

Fiscal 2010 Activities Review and Plan for Fiscal 2011

We ensure safety and trust, promoting business activities in the information age and contributing to the realization of a secure society.

1. Maintaining Unified ISMS Certification for the Group <Ricoh Group/Global>

We passed the second renewal audit for unified ISMS certification for the Group, and renewed our ISMS certification. Ricoh Austria GmbH underwent the audit for the first time and was added to the unified certification. (In total, 85 companies worldwide are certified: 41 in Japan and 44 overseas)

By passing the renewal audit, which required us to make continual improvements, we have been able to confirm that the information security management system we have built to date is continually reviewed with respect to targets, and that management for solving issues is operating properly.



Plan for Fiscal 2011

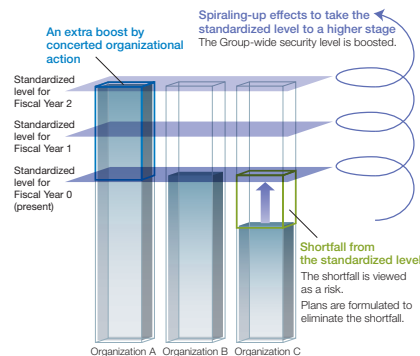
After the renewal audit for unified ISMS certification for the Group, we will conduct the first continuing audit to maintain our certification.

2. Continual Improvement and Deployment of Ricoh Family Group Information Security Measures <Ricoh Group/Global>

In light of changes to the business environment, such as the spread of new IT devices, we have added “Tablet Devices” and “Thin Client Services” as control items and revised our Information Security Measures to issue the fiscal 2011 edition.

We have strived to expand and establish the Information Security Measures. These efforts have included risk assessments conducted by information asset owners based on the Measures and confirmation of the implementation status of the Measures during internal audits.

In doing so, we have standardized information security measures which had been handled independently by each organization and eliminated inconsistencies in the status and content of actions taken. As a result, the security level of the entire Group has been improved through the spiraling-up effects and we have become able to maintain security at stable levels.



Plan for Fiscal 2011

The Information Security Measures have achieved a higher level of completion, but we will continue to review and deploy them to respond to changes in the business environment.

In addition, to promote even more effective information security activities, we will work to achieve innovation and improvement in the methods for implementing and operating IT technology and improve the efficiency of our risk assessment processes.

3. Enhancing the Ricoh Group's Business Continuity Plan and Management <Ricoh Group/Japan>

In our BCM we include maintenance services and supplies of consumables because they are essential to enable the ongoing utilization of equipment installed on customer premises by the imaging solutions business.

We have built our BCM assuming the risk of a disastrous earthquake in the Tokyo metropolitan area, where many of the Ricoh Group's business sites are located, as well as the risk of a Tokai earthquake, which would affect the Numazu-Gotemba district where the production sites for some of our consumables are concentrated. We have also built our BMC assuming the risk of an epidemic of a virulent new strain of influenza, where improper preparatory measures or errors in initial response would have a profound effect on business management, including shutdowns and business interruptions for extended periods due to employees being unable to attend work.

In fiscal 2010, we took the following actions in relation to IT systems:

- Transferred the major network equipment that makes up the company intranet to a data center for disaster recovery
- Transferred the IT systems needed to continue provision of maintenance services and the supply of consumables to customers to a data center for disaster recovery
- Improved the means of communication between emergency centers
- Improved the working conditions for telecommuters
- Upgraded action guidelines

Plan for Fiscal 2011

In light of the experiences from the Great East Japan Earthquake, we will strive to improve, upgrade and expand our efforts on two fronts, namely disaster-prevention measures (measures to anticipate disasters and minimize damages) and BCP (planning and preparation for the continuation of important operations).

- Development and implementation of IT system response plans in line with reviewed assumption of risks and the expansion of business fields subject to BCM consideration
- Review of judgment criteria for the emergency response to be implemented and the initial response flow (confirmation of safety, instructions to return home and remain on standby, etc.)
- Examination of means of communication taking multiple risks into account

4. Continuous Education to Raise Awareness of Information Security Issues <Ricoh Group/Japan>

We provided self-assessment-based education programs for all employees. The aim of the programs was to enable them to act based on proper judgment regarding information security initiatives by having them confirm flawed courses of action and actions that can easily lead to incidents through a self-assessment-based system. As a completion requirement, employees repeated the course until they obtained full marks. In this way, we have sought to raise the awareness of security in all employees.

Plan for Fiscal 2011

We will continue to provide education for all Ricoh Group employees to raise awareness of information security issues. With a heightened awareness of security issues among employees, we strive to make proper security-related judgments in our day-to-day work.

5. Using IT to Prevent Recurrence of Information Security Incidents <Ricoh Group/Japan>

There were no major reportable incidents in fiscal 2010. Information on incidents collected in our database for centralized incident management shows that the number of incidents involving the loss of USB flash drives and SD cards has increased in recent years. We have gone further than simply drawing attention to these incidents. In addition to confirming and thoroughly implementing basic management rules and placing a greater priority on these incidents through internal audits, we have also focused on the characteristic light weight and thinness of these types of media. In most of the incidents caused by these characteristics, the human factor is involved; for example, this media easily drops out of the bag when you take out documents. We have disseminated specific examples of incidents and cautions for handling across the Group.

In addition, based on case examples that have rarely occurred but could have resulted in significant incidents, such as mailing the wrong item or new techniques employed by thieves, we have analyzed the chain of multiple inappropriate responses to define a causal relationship between such responses and incidents. These initiatives have been deployed across the Group in the form of "Learning from Case Examples (Code of Conduct)" activities.

Plan for Fiscal 2011

We will determine the times and organizations for which there is a high probability of occurrence by analyzing the collected data on information security incidents in a bid to prevent incidents through foresight and preparatory measures. In addition, we will strengthen coordination with internal audits by predicting the risk of incident occurrence and developing priority items based on the results of ISMS internal audits.