RISK MANAGEMENT/COMPLIANCE

The OKI Group is working to reinforce risk management under the Risk Management Committee. In accordance with our “Compliance Commitment” and, in order to perform corporate activities fairly, we are focusing on the enhancement of training, and we have established consultation and reporting contacts.

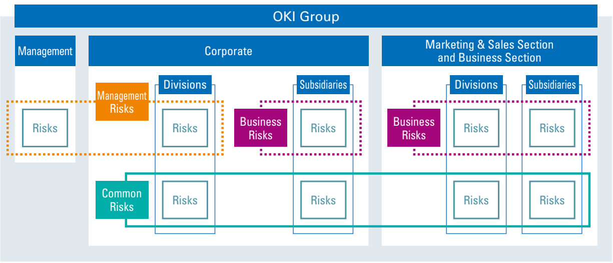
Risk Management Initiatives

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

Risks to be managed are defined and classified into three categories: “management risks” that should be considered at the management level, “business risks” that should be recognized and identified by each division, and “common risks” that are common to each company and division and should be managed cross-laterally. Of these risks, common risks are registered by the control division and preventive measures are deployed within the Group, while the Compliance Committee (see next section) regularly checks the implementation status. In these ways, we are putting in place a sound risk management cycle.

To identify and resolve problems swiftly, we also established the OKI Group Crisis Communication System, which ensures that potential risk events and crises are promptly reported to the Risk Management Committee Secretariat.

Risks to Be Managed



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 consultation and reporting channels (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. In fiscal year 2019, 42 reports and consultations were received at the OKI Group in Japan.

Ongoing Compliance Training

The OKI Group has appointed compliance managers and promoters (around 360 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. In 2017, the Japan Fair Trade Commission issued OKI with a cease-and-desist order and surcharge payment order in accordance with the Anti-Monopoly Act. To ensure this never happens again, we have continued to conduct antitrust-related training, centering on our marketing and sales section.

We provide e-learning to all Group employees in Japan on topics related to 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 fiscal year 2018, we started a unified e-learning compliance training program for some overseas Group companies, and we added subsidiaries in China and India to the program in fiscal year 2019.

Main Compliance Training Programs (for the OKI Group in Japan) in FY2019

Training Overview	Target	Attendance Rate, Number of Participants, etc.
Compliance manager training (group training) July–August 2019 Theme: Risk management to ensure appropriate labor management and quality fraud prevention	Domestic Group managers/ promoters	99.7%
Anti-monopoly Act training (group training) November–December 2019	Domestic Group employees of related divisions	Approx. 1,000 people
Personal information protection and information security (e-learning) August–September 2019	All domestic Group employees	100%
Workplace compliance (e-learning) December 2019–January 2020 Theme: 10 case studies focusing on common risks	All domestic Group employees	99.9%

Approaches to Anti-Corruption

The OKI Group is promoting initiatives to prevent corruption, which is a global issue, based on the "OKI Group Anti-Corruption and Anti-Bribery Policy" that we established in fiscal year 2013.

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. As company bylaws, we established specific rules for recording the exchange of the gifts and receiving/offering entertainment, and compliance with these rules at each Group company is monitored annually by OKI's control division.

In fiscal year 2019, 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. For "continuity of business operations," each business and corporate (headquarter) division develops Business Continuity Management (BCM) and a Business Continuity Plan (BCP), based on BCM Development Guidelines.

In January 2020, we set up a task force to address the COVID-19 pandemic that struck in December 2019. We have since established basic policies (see page 10) and are continuing efforts to prevent the spread of the virus and ensure business continuity.

INFORMATION SECURITY

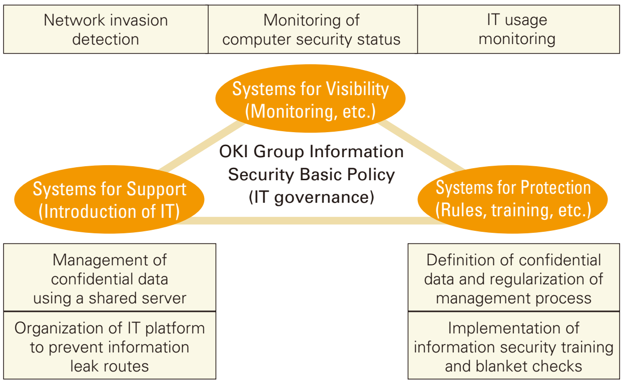
Based on the OKI Group Security Basic Policy, the OKI Group has established a system to ensure information security and works to properly manage and protect company and customer information.

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.

We are also promoting a wide range of measures based on the three mechanisms shown in the figure below. 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


Network invasion detection
Monitoring of computer security status
IT usage monitoring
Systems for Visibility (Monitoring, etc.)
OKI Group Information Security Basic Policy (IT governance)
Systems for Support (Introduction of IT)
Systems for Protection (Rules, training, etc.)
Management of confidential data using a shared server
Organization of IT platform to prevent information leak routes
Definition of confidential data and regularization of management process
Implementation of information security training and blanket checks

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 fiscal year 2019, we strengthened our information security system by acquiring ISMS certification for 15 new divisions in Japan. Overseas, in order to further strengthen IT governance, we are developing communication systems and rules, deploying countermeasure tools, and improving the monitoring environment.

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. The Group's response to the EU General Data Protection Regulation (GDPR) was compiled as a policy document, and measures have been taken based on this.

OKI and seven Group companies have acquired PrivacyMark certification in Japan as of June 2020.