RISK MANAGEMENT/COMPLIANCE

Basic Approach

The OKI Group has set forth "embedding risk management and reinforcing compliance awareness" as a key component of our materiality issues "strengthening management foundation to support sustainable growth". We have positioned fiscal year 2023 as the period for promoting awareness-raising and embedding required operations, and we will continue developing and implementing risk management structures and systems while also promoting training that is effective for further awareness-raising for risk management and compliance.

Risk Management and Compliance Promotion Initiatives

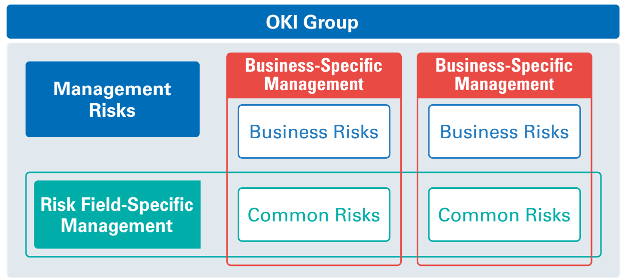
Risk Management Initiatives

The OKI Group has established the Risk Management Committee, which is chaired by the President and includes inside and outside Audit & Supervisory Board members as advisors, 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 responsible divisions. It also deliberates and decides on policies for preventing the materialization of risks and policies to address crisis scenarios.

Risks inherent in each division and subsidiary is categorized to stipulate risk fields, and then the division in charge of each risk field provides relevant risk-management support, guidance, and advice to each division and subsidiary throughout the Group. In addition, we strive to implement business-specific risk management based on an awareness and understanding of risks related to each business.

Through the above management, risks inherent in the OKI Group are defined as falling into three categories: risks that should be managed at the management level (management risks), risks that should be managed and identified in relation to business activity (business risks), and risk fields that are common to divisions and subsidiaries and should be managed across the Group in particular (common risks). We develop materialization prevention measures to be implemented within the Group, and, 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.

Overview of the OKI Group's Risk Management


OKI Group
Management Risks
Business-Specific Management
Business-Specific Management
Business Risks
Business Risks
Risk Field-Specific Management
Common Risks
Common Risks

*Management risks include business risks and common risks that have a large effect on our management.

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, which is chaired by the Chief Compliance Officer, in accordance with the top management's "Compliance Commitment," thereby striving to ensure rigorous compliance. The Committee confirms the single-year plan covering the risks identified as those to be managed by the Risk Management Committee and also regularly monitors the associated progress. In addition, the Committee also deliberates and decides on compliance training plans and oversees their implementation. Moreover, to implement fixed-point observations on the conduct and awareness of executives and employees, we implement annual compliance awareness surveys, and apply the results of these surveys to various measures.

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 we have stipulated whistle-blowing regulations such as those related to the protection of whistle-blowers. We also provide ongoing training related to the purpose of the system as well as whistle-blower confidentiality, and we have established contact points at overseas subsidiaries in line with local laws. In fiscal year 2022, 42 reports and consultations were received at the OKI Group in Japan.

Ongoing Compliance Training

The OKI Group prepares and implements compliance training plans while also taking advantage of various opportunities to communicate information aimed at fostering and raising awareness.

In Japan, the OKI Group holds regular training sessions for compliance managers and promoters (around 330 in total) at our each division and subsidiary is provides training specific to various job positions, and provides common risk-related e-learning to all Group employees. We also have tools in place to foster and raise awareness, including regular reporting of compliance case studies via our intranet and internal newsletters as well as communicating information on the OKI Group Code of Conduct.

We also provide a unified e-learning compliance training program for employees of overseas Group companies, and training was provided to approximately 1,000 employees in fiscal year 2022.

Main Compliance Training Programs (for the OKI Group in Japan) in FY2022

Training Overview	Subject Employees	Attendance Rate
Compliance manager training October to November 2022 (video) Theme: Risk management, the whistle-blowing system, and the prevention of quality fraud	Domestic Group managers/ promoters	100% (approx. 330 persons)
Anti-Monopoly Act training December 2022 to March 2023 (video)	Domestic Group employees of related divisions	95.8% (approx. 1,800 persons)
Personal information protection and information security e-learning (regular and start anytime sessions) Regular session (simultaneous training) August to September 2022	All domestic Group employees	Simultaneous training: 99.7%
Workplace compliance e-learning (regular and start anytime sessions) Regular session (simultaneous training) December 2022 to January 2023	All domestic Group employees	Simultaneous training: 99.9%

Ensuring Fair Business Transactions

Approaches to Anti-Corruption

The OKI Group is promoting initiatives to prevent corruption based on the "OKI Group Anti-Corruption and Anti-Bribery Policy," which stipulates basic items necessary to comply with the anti-corruption laws and regulations of each country and region in order to conduct business properly. We have established administration rules for recording the exchange of gifts and receiving/offering entertainment, etc., and we annually confirm the compliance situation of each OKI Group company.

Ensuring Thorough Compliance with the Anti-Monopoly Act

In February 2017, OKI received a cease and desist order and surcharge order from the Japan Fair Trade Commission in line with Japan's Anti-Monopoly Act as a result of business related to digital wireless communication systems for firefighting and emergency use. To ensure that nothing like this ever happens again, we are implementing comprehensive recurrence prevention measures, including introducing and implementing systems for recording our contact with competing companies as well as Anti-Monopoly Act training centered on our marketing & sales section. In fiscal year 2022—the fifth year since we received the above orders—we implemented training covering an expanded range of trainees based on the theme of gaining an understanding of the details of our violation and our subsequent response while also taking another look at and reviewing our behavior.

In fiscal year 2022, the OKI Group did not have any problems related to competition laws, including bribery and corruption. We will continue increasing the effectiveness of our related systems as we strive to raise awareness of compliance, such as by communicating messages of our top management.

Emergency and Disaster Response

The OKI Group has established Safety Countermeasure Committees at its sites and subsidiaries in order to "protect people's lives," "prevent secondary accidents," "contribute to local communities and foster good relationships with them," and to ensure the "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 to ensure the "continuity of business operations" in the case of not only disasters but other situations as well. In addition, we are supporting independent social contribution activities by employees, including the development of a paid leave system that can be applied to participation in volunteer activities, such as disaster recovery support.

In March of 2023, OKI obtained "Resilience Certification for contribution to national resilience" certification as a company that complies with the requirements of certification for organizations that contribute to national resilience.

INFORMATION SECURITY

Basic Approach

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

As the OKI Group is building a robust IT infrastructure to support its business growth, we are working to strengthen information security from the perspective of minimizing management risks. In addition, we have defined "electronic information leakage" and "cyber attacks" as Group-wide common risks, and, in accordance with the Information Security Basic Policy, we are promoting a wide range of "visibility, support, and protection" measures. 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, establishes information security guidelines in each country and region, appoints security managers at each site, and introduces various risk management tools. In addition, we are working to expand the scope of our information security management system (ISMS). In fiscal year 2022, we made the enhancements below in response to unauthorized file server access during the previous fiscal year.

- Introducing EDR (Endpoint Detection and Response) for all Group PCs and servers, and expanding 24/7 monitoring by external organizations to include the United States and Asia
- Introducing WAFs (Web Application Firewalls) for OKI's websites as a countermeasure against DDoS attacks (distributed denial-of-service attacks)
- Conducting penetration tests* for the Group's remote access environments

*A way to test a system for vulnerabilities by attempting an actual cyber attack

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 related to personal information protection in Europe, Asia, and other overseas business regions. 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 2023, seven companies of the OKI Group have received PrivacyMark certification in Japan.