Fiscal 2012 Activities Review and Plan for Fiscal 2013

1. Outline of Fiscal 2012 Activities

Remarkable changes are now occurring in business processes, office environments and in the behavior of individual employees, with the key phrase “workstyle innovation” being used to describe this trend. We are indeed leading more convenient lives through the utilization of smart devices and thanks to the expansion and regular use of cloud services. This increased convenience, however, is also posing new risks, and in response we are working to ensure that confidentiality and availability of information are compatible by enhancing IT security measures and improving related operational methods.

In response to changes made to the social environment, the Ricoh Group is promoting its PDCA management system to boost the information security level, specifically by revising Ricoh Group standard rules and the Ricoh Family Group Information Security Measures, providing employees with education through e-learning, performing checks and improving information security through internal audits.

2. Maintaining Groupwide Unified ISMS Certification (for ISO 27001)

We passed the annual audit for unified ISMS certification (for ISO 27001) as a group, and maintained our ISMS certification.

The following organizations underwent the audit for the first time and were added to the unified certification. (In total, 69 companies worldwide have received the certification: 22 in Japan and 47 overseas).

-In Japan: Ricoh Production Print Solutions Japan Co., Ltd.
-Overseas: Ricoh India Ltd. and Ricoh UK Products Ltd.

We are satisfied that information security is managed in an appropriate manner.

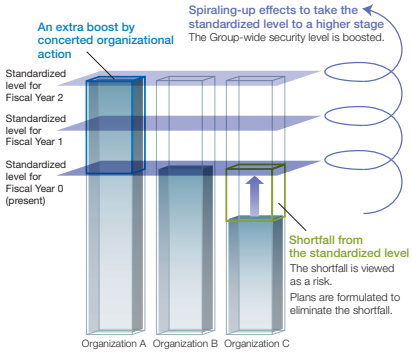
Plan for Fiscal 2013

The Ricoh Group obtained unified ISMS certification in fiscal 2004 and has since been updating it every three years. In fiscal 2013, we will undergo the third renewal audit to maintain our certification. We have thus been updating and maintaining certification for over a decade by responding to technological innovations and other changes in our business environment, including the emergence of new workstyles, expansion and regular use of cloud services and the utilization of smart devices.

3. Continual Improvement and Deployment of Ricoh Family Group Information Security Measures

We established the Ricoh Family Group Information Security Measures to maintain the security level of the entire Group and optimize risk assessments, and have set control items for the daily processing of information (specifically, transport, transmission and the removal of information), thereby making it possible to perform baseline risk assessments. We are also continuously making improvements to respond to new threats and the expansion of new IT devices.

In fiscal 2012, we worked to enhance information security in a practical manner and increase the efficiency of information security-related operations. Specifically, we added IT security measures such as encryption, discontinued procedures for the removal of information and simplified related measures to reduce operational load and increase both the confidentiality and availability of information.



Plan for Fiscal 2013

We will set Group information security measures suitable for new work styles in cooperation with field workers and implement these measures on a global scale.

In addition, we will increase the effectiveness of our information security activities and the latitude of information use by improving both IT implementation and operation.

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

In our BCM[*1] we included maintenance services and supplies of consumables because they are essential to enabling the ongoing utilization of equipment installed on customer premises by the imaging solutions business.

Since fiscal 2011, we have been expanding the scope of business operations targeted for BCM to all areas, including design, development, production, procurement and sales based on the experience we gained from the East Japan Earthquake and Tsunami. Accordingly, we also expanded the quality, quantity and geographic areas regarding our specific BCM processes.

In fiscal 2012, we took the following actions in relation to IT systems:

- -Developed and implemented IT system response plans in line with the reviewed assumption of risks and the expansion of business operations subject to BCM consideration
- -Documentation on actions taken by IT staff
- -Fostered the adherence of IT staff to the action guidelines and provided them with necessary training

Plan for Fiscal 2013 (IT systems)

We will continue to improve, upgrade and expand our efforts on two fronts, namely disaster-prevention measures and BCP[*2].

Disaster-prevention measures: Measures to anticipate disasters and minimize damages

BCP- Planning and preparation for continuation of important operations

- -Review the IT-BCP basic principles, including the concept of a data center for anti-disaster measures, based on the examination of conventional activities and on changes assuming damage announced by governmental agencies
- -Continuous provision of training to foster the adherence by IT staff to the action guidelines, and the identification of problems and examination of measures for improvement through the training

*1 : BCM: Business continuity management

*2 : BCP: Business continuity plan

5. Continuous Education to Raise Awareness of Information Security Issues <Ricoh Group/Global>

We have provided all Ricoh Group employees with education on information security.
Specifically, we provided them with the latest information on the following issues in addition to ensuring that they are aware of the Group's ISMS policies and security measures and reconfirming with them the information security rules that are to be followed on a daily basis:

- -Daily measures to be implemented in response to the information security incidents that have occurred recently, including advanced persistent threat (APT)
- -Scope of information disclosure and rules on copyright, etc. for social media

In Japan, about 40,000 Ricoh Group employees have received the education via the e-learning site.

Plan for Fiscal 2013

We will continue providing all Ricoh Group employees with education on our information security policies and measures and on the information security rules that they need to comply with in their daily operations. We will also focus more on the following issues in consideration of the convenience brought about by technological innovations amid changes in work styles, the vulnerability of information security and compatibility between confidentiality and availability of information:

- -Strict compliance with the rules set in new fields in line with IT progress
  Examples: Rules on the utilization of smart devices, rules on social media and rules on the use of cloud services

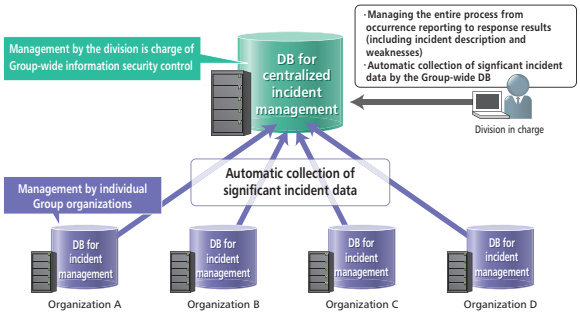
6. Using IT to Prevent Recurrence of Information Security Incidents <Ricoh Group/Japan>

There were no major incidents announced publicly or reported to auditing and supervising organizations in fiscal 2012.
We are implementing the management system by taking the following steps to prevent the (re)occurrence of information security incidents.

(1) We have been sharing information on information security incidents and measures taken to prevent their recurrence across the Group since fiscal 2011.
http://www.ricoh.com/about/security/management/project_report/2012.html

(2) We have included incidents that tend to occur in our daily operations, such as the loss of PCs and external recording media as targets for information security education, thereby ensuring that employees are well aware of the measures to be implemented to prevent the recurrence of similar incidents.

(3) We incorporated important incident information and educational items as priority items to be examined in our internal information security audits, and fostered awareness and improvements across the Group regarding these additions.



Plan for Fiscal 2013

We will work on a continual basis to reduce the number of serious accidents to zero.
Based on the recognition that even relatively minor incidents might be signs of serious accidents to come, we will strive to prevent the (re)occurrence of such incidents.
We will continue to provide information on information security incidents in concert with the educational and internal audit systems, thereby increasing the effectiveness of our (re)occurrence prevention measures.