Sustainability

Compliance

Basic Concept

Integrity represents the foundation of Teijin's compliance and serves as the most fundamental course of action. To ensure that our business activities are carried out with integrity, we rigorously promote the practical implementation of our Code of Conduct as the Corporate Code of Ethics, under the supervision of the Board of Directors. In addition to complying with laws and regulations, we require our corporate officers and employees to act with integrity and in accordance with social norms, based on the concept that promoting compliance is essential for creating a sound corporate culture. To that end, we ensure that the Company's representative directors and other corporate officers lead by example in this regard. At the same time, we provide compliance-related education and awareness activities to the corporate officers and employees of the Company and its subsidiaries. In these ways, we aim to increase shareholder value and enhance the level of employee satisfaction by fostering a corporate culture that respects honest behavior.

Compliance Promotion Structure

The Group Compliance Subcommittee was established and chaired by the general manager of the Compliance and Risk Management Department and is composed of managers from the compliance departments of each business unit. Confirmation on the status of compliance promotion in each department within the Group is done through this subcommittee. We also appoint Compliance Risk Management Promotion Managers in each business and at each Group company to encourage the implementation of compliance-related activities. In addition, we appoint Compliance Managers at regional headquarters to assist in promoting compliance-related activities in accordance with regional characteristics. Under these structures, we verify compliance-related issues in each department within the Group through compliance reports compiled from the hotline reporting system, relevant managerial personnel, and employee awareness surveys. To address the issues identified through these means, we incorporate compliance-related education and awareness activities within the compliance promotion plans of each Group department. By putting such a PDCA cycle into motion within our compliance promotion structure, we are able to ensure sustainable adherence to compliance, and conduct regular evaluation and improvement activities. In this manner, we are working to enhance compliance awareness throughout our organization, foster a corporate culture of adherence to laws and regulations, and minimize compliance-related risks.



Main Compliance Promotion Activities

We feel that promoting compliance is essential for creating a sound corporate culture. Given this, we are engaging in the following initiatives to not only ensure adherence to internal rules and laws relevant to our business, but also to promote a thorough awareness of corporate ethics.

Spreading Awareness about Our Code of Conduct

We distribute our corporate ethics handbook to all employees, translated into multiple languages so that all Group employees around the world can understand our Code of Conduct. In addition, we produce educational videos with subtitles in various languages and disseminate them to all Group companies.

Code of Conduct Video >

Tax Policy of the Teijin Group

In order to comply with laws and regulations regarding the tax practices of the countries, regions and multilaterals in which the Teijin Group operate, we have established a tax policy as a basic standard for taxation in April 2022. By paying taxes appropriately in accordance with this policy, we aim to perform our social responsibilities and become a corporate group that can gain the understanding and sympathy of society at large while at the same time striving to increase our corporate value.

Tax Policy of the Teijin Group

Workshops for All Employees during Corporate Ethics Month

The Teijin Group designates October as Corporate Ethics Month each year. During this period, we conduct training sessions for all Teijin Group executives and employees (including contract and temporary employees) focused on compliance issues identified within the organization.



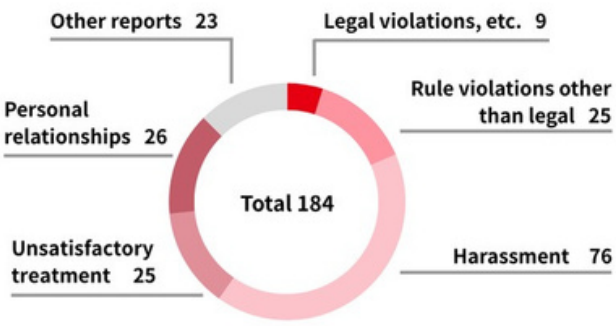
Employee Awareness Survey

We implement an employee awareness survey every year to assess the level of compliance awareness among Teijin Group corporate officers and employees in each country, and to reflect relevant feedback in future compliance promotion activities. In FY2024, the survey was distributed to 15,169 individuals, with a response rate of 72%.

Operating a Hotline Reporting System

We have established a hotline reporting system as a means for executive officers, employees, and business partners to directly report violations or suspected violations of laws and regulations within the Teijin Group. The Compliance and Risk Management Department serves as the secretariat and is responsible for handling these reports. The reporting channel is operated by an independent third party, which allows for anonymous, multilingual reporting 24 hours a day. Furthermore, unless the person who made the consultation or report provides consent, the details of the case will not be disclosed to other executive officers or employees, and any disadvantageous treatment of the whistleblower is strictly prohibited. Information related to received consultations and reports is kept confidential and managed appropriately. Regarding the use of the hotline, we inform employees of its necessity and how to use it through various training programs. The investigation process for reports is stipulated in the "Rules for the Teijin Group's Whistle-Blowing" and is shared internally. Our Code of Conduct also stipulates that we will protect whistleblowers from any attempts to identify them and from retaliatory acts such as harassment. Reports that could pose a significant risk are reported to top management for appropriate action. For reported cases where a response has been completed, the information is anonymized and, with due consideration given to privacy, published on our intranet biannually to help raise employee awareness. The internal reporting system is subject to the oversight of the Board of Directors, and regular reports on the operational status of the internal reporting system are filed with the Board of Directors on a regular basis.

Number of Reports (Including Overseas) in FY2024



Breaches in FY2024

The number of reports received through internal whistleblowing and managerial report cases in FY2024, which were found to be breaches of the code after investigation and for which appropriate measures were taken, is as follows:

Corruption, fraud, or bribery	5
Discrimination or harassment	5
Violation or leakage of customer information	0
Conflict of interest	0
Money laundering or insider trading	0
Others	7
Total	17

Initiatives to Combat Corruption

We established the Teijin Group Anti-Corruption Policy under which we lay out procedures and establish the framework for preventing corruption. In addition, we have formulated conduct guidelines for preventing corruption, which are set forth in our corporate ethics handbook, and work to ensure that our corporate officers and employees rigorously adhere to these guidelines. Additionally, we have established the "Rules on Anti-bribery of Public Officials" as internal regulations, prohibiting any entertainment or gifts to public officials with improper intent. When providing entertainment or gifts to public officials that do not constitute bribery, it is necessary to obtain prior written approval from the responsible person in accordance with the "Guidelines for Provision of Favor to Public Officials". The rules also stipulate reporting obligations, investigations, and corrective measures in response to violations, as well as disciplinary actions for breaches. Strict disciplinary actions will be taken against executives and employees involved in corruption, regardless of their position.

Teijin Group Anti-Corruption Policy

Management of Corruption Risks at Our Business Partners

We conduct due diligence to confirm the validity of transactions with sales agents, suppliers, and other parties to prevent corruption occurring through transactions with business partners. We also engage in due diligence regarding corruption risks at partner companies acquired through M&A. In particular, when starting or continuing the appointment of a sales agent, we confirm corruption risks based on a checklist (confirming presence/absence of items such as special interests with public officials, past corruption, capabilities to perform duties, and claims for unaccounted-for expenditures) and require that the sales agent sign an anti-corruption oath. We clearly communicate our CSR Procurement Guidelines, including the prohibition of bribery, to our suppliers and request their thorough adherence to these guidelines. We also enact measures toward transactions with suppliers that have contributed to corrupt behavior, including the suspension of transactions with such suppliers for a set period of time.

Risk Assessment

We are conducting assessments of each business and site of Teijin Group companies, carried out by an external law firm, to clarify the overall exposure to corruption risks across the Group. The results did not identify any business or site with significant corruption risks. For businesses that deal with public institutions including governmental organizations, however, it was recommended that development of management systems and appropriate regular trainings be conducted, preferably in accordance with Teijin Limited fundamental policies, and taking into consideration local characteristics. Going forward, we will appropriately address any corruption-related risks at each business and business site following the results of the risk assessment.

Educational Activities

We implement anti-corruption e-learning for officers and employees responsible for operations such as sales, procurement, and collaboration with other companies at each business and business site of each Teijin Group company.

Future Issues

We will implement internal audits and risk assessment surveys on a regular basis as we work to set in motion a PDCA cycle to continue to combat corruption. In addition, we are committed to the regular implementation of compliance education and training regarding anti-corruption within the Teijin Group. We will also promote the extensive use of the internal reporting system and consultation hotlines when employees face risks such as bribery. We are also taking measures such as promoting awareness of reporting systems for outside business suppliers.

Continued Operation and Strengthening of the Security Export Control System

For the Teijin Group, whose business is expanding globally, compliance with laws and a fully functioning security export control system are vitally important. In light of this, we have established the Group Security Export Control Regulations governing the corresponding Security Export Control Regulations and Detailed Implementation Rules, which apply to each Group company that conducts exports. We implement this via a dual-level control system, placing specialist back-office staff at the head office and business units to ensure a highly reliable level of security export control. The laws that must be complied with in security export control are frequently amended, so an important factor in training activities is to ensure high levels of awareness and thoroughness within the business units in regard to the latest information. In this regard, we conduct regular training and promote skills development of employees by encouraging them to sit external practical skills certification exams.

Total Risk Management

Total Risk Management

Basic Concept

The Teijin Group positions risk management, alongside compliance, as a key pillar of its internal controls, supported by a comprehensive Total Risk Management (TRM) structure that covers all of its operations. While improving shareholder value, Teijin believes its mission is to undertake business activities that satisfy shareholders and other stakeholders. In achieving this mission, we must address all risks (uncertainties) that pose a threat to its realization. Accordingly, we have adopted an organizational and systematic approach to comprehensively and efficiently identify, assess, and manage the risks affecting the entire Group, and to integrate these insights into Group management. The Board of Directors oversees risk management throughout the entire Teijin Group, recognizing the assessment of both "strategic risks," which originate from the formulation of management strategies and plans, strategic actions, and decisions on individual investment projects, and "operational risks," which involve various adverse events that could negatively impact the Company. These are viewed as critical factors in decision-making. In addition, we require our group companies and their executive officers to fully understand this approach and to address any risks that could threaten our business activities.

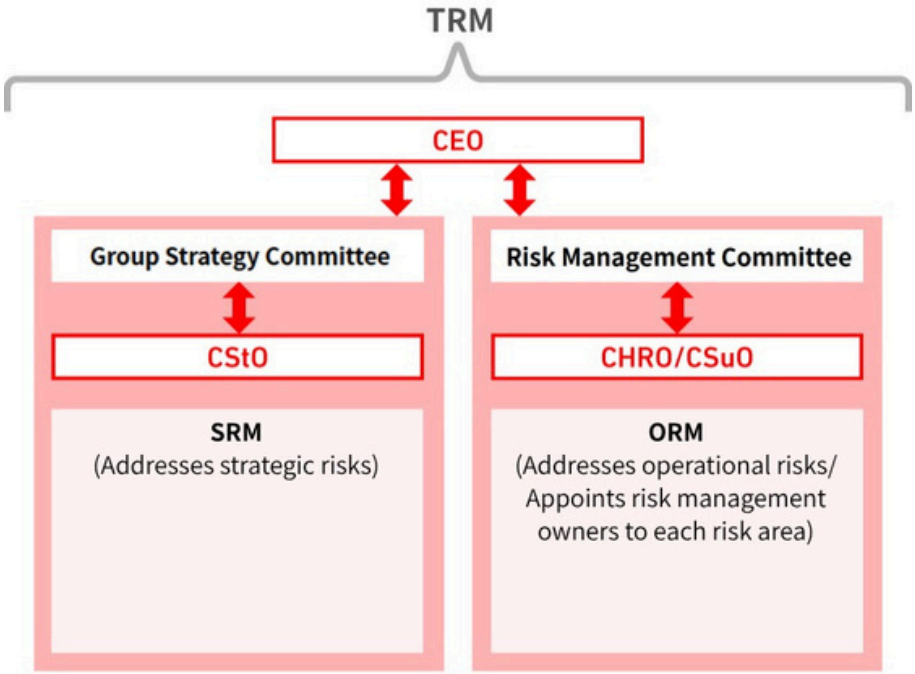
Risk Management Structure

Strategic risk management (SRM)

The Group Strategy Committee, chaired by the CEO and tasked with deliberating key business execu tion issues, promotes SRM initiatives. Specific risks that are currently under review include the potential impact of trade policies resulting from the transition of the U.S. presidency, regulations on carbon fiber in Europe, trends in PFAS regulations, and other case-specific analyses and discussions. The Group also considers various risks such as hostile takeovers, the impact of individual business divestments across the Group as a whole, structural changes in the industry driven by advances in technologies such as AI, and shifts in the global economic framework caused by the fluidity of the international situation and order, thereby responding appropriately to the relevant strategic risks.

Operational risk management (ORM)

The Risk Management Committee, which operates under the CEO, is responsible for ORM, with over sight assigned to the Chief Sustainability Officer. This committee sets policies for managing operational risks and promotes and monitors progress on related initia tives. The CEO chairs the committee, and its members include the Chief Sustainability Officer and others appointed by the CEO.



FY2025 TRM Basic Plan for Operational Risks

In FY2025, following deliberations by the Board of Directors, the Company has established a policy for managing operational risks.

- The Risk Management Committee addresses operational risks that could significantly impact management if they were to materialize.
- For the countermeasures against each risk, we clarify the Risk Management Owner (the responsible executive officer) and the organizations and committees that support them, and work toward highly effective implementation.
- Among the significant risks facing the Group, those deemed most critical are classified as "Major Risk A" and prioritized for countermeasures.

Based on the above policy, the Group identified nine key risk areas in FY2025: major natural disasters, information, geopolitics (economic security), quality, compliance, management (human resources), safety, environment, and society. For each area, we evaluated risks based on (1) impact, (2) probability of occurrence, and (3) expected timing of occurrence. The most significant key risks listed in the table on the next page were identified, and a Risk Management Owner (responsible executive officer) was appointed for each, with clearly defined responsibilities and scope. To further improve the effectiveness of risk management, the Group designated a subset of these key risks as "Major Risk A," indicating the highest-priority risks that require intensive management focus.

Operational Risks: Key Risks and Basic Response Policies

Risk area	Key risks	Risk description	FY2025 Response Policy	Impact	Probability	Time frame	Evaluation*
Major natural disasters	Tokyo Inland Earthquake	A Southern Central Tokyo Earthquake may cause the largest-scale damage in the Tokyo metropolitan area.	Review and implement training according to the BCP for core management functions.	Large	Medium	Short- to long-term	A
	Nankai Trough Earthquake	A magnitude 9 earthquake may cause damage to factories in the Chugoku-Shikoku and Kansai regions.	Update assumptions regarding potential damage to Teijin Group facilities and review BCP measures at each site.	Large	Low	Short- to long-term	B

Risk area	Key risks	Risk description	FY2025 Response Policy	Impact	Probability	Time frame	Evaluation*
	Eruption of Mt. Fuji	Mishima Factory may be completely destroyed by lava flow.	Examine BCP measures in the potential event of a complete destruction of the Mishima Factory.	Large	Low	Medium- to long-term	C
Information	Information security	Disclosure of critical information due to cyberattacks and suspension of operations during system downtime.	Assess and improve support for security levels across the Group.	Large	High	Short-term	A
	DX/AI	Shortage of DX talent within the Group is leading to a decline in overall competitiveness.	Develop training programs for IT personnel and continue implementing Group-wide DX talent development programs.	Medium	Medium	Medium-term	C
Geopolitics (economic security)	Supply chain disruption	Disruption in the supply chain is leading to the suspension of the raw material supplies.	Collaborate with businesses to secure multiple suppliers and put countermeasures in place.	Large	High	Short-term	A
	Technical information Leakage	Targeted attacks that exploit vulnerable areas in management may lead to the disclosure of critical technical information.	Assess the current management status and examine the implementation of stronger controls at factories.	Medium	High	Short-term	B
	Sharp currency fluctuations/rising energy costs	Rising energy costs may be caused by military conflicts, economic disputes, and other factors.	Pursue ongoing responses through business profit-and-loss management.	Medium	Medium	Short- to medium-term	C
Quality	Major quality fraud/ falsification	Noncompliance with laws and regulations during manufacturing or inspection processes.	Conduct corporate quality compliance audits and corrective measures.	Medium	High	Short-term	B
Compliance	Serious misconduct	Delayed initial response may lead to intense media coverage and damage to reputation.	Develop a rapid response framework in the event of an incident.	Medium	High	Short-term	B
Management (human resources)	Talent outflow/ recruitment	Weakened management foundation caused by the ongoing	Promote workplace improvements (job-based roles and career autonomy	Medium	Medium	Medium- to long-term	C

Risk area	Key risks	Risk description	FY2025 Response Policy	Impact	Probability	Time frame	Evaluation*
		outflow of talent or challenges in recruitment.	support) while regularly monitoring turnover rates at key Group companies.				
Safety	Fire/explosion	Long-term suspension of manufacturing and supply caused by fires or explosions at factories, leading to loss of customers or potential lawsuits.	Verify and diagnose site-specific measures to prevent major disasters, such as leaks or fires, and review disaster prevention management.	Medium	Medium	Short-term	C
Environment	Climate change (transition risk)	Delays in responding to environmental regulations, information disclosure obligations, or customer demands for CO2 reduction could lead to customer loss and investor defection.	Pursue ongoing monitoring of global regulatory trends and respond promptly.	Small	Medium	Medium- to long-term	C
Society	Supply chains/ human rights	Inadequate response to regulatory tightening or discovery of human rights violations could lead to reputational damage, customer loss, litigation, and talent attrition.	Address and monitor issues in high-risk businesses based on external risk assessments (surveys).	Medium	Low	Medium-term	C

*Evaluation: A = Major risk A, B = Major risk B, C = Other risk

Information Security and Personal Information Protection

Information Security and Personal Information Protection

The Teijin Group strives to maintain and improve information security in recognition of the risk of an information security incident undermining our competitiveness or hindering business continuity, as well as the risk of incurring fines for legal violations. We have established the Teijin Group Regulations for Information as our basic policy on information security. In these regulations, we address information security risks, such as the leakage or falsification of confidential information, and work to avoid and mitigate them from the perspectives of physical, technical, and human threats and vulnerabilities. The Teijin Group has also established the Teijin Group Regulations for Personal Information Protection as its basic policy on the protection of personal information, and we are responding appropriately to personal information protection laws, for which legislation is advancing globally.

Privacy Policy >

Main Initiatives

The Teijin Group is promoting the building of an information security governance structure and process.

Information security governance structure

The Teijin Group has appointed a Chief Digital Officer, who is a corporate officer, as the person responsible for planning, executing, promoting, and overseeing policies related to global IT governance (human resources, structure, rules, operations, information security, investment, and costs). We have also established an information management structure within the Group by defining the roles and responsibilities of the general manager of the information systems department, the IT officer appointed for each organization (department, company, business, etc.), and each employee. Additionally, under the Chief Digital Officer's supervision, we have established an Information Security Committee with the general manager of the information systems department as chairperson and the division general manager of each business's IT division and each indirect division general manager as members. This committee promotes cross-group initiatives related to information security and educational activities. As a response to information security incidents, we have established a specialized security organization (CSIRT: Computer Security Incident Response Team) that works on preventive activities and ensures a swift response when an incident occurs. This organization monitors our information systems and data for attacks and suspicious activity around the clock, while also working on the continuous improvement of all CSIRT activities, including improvements to our information security systems. We have been a member of the Nippon CSIRT Association (NCA) since 2016, through which we gather and utilize the latest information on cyberattacks and know-how from other companies on a daily basis. Furthermore, in preparation for incidents such as ransomware attacks, we strive to ensure the integrity and protection of data through measures including data encryption, backups, and log monitoring.

Information security management processes

Through our information management structure, the Teijin Group periodically checks the management status of information assets such as information systems, networks, facilities, personal information, and confidential information within each organization. We strive to maintain and improve information security by classifying the importance of these assets, identifying threats, assessing risks, and then implementing

appropriate countermeasures. Additionally, the corporate audit department conducts information security audits for all Group companies from an independent standpoint.

Escalation process for information security incidents

The Group Risk Management Regulations of the Teijin Group stipulate the reporting and handling procedures for incidents and accidents. We also have a system in place to receive reports from those who discover suspicious emails or security incidents 24 hours a day, 365 days a year.

Information security education

With the goal of enabling every employee to properly utilize information assets while responding to growing security risks, the Teijin Group works to ensure that each individual acquires the essential awareness and knowledge needed to protect the Group's information assets. To this end, we regularly provide information security education through e-learning and group work by organizational unit, along with hands-on response training using simulated targeted-attack emails for all executive officers and employees.

Appropriate response to personal information protection

We work to ensure compliance with laws and regulations in each country and region, and to thoroughly implement related measures through a system that assigns a "person responsible for protection of personal information".