RISK MANAGEMENT/COMPLIANCE

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

Advancement of Risk Management

OKI is working to reinforce risk management under the Risk Management Committee (with the president as Committee Chairman, and outside directors and Audit & Supervisory Board members as advisors). The committee deliberates and decides basic policies relating to managing risk that accompany the Group's business activities. The committee receives reports on risk information that accompany business activities from executive officers and divisions and promotes measures to prevent manifestation of risks.

The compliance risks (risks associated with violation of laws, regulations and in-house rules) requiring common management across the Group are managed by the Compliance Committee (the chair is a chief compliance officer), which oversees the Control Division that registers risks and implements preventive measures within the Group, thereby building and operating the management cycle that carries out regular verification of implementation status. Moreover, in order to discover and rectify improper activities at an early stage, we have established consultation and reporting channels 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 2017, we further enhanced this system with the establishment of new external and common contacts for the OKI Group.

Emergency/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 a Business Continuity Plan (BCP), based on BCP Development Guidelines. The contents of each BCP are reviewed annually to improve its effectiveness. In fiscal year 2017, we worked on strengthening collaboration between relevant departments from the time an earthquake hits through to BCP activation.

Enhancement of Compliance Training

The OKI Group implements training sessions for compliance managers at six sites in Japan for employees at the senior manager level as regular training. Participants learn in these sessions, and roll out the gained knowledge in their business units. The deployment of such knowledge is checked through an e-learning program for all executive officers and employees of the Group. We have tools in place to promote learning and retention of program content such as sharing specific examples through the booklet called "Case Examples of Compliance" on the Internet.

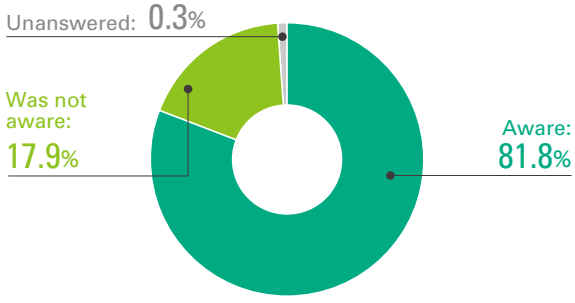
Participation Rates in Compliance Training Programs (for the OKI Group in Japan) in Fiscal 2017

Training overview	Participation rate
Training sessions for compliance managers (implemented in July-August 2017) Main themes: Anti-Monopoly Act, measures against anti-social forces, internal whistle-blowing system	100%
The e-learning program (about on-the-job compliance) (implemented in December 2017 to January 2018)	100%
e-learning courses on "Anti-Monopoly Act" (implemented in February-March 2018)	98.6%

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.

Compliance Awareness Survey Results (implemented in February 2018)

Were you aware that external and common contacts for the OKI Group have been established as part of the internal whistle-blowing system?



Approaches to Anti-Corruption

Anti-corruption is principle 10 raised in the United Nations Global Compact, and is a global social issue. We are promoting anti-corruption initiatives based on the "OKI Group Anti-Corruption and Anti-Bribery Policy" that we put into practice in fiscal year 2013.

The "OKI Group Anti-Corruption and Anti-Bribery Policy" sets out fundamental points for carrying out operations properly while complying with the anti-corruption-related regulations applicable to each country and region in which the OKI Group operates. As company bylaws, we established specific rules for recording the exchange of gifts and receiving/offering entertainment, and compliance with these rules at each Group company is monitored annually by OKI's Control Division.

Initiatives for Thorough Compliance with Anti-Monopoly Act

In February 2017, the Japan Fair Trade Commission issued a cease and desist order in accordance with the Anti-Monopoly Act and ordered OKI to pay fines with regard to trade related to digital wireless communication systems for firefighting and emergency use. We are working on prevention measures to ensure this never happens again.

In fiscal year 2017, we reviewed our regulations on complying with the Anti-Monopoly Act and implemented a system for recording contact with our competitors. Moreover, in light of this incident, starting with Anti-Monopoly Act training implemented in April at the same time as fiscal year policy briefing sessions, we are endeavoring to make employees fully aware of our compliance rules by focusing repeatedly on the Anti-Monopoly Act in training sessions for compliance managers, e-learning programs and other occasions.

In addition to continually monitoring the implementation of Anti-Monopoly Act-related rules and improving the effectiveness of our framework, we will strive to generate a sense of compliance awareness by continuing to send out compliance messages from top management.

ESG SUPPORTS CORPORATE VALUE

INFORMATION SECURITY

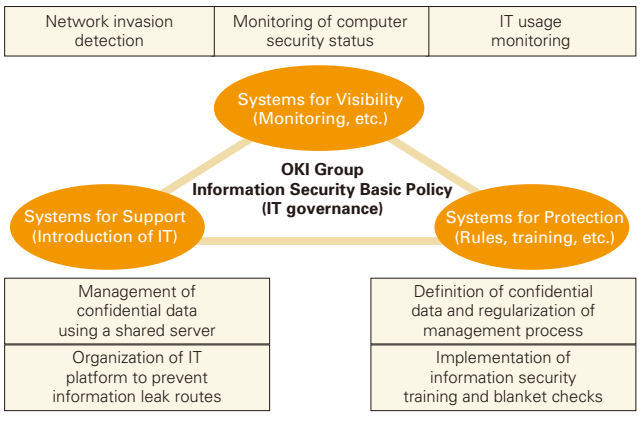
Based on the OKI Group Security Basic Policy, the OKI Group has established a system to ensure information security and works to properly manage and protect company and customer information.

Three Systems of Information Security

In the OKI Group, we use the three systems shown in the diagram below to broadly promote information security measures for computers, networks and information systems. We have established an organization specializing in security incident response called OKI-CSIRT*, which collaborates with external organizations, in order to enhance our preventive measures against threats to computer security in the Group and improve our capacity to respond to them.

To further enhance the effectiveness of our responses when an incident occurs, in fiscal year 2017 we conducted drills that simulated cyber attacks and information leaks so we could check how our company-wide emergency communication system fared.

*CSIRT: Computer Security Incident Response Team



Enhanced Actions at Overseas Sites

The OKI Group has promoted information security measures at overseas sites, including such actions as laying down information security guidelines in each country and region, appointing security managers at each site, and adopting control tools.

In fiscal year 2017, we stepped up the targeted e-mail attack drills that we had so far implemented in Japan to include all e-mail users at our sites in Europe, the US, China, and Asia.

Enhancing Protection of Personal Information

We in the OKI Group have enhanced the 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 in Group companies. In addition to revising its related rules in fiscal year 2017 in response to the amended Act on the Protection of Personal Information, OKI examined how it should respond to the EU General Data Protection Regulation (GDPR) and accordingly formulated a policy in May 2018.

OKI and seven Group companies have acquired PrivacyMark certification in Japan as of June 2018.