

RISK MANAGEMENT/COMPLIANCE

The OKI Group is working to reinforce risk management under the Risk Management Committee. The Compliance Committee plays a central role in promoting compliance initiatives, and we have established consultation and reporting contacts as one of the self-mechanisms for early discovery and rectification of internal compliance problems.

Risk Management Initiatives

The OKI Group has established the Risk Management Committee, chaired by the President, to ensure that risks related to corporate activities are grasped and managed properly. The Committee deliberates and decides on basic policies for risk management and identifies risks to be managed based on such policies and the division responsible for said risks. It also deliberates and decides on policies for preventing the materialization of risk and policies to address crisis scenarios.

Risks inherent in each company and division are defined and classified into three categories: risks that should be considered at the management level (management risks); risks that should be recognized and identified in relation to business activities (business risks); and risks that are common to each company and division and should be managed across the Group (common risks). Of these risks, the risks to be managed are chosen. The responsible control division deploys preventive measures for common risks within the Group, while the Compliance Committee (see next section) regularly checks the implementation status. In this way, we are putting in place a sound risk management cycle. Since fiscal year 2020, OKI has identified the business risks for each of its business groups in order to strengthen the management of these risks, and the same was done at major subsidiaries in fiscal year 2021. OKI is making progress in creating the management cycle and developing its framework.

To swiftly identify and resolve problems, we also established the OKI Group Risk Incidents Reporting System, which ensures that potential risk events, crises, and situations that may lead to such events are promptly reported to the Risk Management Committee.

Related information: Website "Business and Other Risks"
<https://www.oki.com/en/ir/corporate/risk.html>

Initiatives to Promote Compliance

The OKI Group has established the Compliance Committee (with the Chief Compliance Officer as Committee Chairman) in accordance with the top management's Compliance Commitment thereby striving to ensure rigorous compliance. The Committee regularly monitors the management progress of the common risks identified by the Risk Management Committee. The Committee also deliberates and decides on compliance training plans and oversees their implementation. Moreover, we implement fixed-point observations on conduct and awareness relating to compliance of executives and employees, and to make the most of such measures, we implement compliance awareness surveys on an ongoing basis.

In order to discover and rectify improper activities at an

early stage, we have established a whistle-blowing system (in-house contact point, Group-wide contact point, and external contact point) to enable anonymous reports, as well as reports to outside directors and Audit & Supervisory Board members at every Group company, and stipulated whistle-blowing regulations such as those about the protection of whistle-blowers. We have also developed internal regulations in line with the revision and enforcement of the amended Whistleblower Protection Act in June 2022, and provided internal training on re-ensuring the confidentiality of whistle-blowers. In fiscal year 2021, 23 reports and consultations were received at the OKI Group in Japan.

Ongoing Compliance Training

The OKI Group has appointed compliance managers and promoters (around 310 in total) who play a key role promoting compliance in the workplace at each company and division in Japan. We also hold regular training sessions for these compliance managers and promoters. We are holding ongoing anti-monopoly law training centered on the marketing & sales section. In fiscal year 2021, the group training was held via video conference in order to prevent the spread of COVID-19.

We provide e-learning to all Group employees in Japan on topics related to shared risks, such as personal information protection, information security, and common risks. We also have tools in place to ensure that the content of the training is widely disseminated. These include regular reports of case studies on compliance issued via our intranet and internal newsletters.

In addition, in fiscal year 2018, we started a unified e-learning compliance training program for employees of overseas Group companies, and training was provided to approximately 1,100 employees in fiscal year 2021.

Main Compliance Training Programs (for the OKI Group in Japan) in FY2021

Training Overview	Subject Employees	Attendance Rate
Compliance manager training October to November 2021 (video) Theme: Risk management, learning from risk cases; Introduction to internal auditing	Domestic Group managers/promoters	100% (approx. 310 persons)
Anti-monopoly Act training December 2021 to March 2022 (video)	Domestic Group employees of related divisions (sales, etc.)	100% (approx. 2,200 persons)
Personal information protection and information security e-learning (regular and start anytime sessions) Regular session (simultaneous training) August to September 2021	All domestic Group employees	Simultaneous training: 99.9%
Workplace compliance e-learning (regular and start anytime sessions) Regular session (simultaneous training) December 2021 to January 2022	All domestic Group employees	Simultaneous training: 99.9%

Approaches to Anti-Corruption

Anti-corruption is a global issue included in the Ten Principles of the United Nations Global Compact. The OKI Group is promoting initiatives to prevent corruption based on the "OKI Group Anti-Corruption and Anti-Bribery Policy."

The "OKI Group Anti-Corruption and Anti-Bribery Policy" complies with anti-corruption laws and regulations that apply in each country and region where the OKI Group operates, such as the Japanese Unfair Competition Prevention Act, the US Foreign Corrupt Practices Act, and the UK Bribery Act. The policy defines the basic requirements for complying with laws and regulations and conducting business appropriately. Furthermore, we established specific administration rules for recording the exchange of the gifts and receiving/offering entertainment, and each OKI Group company monitors compliance with these rules annually.

In fiscal year 2021, there were no issues related to bribery or corruption in the OKI Group.

Emergency and Disaster Response

The OKI Group has established Safety Countermeasure

Committees at its domestic and overseas sites, as well as at subsidiaries, in order to ensure "protect people's lives," "prevent secondary accidents," "contribute to local communities and foster good relationships with them," and "continuity of business operations" in the event of disasters. Among them, OKI established and conducts regular reviews of the Business Continuity Management (BCM) / Business Continuity Plan (BCP) based on the BCM Development Guidelines in each division for the "continuity of business operations."

In fiscal year 2021, the COVID-19 Task Force that was established in January 2020 continued to conduct initiatives to prevent the spread of the virus and maintain business continuity, such as transmitting information about the status of the virus in Japan as well as identifying and handling those infected inside the Group. In the wake of the outbreak of the Russia-Ukraine issue in February 2022, response headquarters were established in the relevant business divisions and continue to deal with the situation in coordination with the sites.

OKI is also striving to respond more quickly and appropriately by continuously reviewing initial countermeasures for natural disasters, such as earthquakes, typhoons, and floods.

INFORMATION SECURITY

Based on the OKI Group Information Security Basic Policy, the OKI Group has established a system to ensure information security to properly manage and protect company and customer information.

Policy on Information Security Initiatives

The OKI Group is building a robust IT infrastructure to support its business growth. As part of this effort, we are working to strengthen information security from the perspective of minimizing management risks. As our Risk Management Committee has defined "electronic information leakage" and "cyber attack" as common risks, we have made it clear that measures for information security are an important part of management and we are proceeding with them.

In accordance with the Information Security Basic Policy, we are promoting a wide range of "visibility, support, and protection." In addition, we established OKI-CSIRT* as a specialized security incident response organization tasked with strengthening our ability to prevent and respond to incidents.

*CSIRT: Computer Security Incident Response Team

Strengthening Information Security Measures

The OKI Group constantly monitors global trends and promotes information security measures in Japan and overseas. We also establish information security guidelines in each country and region, appoint security managers at each site, and introduce various risk management tools. In addition, we are working to expand the scope of our information security management system (ISMS).

Unauthorized Access to File Server

In November 2021, OKI confirmed that a third party gained unauthorized access to our file server in Japan via an overseas subsidiary. The OKI Group takes this incident seriously and has taken measures to strengthen our security measures, including the introduction of suspicious behavior detection mechanisms and the establishment of a monitoring system for all Group computers and servers. To prevent a recurrence, we will adopt more advanced security measures, such as enhanced authentication infrastructure and domestic and overseas security controls.

Enhancing Protection of Personal Information

We in the OKI Group have enhanced protection of personal information, based on the Privacy Policy. We have committed to the protection of personal information under the leadership of our Chief Privacy Officer. Privacy managers have been appointed in all divisions and subsidiaries. OKI is taking measures based on regulations for the personal information protection laws in the EU as well as other overseas regions and countries. The website of each Group company has a cookie banner that complies with applicable regional and national privacy protection legislation and cookie regulations.

As of June 2022, seven companies of the OKI Group have received PrivacyMark certification in Japan.