

4

Promoting Internal Control

Securing Internal Control As a Step to Becoming a Global Enterprise with Greater Added Values

The Ricoh Group is strengthening and promoting internal control aimed at the “maintenance of a high degree of confidence in financial reporting,” “increased business effectiveness and efficiency,” and “compliance with laws, code of conduct and internal rules” in its quest to become a global company with greater added values. Subsequent to the enactment in July 2002 of the Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley Act, also known as SOX) in the United States, corporations with financial reporting based on generally accepted accounting standards in the United States (U.S. GAAP) faced the urgent task of complying with the requirements stipulated in Section 404 of the Act. The following section describes examples of actions taken by the Ricoh Group with respect to internal control.

Ricoh Group’s Efforts to Ensure Compliance with the U.S. SOX Act

A broad range of actions have been initiated by the Ricoh Group since 2003 to strengthen and promote internal control and to encourage its further penetration, as well as to ensure compliance with the SOX Act of the United States. Additionally, in fiscal 2006, it established a Basic Policy Concerning the Development of an Internal Control System in a move to comply with the new Company Law. Based on the results of the effectiveness assessments by the Group-level internal control, it completed the Fiscal 2006 Internal Control Report, which was compiled and certified by a third-party auditor.

During fiscal 2007, internal control functions were reorganized and strengthened, and a department dedicated to internal control was created. The Basic Policy Concerning the Development of an Internal Control System was partly amended to reflect the formation of an internal control committee within the Group Management Committee (GMC) and other changes.

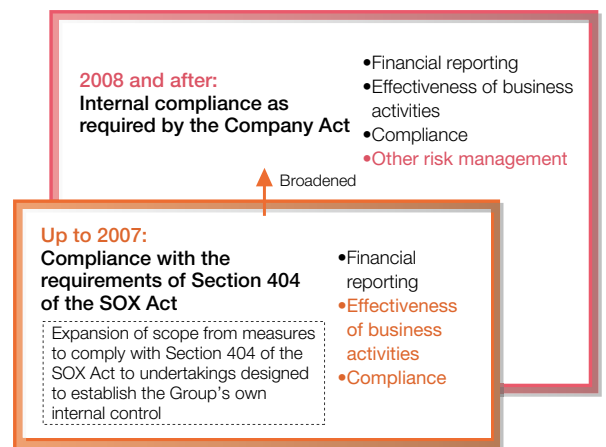
Key activities are outlined below.

Integrated Internal Auditing Resulted in Increased Effectiveness and Efficiency of Audits

The Ricoh Group conducted integrated internal audits to address issues covered by the SOX Act, task audits, accounting audits, business process risk management audits, and theme audits. As part of this, audits were used to establish connections with process results using SOX-compliant tools such as flow charts and a risk control matrix as core auditing tools.

Comprehensive internal auditing has three main advantages. First, on-site inspections by Internal Management and Control Division lead to more effective risk management by each company and department. Second, examinations that focus on “results” of processes as the starting point of observations—in addition to conventional process-oriented examinations—boost auditing efficiency and effectiveness. Third, integrated auditing reduces redundancy in the items to be audited and the time required for auditing, benefiting both the auditing and audited parties. The Ricoh Group’s internal control concept has broadened each year, undergoing the transformations shown in the diagram.

Evolution of internal control concept



Readiness for the Financial Instruments and Exchange Law Achieved by Leveraging Experience of SOX Compliance Measures

Subsequent to the legislation of the Financial Instruments and Exchange Law in June 2006, the Financial Services Agency issued Evaluation and Auditing Criteria for Internal Control Pertaining to Financial Reporting and Implementation Criteria. In a parallel move, the Ministry of Economy, Trade and Industry (METI) published IT Control Guidance Pertaining to Financial Reporting. The Ricoh Group believes that the measures it took to comply with the SOX requirements have readied the Group to meet the internal control requirements as set forth in the law in terms of overall internal control for the Group and control of business process flows other than IT control. For IT control, work is already underway to comply with the relevant requirements of Section 404 in line with the overall IT control framework including governance and business processing control.

For IT control matters relating to financial reporting that require action, the above guidance published by METI provides models for (1) internal IT control in an entire corporate group (group-level IT control), activities to create an environment for effective business processing control directly concerning the reliability of financial reporting (overall IT control), and (3) internal control embedded in business processes designed to ensure accurate processing and recording of all approved tasks in the sphere of information technology that controls business (control over IT business processing).

The frameworks for “Internal Control Pertaining to Financial Reporting” and for “IT Control Guidance Pertaining to Financial Reporting” are both based on the COSO* control. No significant differences are observed in the two frameworks, since their basic components are group-level IT control including IT governance, overall IT control including IT security, and control over IT business processing. Therefore, the experience of administering measures for compliance with the SOX Act can be fully leveraged in meeting the IT control requirements specified by the law.

*An internal control framework released by the Committee of Sponsoring Organization of the Tradedway Commission in 1992. It serves as the de facto global standard.

Integrating Information Security with IT Control-related SOX Requirements

Actions for ISMS are similar to actions to comply with the IT requirements of the SOX Act. The Ricoh Group, which formerly administered separate actions, is now taking an integrated approach for increased efficiency by devising actions to address the two challenges simultaneously. Some examples are detailed below.

Although information security activities and activities geared to SOX compliance share the same risk approach, the former require management measures based on risk assessment primarily of information assets (static), while the latter focus on control based on risk assessment primarily of work processes (dynamic). For this reason, it is difficult to bridge the two spheres in terms of the classification of matters exposed to risks, and descriptions of risks and control measures. In the past, some matters that were already assessed in terms of information security had to be assessed once again in view of the SOX Act. This caused redundant confirmation efforts by the IT department and redundant effectiveness assessments by the auditing department. And because of the gap between information security activities and SOX compliance activities, there was little opportunity to apply to a wider range of systems the know-how gained in achieving stronger internal control through SOX-related systems.

To address these difficulties, the Ricoh Group prepared RFG ISMeasures for the classification systems of assets and tasks covered by the two spheres and for equivalent or corresponding risks and control mechanisms as a first step toward the full integration of ISMS and SOX-IT activities. The RFG ISMeasures allow the diverted use of SOX-related operational test results for the purpose of information security and eliminate redundant work. Also, regarding system development, the Ricoh Group ensures that, from the very start and not as something added on later, criteria reflecting the SOX requirements are fully incorporated into

developmental and operational specifications of systems subject to the SOX Act.

The Ricoh Group will continue to work hard to increase ability and efficiency in compliance matters, by expanding RFG ISMeasures applicable to the two spheres.

Note: Reporting requirements for the assessment and auditing criteria for internal control of financial reporting are diverse. This report primarily deals with IT control and IT security governance. For more detail, please consult securities reports and internal control reports.

■ Sample screen showing RFG ISMeasures (integration/fusion of general SOX-IT control)

