the CFO. The CSIRT appoints 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.

*1Governance, Strategy, Risk Management, Metrics and Targets > Governance
https://www.fujioil.co.jp/en/sustainability/sustainability_management/#governance
*2 Governance, Strategy, Risk Management, Metrics and Targets > Metrics and targets
https://www.fujioil.co.jp/en/sustainability/sustainability_management/#index

Strategy

The Fuji Oil 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 risks may lead to failures in business continuity and damage to corporate value, such as system destruction or confidential information leaks caused by cyber-attacks. Enhancing measures against risks can be an opportunity to foster trust among stakeholders and increase corporate value.
Our Group formulated the Information Management and Information Security Regulations 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 fulfill 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

The Fuji Oil Group systematically manages risks and opportunities related to information security, an area of sustainability matters that address material ESG issues, in alignment with group significant risks.

Education

Since FY2018, we have been conducting IT security training for our Group employees to raise awareness, mainly by e-learning programs. The completion rate of e-learning programs in FY2024 was 97.2%.* We will work to develop the content of the training and encourage participation with the aim of achieving 100% completion 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 the Plan-Do-Check-Action (PDCA) cycle for correction. The frequency of these internal audits means that all companies within the Group are audited over a period of around three years. In FY2024, we updated the evaluation items covered by the audit, which ensures that we now conduct more effective internal audits and self-assessments, including OT* security measures and cloud services used by business divisions.
Results are reviewed for each company subject to internal audits. 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

FY2024 Goals	FY2024 Results	Self-assessment
Continue conducting measure evaluations by CSIRT, which include internal security audits (FY2024 plan: IT evaluation for 12 companies, OT evaluation for six companies)	IT evaluation for 14 companies and OT evaluation for seven companies	○
Introduce technical measures (FY2024 plan: The entire Group except for very small business sites and those with low investment ratios)	Introduction has been completed at all target companies, with some exceptions where certain measures have not yet been introduced	○
Conduct education through global e-learning program to raise employees' security awareness	Completed according to the plan	○

Analysis

We plan to move away from using a COBIT*1-based evaluation of IT security measures at Group companies, instead use our own indicators*2 based on frameworks including NIST CSF 2.0*3 from FY2025 onwards.
This change is intended to shift the focus of our IT security measures from strengthening overall IT governance to enhancing further practical risk response.

*1 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.”

*2 Strength of measures will be assessed and scored on a scale of 1 to 3 (where 3 is the highest level).

*3 NIST CSF 2.0: A standard framework for strengthening security measures, with actions defined under six core functions: Identify, Protect, Detect, Respond, Recover, and Govern.

Our target for FY2025 to FY2027 is that all Group companies should aim for a score of 2 for all six functions.
Blommer and Fuji Oil Co., Ltd. will aim for a score of 3 for Detect and Recover, as these two functions are particularly important for business.

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.

- Continue conducting measure evaluations by CSIRT, which include internal security audits (FY2025 plan: IT evaluation for six companies)
- Prepare new audit procedure documents for IT and OT audits, and define assessment criteria for audit items
- Conduct education through global e-learning programs to raise employees’ security awareness (Target: 100% completion rate)