Fiscal 2013 Activities Review and Plan for Fiscal 2014

1. Outline of Fiscal 2013 Activities

In fiscal 2013, cyber attacks, particularly targeted attacks seeking to breach the information system of a particular company or organization, posed a major threat. At the Ricoh Group, the website of a subsidiary was targeted by such an attack, which, regrettably, caused inconvenience to our customers. (Please refer to "6. Using IT to Prevent Recurrence of Information Security Incidents" below.)

Under the watchword of "workstyle innovation," business process innovation is promoted by introducing in-house SNS. As a result, remarkable changes are occurring in office environments and the behavior of individual employees. 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, also poses far-reaching new risks. To address the situation, we are working to raise employees' awareness of the updated Ricoh Family Group Information Security Measures, enhance IT security measures (e.g. introducing full disk encryption for externally portable PCs) and improve related operational methods so as to make the confidentiality and availability of information compatible.

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.Third Renewal of Groupwide Unified ISMS Certification (for ISO 27001)

Since its initial attainment of unified ISMS certification in December 2004, the Ricoh Group has successfully updated its certification by passing annual audits and triennial renewal audits conducted by a third-party auditor. We were audited for the third renewal in fiscal 2013 and we will retain our certification in fiscal 2014.

As of December 2013, a total of 66 Ricoh Group companies (19 in Japan and 47 overseas) have been certified. There were no additional certifications during the fiscal year, either by a domestic or overseas company. For the scope of the certification, please refer to the list of Ricoh ISMS registrations prepared by an external certification body.
http://www.bsigroup.com/ja-JP/ISO27001/ricoh/ (in Japanese)

Plan for Fiscal 2014

In fiscal 2014, we will undergo an annual 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. We also intend to accomplish the transition to ISO/IEC 27001:2013 (JIS Q 27001: 2014) during the fiscal year.

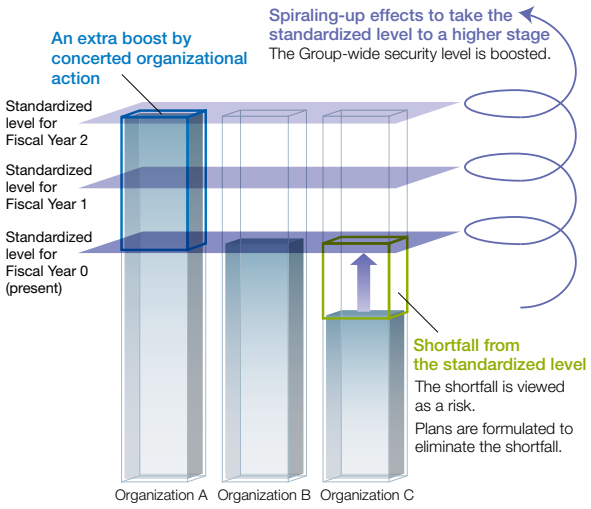
3.Continual Improvement and Deployment of Ricoh Family Group Information Security Measures

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 2013, the applicable ISO/IEC standard was revised to ISO/IEC 27001:2013 (JIS Q 27001: 2014). Accordingly, necessary revisions were made to the aforementioned information security measures to address the latest international standards.

In fact, most of the revised requirements call for measures that we have already long been practicing. For example, "5.1b): Ensuring the integration of the ISMS requirements into the organization's processes." is consistent with our "Corporate Information Security Culture, under which we aim to ensure that all employees take secure actions during their routine work. In other words, our information security activities are integrated into our operational processes, which means that we have already been in compliance with the new provisions since we initially obtained certification.

At the same time, we added a new standard that corresponds to the revised requirements for operational use of cloud systems. As technological innovations in this area are taking place rapidly, we intend to build and operate appropriate security measures through many discussions between cloud system users and operators within the Group, rather than establishing detailed regulations.



Plan for Fiscal 2014

In fiscal 2013, the Ricoh Group launched a project for promoting innovation for new workstyles. Drawing on the pilot experience obtained from this project, we will formulate applicable information security measures designed to support our new project together with those who actually use the systems, and will implement the measures established 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

Information pertaining to our risk management, as part of the governance efforts of the Ricoh Group, is now publicly disclosed. For details of our business continuity plan (BCP), please refer to:
http://www.ricoh.com/about/governance/risk.html

This section focuses on the activities on BCP and BCM (business continuity management) related to our IT infrastructure. In fiscal 2013, we conducted specific measures to solidify our BCP systems, such as holding contingency drills and improving the BCP systems based on the findings of the drills. We were able to implement such measures because we were in a phase where a solid system was in place to operate the PDCA cycle in a continuous and steady manner.

(1) Drills held in fiscal 2013
The following drills were held during the fiscal year:

	Drill descriptions	Feedback on the drill results
1	Drill focusing on initial response to an emergency (Assessing damage, deciding on the necessity of establishing an emergency command post, etc.)	After the drill, collect participants' feedback on the procedures, including written procedures. The feedback collected was incorporated into the revised written procedures.
2	Drill focusing on checks to confirm the operational status of IT systems in the event of an emergency	Verified whether or not relevant checking procedures were in place and identified problems present in written procedures. Where necessary, a request was made to establish or revise the relevant procedures.
3	Drill focusing on collaboration in the initial response with IT units of Ricoh Japan Corporation, a sales subsidiary.	Reviewed the basic actions to be taken as a collaborative initial response. There were no reportable findings.

(2) Data continuity (backup system)
Simultaneous loss of both primary data in an information system and its backup data would have a critical impact on business continuity. In addition to implementing basic measures, i.e., remote storage of backup data, physical transfer by the transportation of backup tapes as well as creating and storing backups online in a cloud environment have now been added to our data continuity measures. The method that should be adopted is determined primarily based on the importance, volume, and update frequency of the backup data.

News

Ricoh Industry Company,Ltd. , Tohoku Office of Ricoh Technologies Company,Ltd. and PC Unit Products Company of Ricoh Company,Ltd. acquired ISO 22301 for their business continuity management systems (BCMS) and completed their registration in December 2013. The following related information from the Ricoh Group appears on the website of the Ministry of Economy, Trade and Industry:

- The Ricoh Group's basic policy on BCP and recovery target objective
- Background and objectives of our seminars for suppliers
- Key points in building BCP/BCMS

http://www.meti.go.jp/policy/economy/hyojun/group-ms/index.html (in Japanese)
http://www.meti.go.jp/policy/economy/hyojun/group-ms/c_group_17.html (in

Plan for Fiscal 2014 (IT Systems)

We will continue to improve, upgrade, and expand our efforts with even more specificity, focusing both on disaster-prevention measures and BCP.

1. Review of mission-critical IT systems that are subject to BCP as well as status checks on necessary measures

2. Conducting periodic drills as an established regular activity
We are planning to hold drills as part of PDCA management systems.

3. Expansion of the scope of domestic subsidiaries that participate in collaboration drills
We are planning to place additional emphasis on domestic affiliates with which we should collaborate and expand our drills to include them.

Disaster-prevention measures: Measures to anticipate disasters and minimize damage
BCP: Planning and preparation for continuation of important operations

5. Continuous Education to Raise Awareness of Information Security Issues

We offered an e-learning program on information security to all Ricoh Group employees.
The program was designed to raise employees' awareness and improve their understanding of information security through answering "what-would-you-do" questions pertaining to strict compliance with the rules regarding SNSs and other new fields emerging in concert with progress in information technology as well as on basic traditional rules. In Japan, about 40,000 Ricoh Group employees received this education via the e-learning site. In addition, we also offered training programs for specific job levels and positions, such as for new employees and ISMS Office staff, as well as other e-learning and classroom training programs as part of our annual training programs.

Plan for Fiscal 2014

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 workstyles, the vulnerability of information security and compatibility between confidentiality and availability of information:

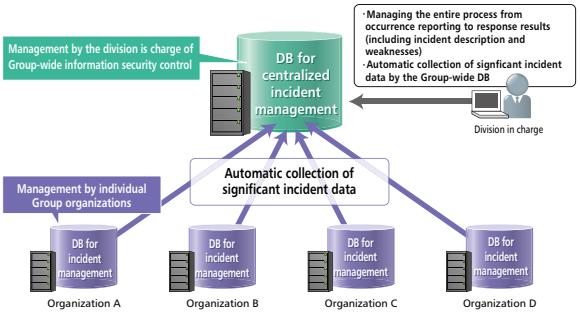
■Strict compliance with the rules set in new fields in line with IT progress
Examples: Rules on the utilization of smart devices, rules on social media and rules on the use of cloud services

6.Using IT to Prevent Recurrence of Information Security Incidents

We regret the occurrence of a major incident in fiscal 2013. For details of this incident, please refer to:
"Notice on unauthorized change of the Printout Factory website"
http://www.ricoh.co.jp/sales/news/130603.html (Japanese)

We extend our deepest apologies to those who visited the website during the affected period for the inconvenience and problems that this incident may have caused them. Acknowledging the seriousness of this incident, we will make utmost efforts to prevent a recurrence.

We operate our management system to prevent the occurrence and recurrence of information security incidents by following the steps specified below:
(1) Sharing information on information security incidents and measures taken to prevent their recurrence across the Group. We have been taking this measure since fiscal 2011.
(2) Continuing to include 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)Incorporating important incident information and educational items as priority items to be examined in our internal information security audits, and fostering awareness and improvements across the Group regarding these additions.



Plan for Fiscal 2014

We will work on a continual basis to reduce the number of serious accidents to zero.
Going forward, we will place particular focus on web-related incidents, which are anticipated to increase in the future. At the same time, we will also strive to prevent the occurrence and recurrence of traditional types of information security incidents in tandem with our educational programs and internal audit systems by using IT systems in a greater capacity and more effective manner.