

# 2

## ISMS in Action (Japan) Case 2: Major Accounts Marketing Division, Marketing Group, Ricoh Company, Ltd.

### Putting Information Security Management into Practice for the benefit of Customers

The Major Accounts (MA) Marketing Division, the only section within Ricoh proper engaged in direct sales, sells office automation equipment and solutions and performs maintenance for leading private corporations, the central government, municipal governments and universities. Through its interaction with customers, at an early stage it became aware of the importance of information security, and in 2003 it became the first unit in the Ricoh Group to obtain ISMS certification. Upholding the dual goals of information use and protection, it produces security solutions whose usability is confirmed through company practices.

#### MA Marketing's Initiatives for ISMS and Personal Information Protection

The MA Marketing Division undertakes the following activities and proposes to customers solutions that reflect the results of these activities.

##### 1) Development of 18 IT databases and navigators

The Division developed 18 databases and navigators for centralized management of a complete range of information security-related information, which reduced the administrative burden on the personnel in the front lines of sales activities.

##### 2) Twice-monthly security subcommittee meetings

The subcommittee formulates actions to be taken after confirming the state of progress in remedial matters pointed out in incident reports, by workplace patrolling and in audits/examinations, and proposes them to the Information Security Committee.

##### 3) Monthly security patrolling at departmental level

Designated persons confirm the state of compliance and provide guidance through regular follow-up activities.

##### 4) Periodic education for employees by function and rank (at least one session every six months)

Activities include distributing the practical rulebook.

##### 5) Periodic internal audits and follow-up audits (twice yearly)

Issues identified during an audit are shared by all employees to bring improvements.

- 6) Centralized control of mobile PCs, home PCs and USB flash memory and their lend/return
- 7) Readiness to comply with requests by customers and business partners for information, surveys concerning actions and trends (second-party audits)
- 8) Sharing of information on incidents for better preventive measures

Inventory of Assets, the information owners of all 75 organizations completed workflow charts for all of their respective organizational functions. Then, a risk assessment was made of all information assets using the RFG ISMeasures. These assets included workflow-related input information, facilities and equipment used for processing, and output information drawn from these. This resulted in increased efficiency in extracting information assets of higher priority, and a solid foundation for information security was completed. Periodic reviews have been done since then to ensure that information assets are in good order.

#### Tips on Building ISMS (Extracting Information Assets)

To prepare the Inventory of Assets, an ISMS requirement as specified in Annex A.7.1.1

#### ■ Development of ISMS management (FY2006–FY2007)

	Fiscal 2006	Fiscal 2007
Key assessments, audits	<p>For increased penetration</p>	<p>For increased optimization</p>
Backgrounds	May JISQ 27001 May Revised JISQ 15001 October Surveillance Audit (second year) including assessment for transition to ISO 27001	August Renewal Audit (3rd year) Advances made in international standards of BCP Progress made in Group information security governance
Aims of initiatives	<b>Readiness for ISO 27001 and establishment of security governance</b> <ul style="list-style-type: none"> <li>• Stepped-up efforts to formulate RFG ISMeasures for information security measures.</li> <li>• Assessment of effectiveness of management measures with information holders as key players</li> <li>• Stronger monitoring and reviews</li> <li>• Boosting awareness of individual members</li> </ul>	<b>Higher maturity through the formation of information security governance</b> <ul style="list-style-type: none"> <li>• Operations based on RFG ISMeasures</li> <li>• Continual improvement made by monitoring the effectiveness of the entire ISMS and daily management</li> <li>• Voluntary implementation of security patrols (monthly)</li> </ul>