

Building Foundations for Group ISMS around RFG ISMeasures

Since April 2007, the Ricoh Group has made an all-out effort to disseminate to Group companies a set of RFG ISMeasures established a month earlier and to make sure they take root. Equipped with the RFG ISMeasures, the Ricoh Group aims to continuously raise the level of information security of its companies in order to further strengthen the foundations for the delivery of new value to customers.

Raise the Level of Security for the Entire Group

For the Ricoh Group to fulfill its corporate social responsibility and to increase corporate value through information security initiatives, it is essential to transcend organizational borders and raise security to a uniform level across the board.

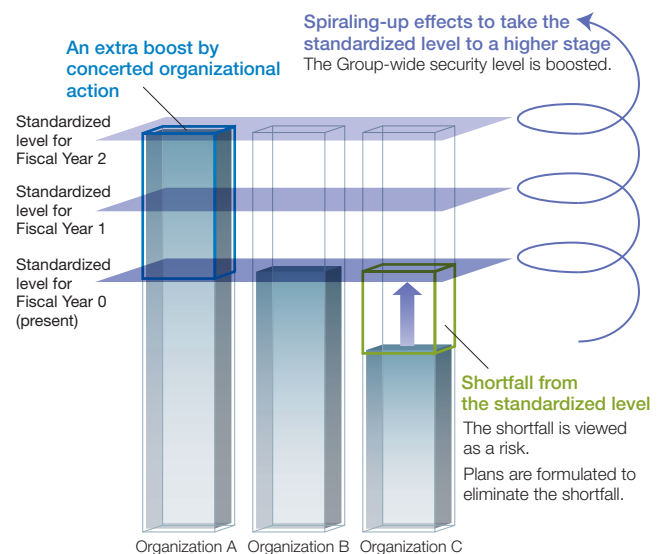
The companies of the Group vary in terms of size and corporate culture. And, they are engaged in a broad range of activities from research, development, design and production to sales and service. In addition, the level of information security undertaken individually is also likely to vary from one company to another. The Ricoh Group realized that a set of common standards serving as unified Group-wide policies would be needed to solve these problems and to increase the effectiveness of Group ISMS—a foundation for information security activities. In addition, specific performance standards were needed since ISO/IEC 27001 does not specify to what degree individual safety measures should be implemented. Discussions began in December 2005 to determine the performance standards corresponding to various risk levels consistent with the requirements of international standards. These were finalized as RFG ISMeasures in March 2007. Full-fledged dissemination of the standards across the Group began in April 2007 to ensure that they would take root in every Group company.

RFG ISMeasures Specific to Information Asset Classes Categorized by Importance

The purpose of establishing RFG ISMeasures and disseminating it across the Group is to increase the level of information security practiced by individual companies to a standardized security level, and to trigger spiraling-up actions to continuously raise this level. To achieve this, the ISMS framework is used to take inventory of the information assets of Group companies, conduct risk analysis of each asset, identify weaknesses, and take appropriate actions for proper management.

To assist these efforts, the RFG ISMeasures specify handling standards for various classes of information assets. Information is first roughly grouped into information contents, hardware, software, services and affiliated organizations categories. It further undergoes two stages of checks known as “Required Measures” and “Recommended Measures,” depending on the operational importance of the specific information.

■ Spiraling up for standardized level

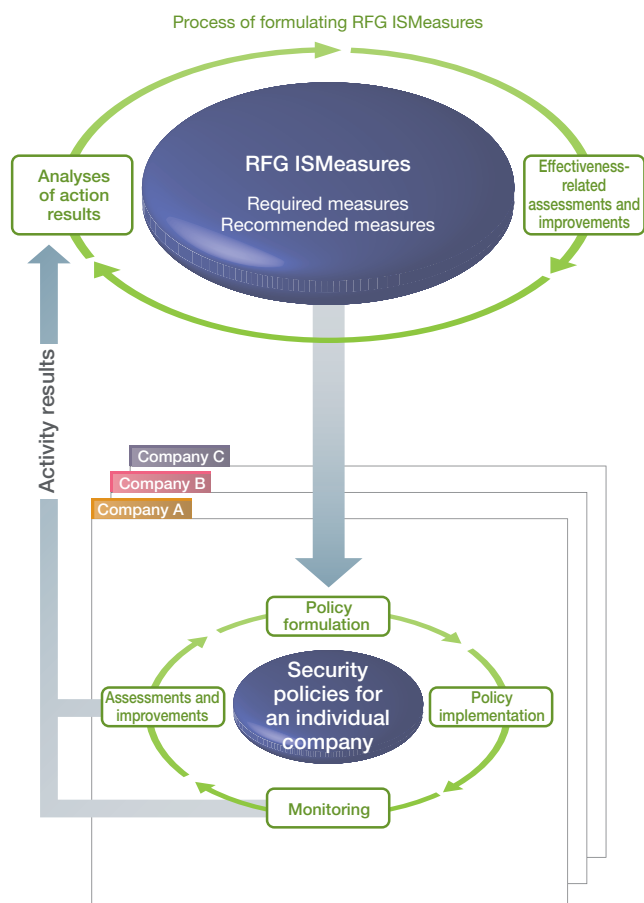


Policy Formulation Based on RFG ISMeasures and Requirements of Specific Workplaces

Required measures must be implemented across the Group. The Information Assets Control owner at each workplace compares the necessary security level and other requirements for a specific information asset against its present level of security management, assesses the risks and determines whether a shortfall exists, and takes appropriate steps to address those risks. Recommended measures may be taken at the discretion of each workplace to suit its task characteristics. After a comparison similar to the above is performed, recommended measures may be implemented if necessary in view of the specific task of the workplace. Moreover, if there should be more points of compliance in light of the functions, characteristics and present state of the organization, these may be added. This approach allows the RFG ISMeasures to be optimized to suit individual workplaces, which results in a set of security policies unique to each company. These are integrated into daily tasks and carried out and refined by line managers, who are engaged in PDCA-based daily management.

The state of the management system is also assessed in order to review the control level administered by an organization and confirm the proper functioning of the PDCA cycle, and to the purpose relating to the handling of information assets. Special tools are also available to facilitate these risk assessment procedures.

■ Risk assessments by individual companies based on RFG ISMeasures



Simplifying Risk Assessment Techniques

One advantage of managing information security with RFG ISMeasures at the core is simplified risk assessment, which allows line managers to manage information assets without using technical jargon. Risk assessment is carried out, even in the absence of technical knowledge, by the use of risk assessment tools based on RFG ISMeasures. This also establishes a mechanism for third-party organizations to confirm the conformity and effectiveness of risk assessment with internal and external audits. The control division of the headquarters collects the results of security activities by Group companies and summarizes these results for the future assessment and improvement of RFG ISMeasures. The RFG ISMeasures are updated in step with external changes and the state of the Ricoh Group, while the security level is scaled upward with an extra boost by the entire Group's spiraling-up effects.

■ RFG ISMeasures sample

