

**The Issues of Internal Controls
from the Perspective of
Information Security**

Keiichi HIMENO

Nomura Research Institute

The Issues of Internal Controls from the Perspective of Information Security

Keiichi HIMENO

- I The Roles of Information Security and Associated Loopholes
- II Overall IT Control as Seen in the Exposure Draft
- III Questionnaire Surveys Reveal Current Information Security Measures and Issues
- IV Toward Establishing Efficient Internal Controls through the Use of Information Security

In 2006, internal controls within a company attracted a great deal of attention, with the IT industry proposing a wide range of solutions (problem-solving systems) to deal with the New Company Law and the Financial Instruments and Exchange Act (also known as the Japanese version of the SOX Act). In November 2006, the “Proposed Evaluation and Auditing Standard on Internal Controls over Financial Reporting (Exposure Draft)” was announced. This standard serves as the guidelines for developing an internal control system as provided for in the Japanese version of the SOX Act. Pursuant to these guidelines, every company will be expected to put all their efforts into complying with the Japanese version of the SOX Act.

To identify the issues that must be resolved relative to internal controls from the perspective of information security, NRI Secure Technologies conducted surveys and research activities. These surveys revealed that, regarding information security measures, many companies have perfect technical measures in place, but their employees have not been fully educated in the fundamentals of information security. We also found that some employees fail to observe the company rules that have been established.

In order to develop an overall IT control system efficiently, it is important to pay attention to information security. I believe that it will be even more vital for management executives to be fully involved in order to achieve the reforms in attitudes needed to attain compliance (observance of rules).

I The Roles of Information Security and Associated Loopholes

In 2006, considerable attention has been given to internal controls in companies, with the IT (information technology) industry being active in proposing new solutions (problem-solving systems) for dealing with the New Company Law and the Financial Instruments and Exchange Law (the Japanese version of the SOX Act).

In November of 2006, the Financial Services Agency announced the “Proposed Evaluation and Auditing Standard on Internal Controls over Financial Reporting (Exposure Draft),” which serves as guidelines for developing an internal control system as specified in the Japanese version of the SOX Act. Based on comments received from the public, the final version will be implemented in 2007.

What exactly are these internal controls? As defined in the exposure draft, “internal controls refer to processes that are incorporated in business activities and that are implemented by all people involved within an organization in order to rationally guarantee the attainment of four objectives, namely, achieving effective and efficient business activities, ensuring the reliability of financial reports while observing laws related to business operations, and preserving assets. The processes consist of six basic elements, namely, the control environment, risk assessment and preventive measures, control activities, information and its distribution, monitoring activities, and IT control.”

The term “IT control” mentioned in this definition is not clearly stated in the US SOX Act (Sarbanes-Oxley Act; the Public Company Accounting Reform and Investor Protection Act), on which the Japanese version is based. The inclusion of IT control in the proposed standard (exposure draft) has given rise to expectations among IT vendors for opening up new business opportunities, resulting in the appearance of a sort of social phenomenon that can be described as an “internal control solution boom.”

Although it is easy to use the term “internal controls,” the actual objectives vary depending on the focus of a company’s management. Furthermore, solutions offered for each type of internal control have not yet necessarily been optimized. Therefore, we face a problem in that there are currently very few general-purpose systems. In addition, because it is difficult to identify cost effectiveness in this field, there are also doubts about whether an internal control system that can justify an enormous investment can be developed efficiently.

Because of this, there are probably many management executives and IT personnel who, when faced with the issue of how to develop an internal control system that is both efficient and effective, would like to learn from the innovative examples set by other companies.

In this paper, we look at the roles of information security and associated loopholes as it relates to the development of overall IT control systems.

Of particular relevance to information security is the fact that many people perceive it as being nothing more than one aspect of IT. This stems from the fact that internal controls have never been actively discussed from the perspective of information security.

This paper first looks at the issues related to “the use of IT” aimed at the development of internal control systems, as stated in the exposure draft. After taking a general view of the overall business solutions that are generally considered as addressing information security, I will explain the current state of internal controls relative to information security and how they are likely to develop in the future. In addition, from the standpoint of company management, I will also explain an approach for efficiently developing internal control systems that ensures information security as well as the importance of the commitment of management executives.

II Overall IT Control as Seen in the Exposure Draft

Currently, we are seeing a rapid increase in the amount of material concerning how to deal with the Japanese version of the SOX Act and overall IT control, both in print and on the Internet. Nevertheless, there is relatively little information on the objectives of overall IT control and optimal solutions for developing efficient internal control systems. Below, I describe how the participation of management executives is important as indicated in the exposure draft, and the ways in which information security is related to internal controls as laid down in the Japanese version of the SOX Act.

1 Overall IT Control and Third-Party Certification

Table 1 is an extract from the exposure draft reference material, showing the IT-related activities mentioned in “Example Evaluation Items for Internal Controls.”

In the same way as other items in the exposure draft, overall IT control is only covered in abstract terms, such that individual companies can achieve it in their own particular way. In addition, regarding the way in which internal control systems are developed, companies are given an extremely wide range of discretion in the courses they take. The result is that there may be management executives and IT personnel who are puzzled about where to begin their efforts.

Furthermore, if a company applies overall IT control without explicit objectives, its IT investment may become excessive. To prevent such a situation, the exposure draft includes a sentence that states “For the internal control reporting system specified under the Financial

Table 1. “Example Evaluation Items for Internal Controls” in the Exposure Draft (IT-related Activities)

<ul style="list-style-type: none"> • Have management executives formulated appropriate IT strategy, plans, etc.? • Have management executives understood the IT environment properly when developing the internal control system? Have they clearly indicated their policy based on this understanding? • To reduce risks that hinder the achievement of producing reliable financial reports, have management executives made proper decisions on differentiating between those control aspects that are done manually and those that can rely on IT? • When using IT to set up control activities, have risks newly incurred using IT been considered? • Have management executives set up appropriate policies and procedures for overall IT control and IT-related business process control?

Note: IT = information technology.
 Source: Financial Services Agency, “Proposed Evaluation and Auditing Standard on Internal Controls over Financial Reporting (Exposure Draft)—(Reference 1) Example Evaluation Items for Company-wide Internal Controls Relating to Financial Reporting”.

Instruments and Exchange Law, the establishment of IT control is required to ensure the reliability of financial reports, and the establishment and operation of IT control to achieve purposes other than ensuring such reliability is not directly required.” As the assumed background factor behind this inclusion, auditing firms in the US implemented measures in compliance with the SOX Act; as a result, investments made by companies subject to auditing have become excessive, leading to a need for reviewing the best way to implement the Act.

For current corporate activities, IT is vital to all business processes. Because of this, the coverage of overall IT control required under internal controls is extremely

extensive, making it very difficult to determine just where to begin to develop an internal control system.

In this regard, the following systems can provide references for ways of developing internal control systems. They are ISO9001 (quality management system), which gained considerable attention in the 1990s as a modern service management quality control method, ISO27001 (conformity assessment scheme for information security management systems (ISMS)), for which third-party certification was started by JIPDEC (Japan Information Processing Development Corporation) in 2001, and ISO20001 (conformity assessment scheme for IT service management systems (ITSMS)), for which third-party certification is scheduled to start in April 2007.

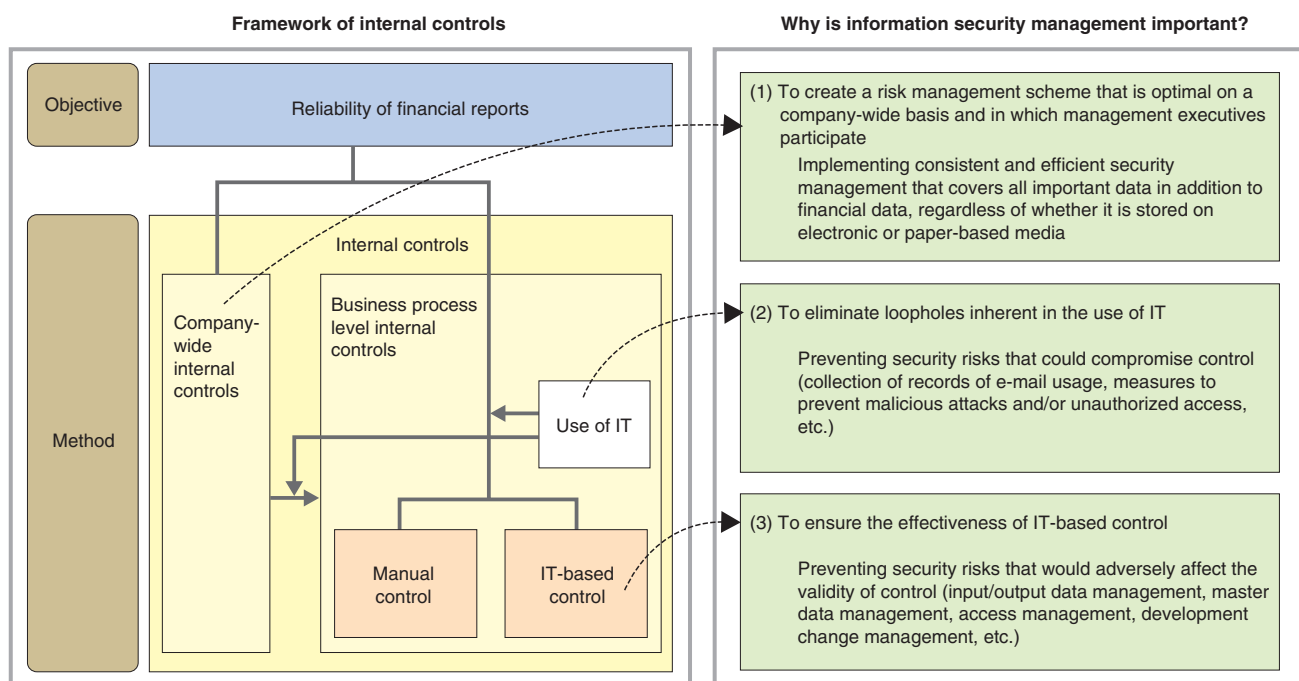
The reasons why these systems can serve as references include (1) the change management and access management implemented under ISMS and ITSMS overlap in some aspects with measures required for overall IT control, and (2) all of these international standards ensure objectivity because a third party entity certifies that the internal controls within an organization are functioning properly through implementation of the PDCA (plan, do, check, act) cycle.

Specifically, a major advantage of third-party certification as described above is that it facilitates company understanding of the critical features in the development of an overall IT control system.

2 Importance of Information Security Management

Figure 1 shows the framework of internal controls specified in the Japanese version of the SOX Act and

Figure 1. Reasons Why the Improvement of Information Security Management is Important under the Japanese Version of the SOX Act



the reasons why the improvement of information security management is effective.

The framework of the internal control system required under the Japanese version of the SOX Act is shown on the left.

The major goal and objective of the Japanese version of the SOX Act is to guarantee the reliability of financial reports. This objective is achieved by the use of internal controls, which can be broadly divided into company-wide internal controls and business process level internal controls. Of these two, business process level internal controls are achieved through three control methods, namely, manual control, the use of IT and IT-based control.

The reasons why information security measures are so important are listed in the right-hand part of Figure 1. Before looking at that, however, let's spend some time considering the concept of information security measures.

Discussions on information security measures often refer to the three essential elements of CIA. This term is obtained by taking the first letter of the essential information security elements defined by the International Organization for Standardization (ISO), namely, "confidentiality," "integrity" and "availability." That is to say, the objective of information security is to assure confidentiality, integrity and availability. Therefore, the development of an internal control system should also emphasize CIA.

There are three reasons why information security management is important for the development of an internal control system: (1) to create a risk management scheme that is optimal on a company-wide basis and in which management executives participate, (2) to eliminate loopholes inherent in the use of IT and (3) to ensure the effectiveness of IT-based control.

Reason (1) means that the participation of management executives is essential to develop a company-wide internal control system and that, for this purpose, a risk management system that is optimized from the perspective of the entire company must be provided.

Reason (2) aims to eliminate those security risks that would render control invalid by collecting records of e-mail usage and implementing measures to prevent malicious attacks and unauthorized access.

Reason (3) aims to prevent security risks that would adversely affect the validity of control by implementing input/output data management, master data management, access management, development change management, etc.

3 Importance of Access Management

As described above, when developing an internal control system, it is particularly important to ensure integrity (the integrity of financial information in the case of the Japanese version of the SOX Act) among CIA elements.

To ensure the integrity of information, it is essential to prevent the tampering of data, which requires the establishment of mechanisms whereby only persons with the required authority can access the data. To ensure such integrity of information, there is a need for distinguishing levels of authority and an access management technology that supports such distinction.

Figure 2 illustrates this concept. This illustration shows the flow of access management that allows access only to those persons with the required authority. Both security/IT personnel and personnel engaged in business activities are working together to establish this flow.

Access management technologies can be categorized into "user authentication," "entry/exit management," "logical access control," "log acquisition/analysis," etc. In particular, from the perspective of preventing unauthorized persons from accessing or tampering with data, a company must adopt the principle of "need to know, need to do" (whereby only those persons who absolutely must access the data are allowed to do so). In other words, it is extremely important to properly implement information security management by clarifying individuals' authorities and by accurately reflecting any changes in the authorities designated in the system such as to allow data reference or updating due to personnel transfers, etc.

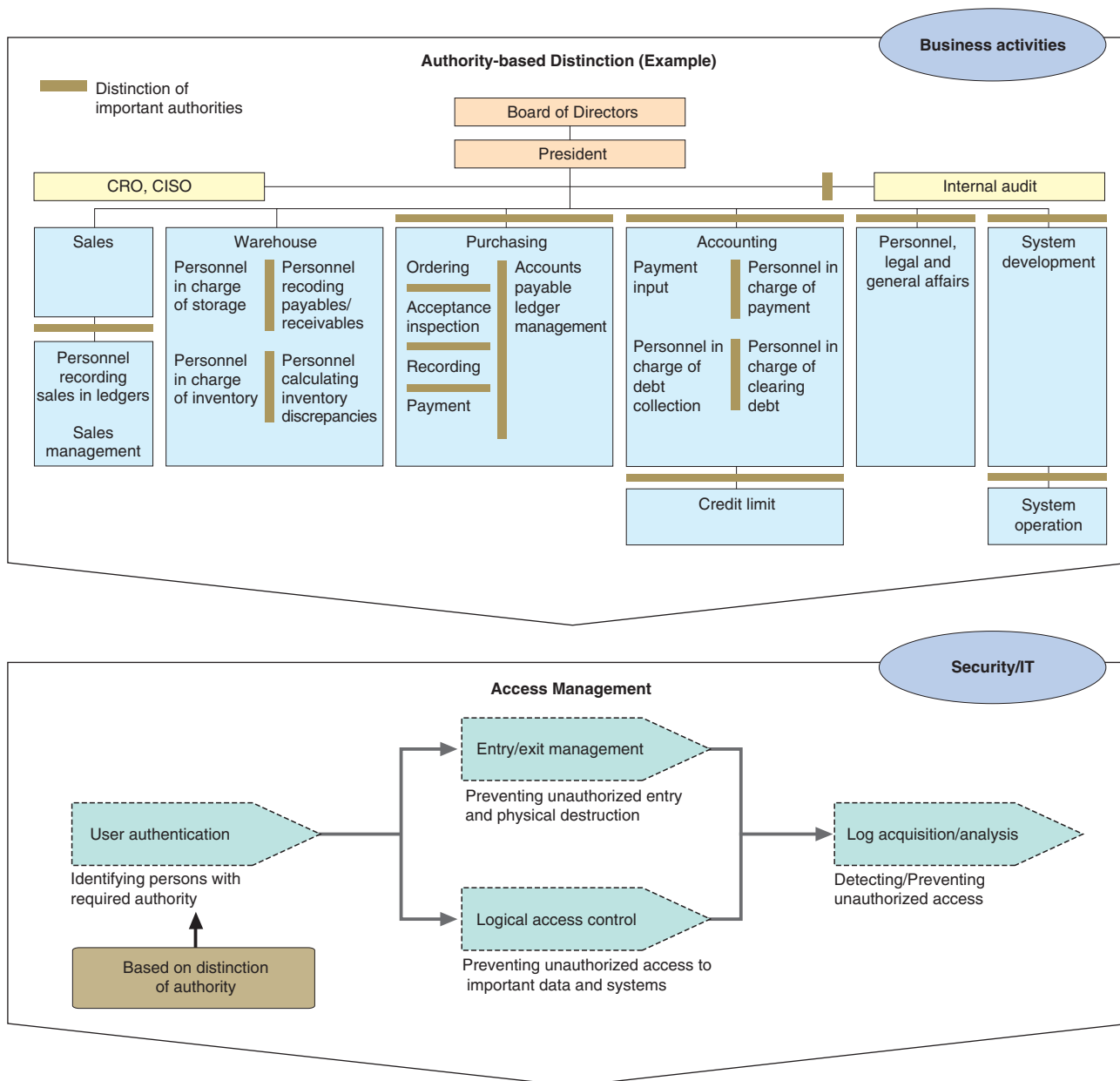
III Questionnaire Surveys Reveal Current Information Security Measures and Issues

Companies first really began to take information security seriously in April 2005, with the enforcement of the Personal Information Protection Act and the e-Documents Act. This latter act consists of two laws: "Act on the Use of Information and Communications Technology for the Storage, Etc. of Documents by Private Entities, Etc." and "Act on the Amendments, Etc. to Related Laws As Required by the Enforcement of the Act on the Use of Information and Communications Technology for the Storage, Etc. of Documents by Private Entities, Etc."

NRI Secure Technologies, Ltd. has been continuously conducting surveys to determine the extent to which companies and consumers are aware of information security. The trend that the results of these surveys suggest is that the increased awareness of information security nearly overlaps the increased opportunities of developing internal control systems (the Japanese version of the SOX Act, and the New Company Law that came into force in May 2006). This trend is seen as a major change for company management.

The following section provides a general view of the current status and issues related to overall IT control, as

Figure 2. Flow of Establishing Access Management System to Distinguish User Authority



Note: (1) CISO = chief information security officer, (2) CRO = chief risk management officer.

revealed by the data gained from the Report on the 2006 Survey on Information Security Status in Companies published in July 2006 (survey was conducted in May of the same year) and the Survey on Attitudes toward Information Security, which was aimed at businesspersons and conducted in November of the same year (Table 2).

1 Information Security Measures Adopted by Companies

Figure 3 shows the extent of conformity by companies with the laws and regulations related to information security.

The “already complied” responses were most common for the Personal Information Protection Act (81%),

while for other laws and regulations, there currently seems to be less urgency to conform.

When these surveys were conducted, the number of “already complied” responses for the Japanese version of the SOX Act was a mere 0.9 percent, with 16.4 percent stating that they “will comply during fiscal 2006.” If the proposed standards are implemented in fiscal 2007, the 71.8 percent of respondents who said that they were “studying their compliance” are expected to rapidly take measures to comply.

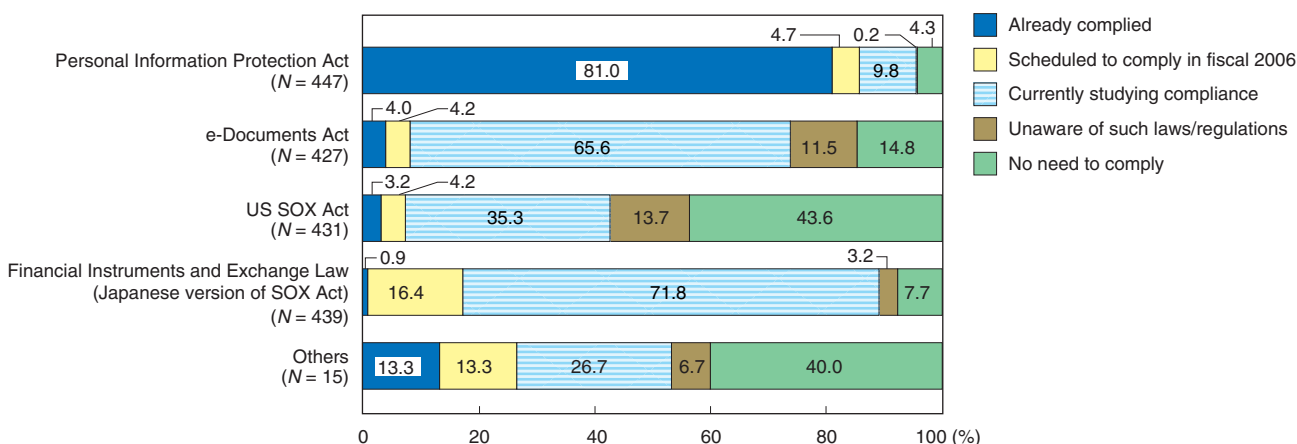
Figure 4 shows the results of a self-evaluation of the information security measures that companies already have in place.

This self-evaluation of information security measures overall elicited very few responses of “very confident.” Even after combining the responses of “very confident”

Table 2. Overview of Questionnaire Surveys Related to Information Security

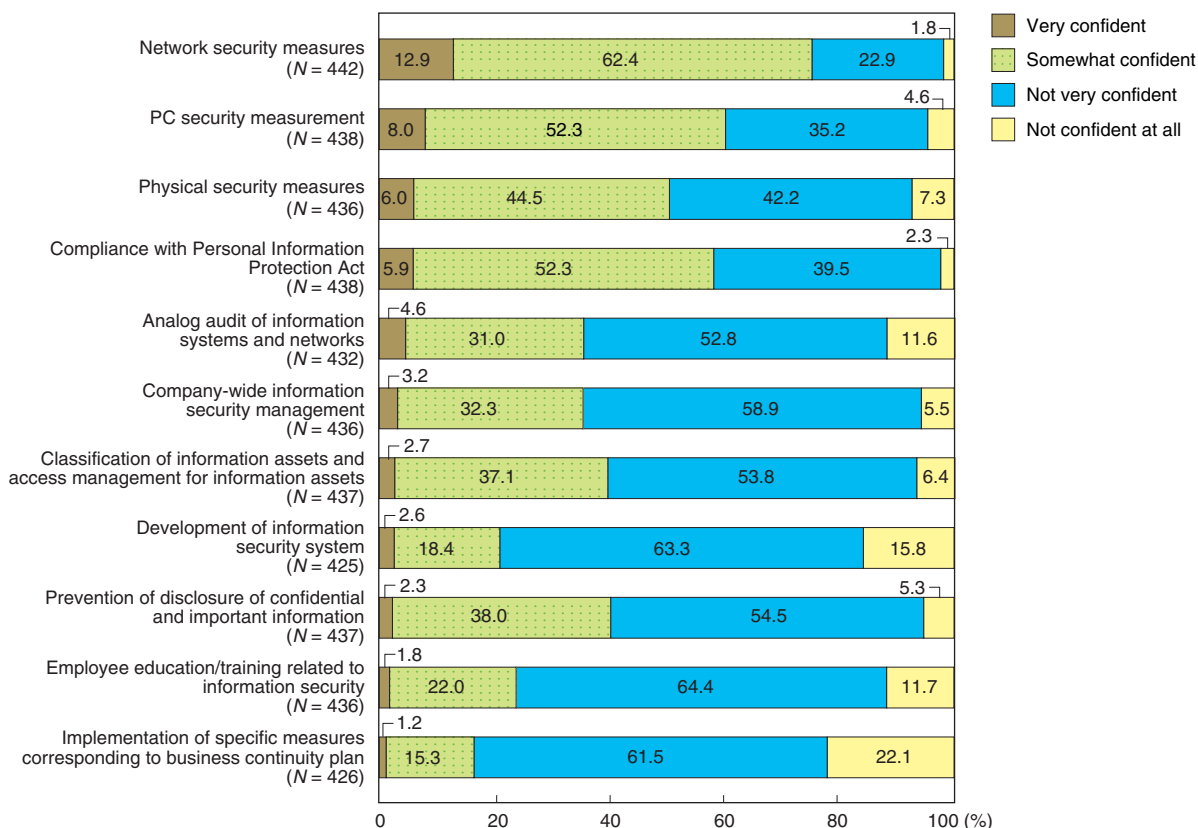
Survey on Information Security Status in Companies		Survey on Attitudes toward Information Security	
Survey period	May 15 – May 31, 2006	Survey period	November 17 – November 21, 2006
Survey method	Postal mail	Survey method	Web-based questionnaire
Target	Total of 3,001 companies consisting of those with 300 or more employees (listed on the 1st and 2nd Sections of the TSE, as well as unlisted companies) and those with fewer than 300 employees (listed on the 1st and 2nd Sections of the TSE)	Target	Business people (extracted by using their attributes from the responses obtained from the questionnaire targeting consumers)
Number of responses	449 companies	Number of responses	1,266 persons
Response rate	15.0%	Conducted by	Yahoo! Research

Figure 3. Compliance with Laws and Regulations Related to Information Security



Source: NRI Secure Technologies, "Survey on Information Security Status in Companies," May 2006.

Figure 4. Self-Evaluation of Information Security Measures Already in Place



Source: NRI Secure Technologies, "Survey on Information Security Status in Companies," May 2006.

and “somewhat confident,” we found that we had responses of “confident” exceeding 50 percent for only four items, namely, “network security measures” (75.3%), “PC security measures” (60.3%), “compliance with the Personal Information Protection Act” (58.2%) and “physical security measures” (50.5%).

Because many of these measures rely on technology-based control such as entry/exit management and network applications, they can be expected to produce some effects to ensure information security.

On the other hand, if we combine the responses of “not very confident” and “not confident at all,” we found that we had “not confident” responses for “implementation of specific measures corresponding to business continuity plans (BCP)” (83.6%), “development of information security systems” (79.1%) and “employee education/training related to information security” (76.1%).

Thus far, I have explained the significant role that information security measures play in developing overall IT control systems. In view of the current status of information security measures in companies, while technology-based management has been implemented, many companies responded that they were “not confident” in the restoration measures that were applied to incidents such as the occurrence of security-related problems or accidents, organizational management and human resource management (such as the development of information security systems and information security education). In comparison with technology-based measures, these measures probably need some time to take effect.

2 Information Security Management from the Perspective of Employees' Actions

Consequently, do no other major problems arise if companies have prepared in-house documents such as information security management regulations and security-related rules in order to establish internal controls?

To answer this question, we have conducted a survey aimed at businesspersons. Prior to this survey, there was very little data as to whether a company had documented rules on information security and, even when those rules were in place, the extent to which the employees observed the rules. Therefore, we targeted this Web-based survey at business people in order to gather responses to the above questions.

The results revealed that if a company merely creates in-house rules and then documents them, it is not possible to prove that internal control is being appropriately applied. This is where the fundamental difficulty with the establishment of internal controls lies.

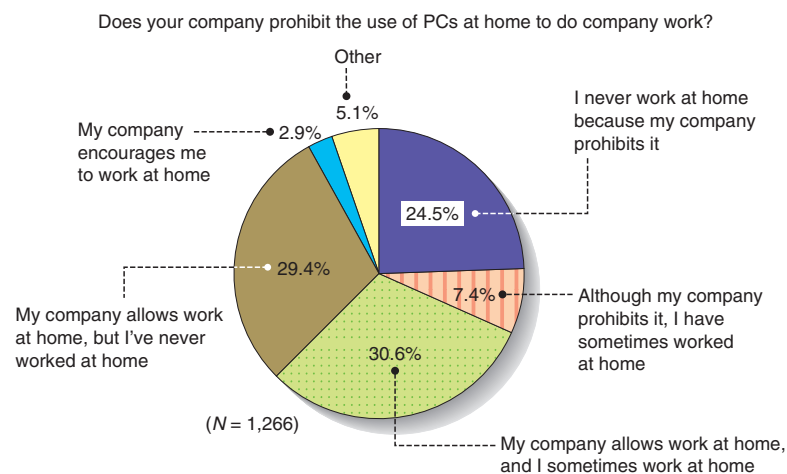
Figure 5 illustrates the responses that we obtained about “relationships between the use of a PC to do company work at home and compliance with company rules.” In response to this question, we found that 7.4 percent of the respondents still used PCs at home for work despite the existence of company rules prohibiting such use. In cases where there is no rule prohibiting the use of a PC to do company work at home, this figure rose to 30.6 percent of the respondents.

We find the responses to the former question extremely serious from the standpoint of establishing internal controls within a company because such attitudes may lead to greater risks of a company’s information being disclosed.

The responses to the question in the second case indicate that since the establishment of these rules is left to the discretion of individual companies, many companies do not have in-house rules in place. Such companies should recognize that they face the risk of connecting PCs owned by individual employees to the corporate network.

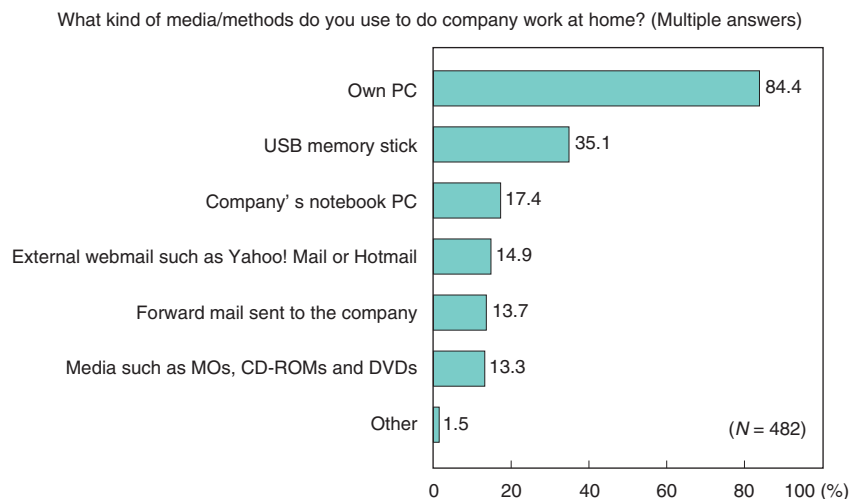
Figure 6 shows the responses received when those persons who “had used a PC at home for company work” were asked about the types of media and methods used to do such work. Among these, by far the largest proportion answered that they used their own (home) PC

Figure 5. Use of PCs at Home to Do Company Work and Compliance with Company Rules



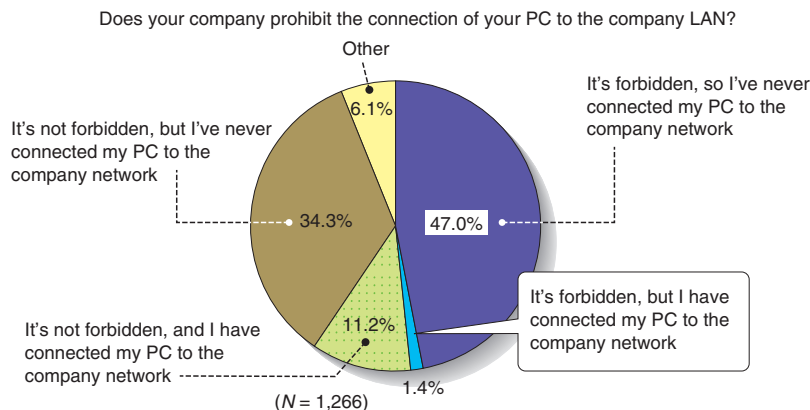
Source: NRI Secure Technologies, “Survey on Attitudes toward Information Security,” November 2006.

Figure 6. Media/Methods Used to Do Company Work at Home



Notes: (1) CD-ROM = compact disk-read only memory, (2) DVD = digital versatile disk, (3) MO = magneto optical disk, (4) USB = universal serial bus. Source: NRI Secure Technologies, "Survey on Attitudes toward Information Security," November 2006.

Figure 7. Rules Governing Connection to the Company LAN and Compliance with Those Rules



Note: LAN = local area network. Source: NRI Secure Technologies, "Survey on Attitudes toward Information Security," November 2006.

(84.4%), 35.1 percent used a USB memory stick to transport their work and 17.4 percent used their company notebook PC. Because a relatively large number use USB memory, if such media are not equipped with data security measures applied under a company's information security measures, such as data encryption or protected by authentication based on biometrics such as fingerprint, it is clear that the use of these types of media presents a major risk of data leakage.

Figure 7 shows the responses obtained when we asked whether people had connected their own notebook PC to their company's LAN (local area network), despite the existence of a rule that specifically prohibits such connection.

For this question also, we found that 1.4 percent responded with "even though connecting my own PC is prohibited, I have in fact done this." If a PC that is infected with a virus is brought into the company and connected to the corporate network, there is an extremely high risk of that virus spreading to other PCs on the network and/or of data being disclosed as a result. In

those companies where unauthorized access to the corporate network is prohibited, there is a need for employee training to stress the importance of observing these rules.

Furthermore, to minimize the consequences of human error from the perspective of information security management, it is important to adopt technology-based measures (for example, preventing the use of unauthorized PCs on the network, introducing a quarantine network, etc.) in establishing internal controls.

We are still seeing cases where, despite the establishment of in-house information security rules, employees take their notebook PCs out of the company in defiance of the rules, after which the PCs are stolen or data was disclosed. Therefore, it is a matter of urgency for every company to place the highest priority on ensuring that all of its employees are well aware of the importance of information security.

The results of these surveys have made us realize that, from the perspective of information security, there are loopholes in internal controls in the IT field, such as the

potential risk of the disclosure of data through employee actions.

IV Toward Establishing Efficient Internal Controls through the Use of Information Security

From the perspective of the management of a company, in many cases, internal control systems are developed for the purposes of abiding by laws and regulations and maintaining the social reliability of a company. However, these measures place an enormous burden on the front-line departments.

When there is a need to ensure accurate financial information as specified under the Japanese version of the SOX Act, data integrity is required. Therefore, it is important to be able to detect the use of an incorrect procedure, if one is inadvertently applied.

When considering internal controls from the perspective of information security, I believe that it is particu-

larly important to ensure integrity such as by providing a function to support the distinction of persons with the required authority (access management, for example).

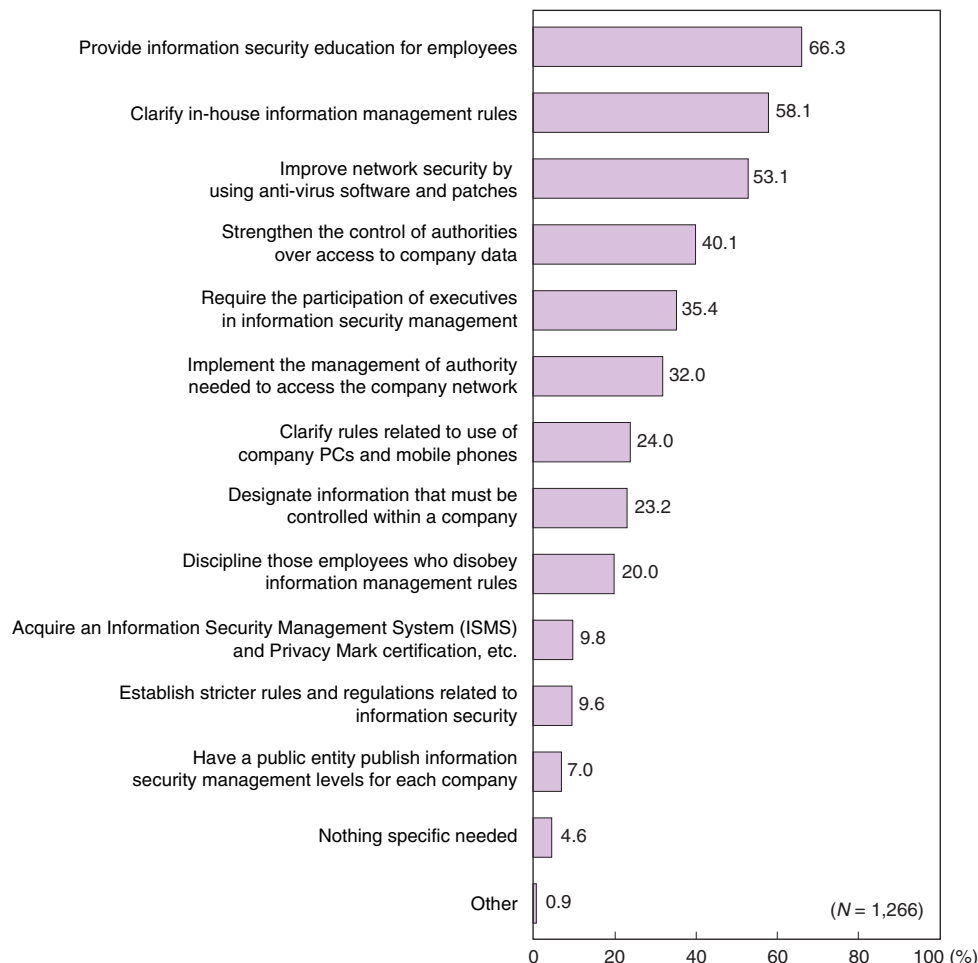
To conclude this paper, I would like to introduce the data obtained from a survey on businesspersons' attitudes toward "measures for fully implementing information management in a company" (Figure 8).

As "measures for fully implementing information management in a company," we found that the most common were "implementation of information security training for employees" (66.3%), "clarification of in-house information management rules" (58.1%) and "enhancement of network security through the application of anti-virus software and patches" (53.1%). Subsequent to these were "strengthening the control of authorities over access to company data" (40.1%) and "participation of management executives in information security management" (35.4%). Of course, all of these items are indispensable in developing a company's appropriate internal control system.

In fiscal 2007, I believe that there will be a rush to apply the measures required under the Japanese version of the SOX Act. As mentioned in the previous section,

Figure 8. Measures for Fully Implementing Information Management in a Company

What kind of measures do you think should be adopted to fully implement information management in your company? Select 5 items that most closely indicate your thoughts (Multiple answers).



Source: NRI Secure Technologies, "Survey on Attitudes toward Information Security," November 2006.

the guidelines indicated in the exposure draft take a position that facilitates the use of IT according to the actual situation of each company. Internal controls established under the Japanese version of the SOX Act include an evaluation process after internal controls are implemented. If this evaluation reveals that the company-wide internal controls are satisfactory, the law also states that the business sites that must be evaluated can be reduced, also enabling a company to reduce the workload related to evaluation.

Because only management is in a position where it can review company-wide rules, facilitate a reform in the attitudes of employees and all related persons, incorporate such rules into all business activities and establish a company-wide system, management executives must be very active in educating company employees about information security and preventing the disclosure of personal and confidential information.

In particular, to deal with those employees who choose to ignore company rules, it is necessary to change the

way of thinking and consider such ignorance as a known condition in adopting appropriate measures.

In this sense, there will also be an even greater need for positive participation by management executives and their taking responsibility for developing an internal control system within a company with respect to activities to reform employee attitudes to facilitate compliance with company rules and to introduce tools to minimize the risks caused by employee errors or malicious behavior (such as introducing quarantine networks and so-called “thin clients” (PCs with no built-in memory or storage devices)).

Keiichi HIMENO is a senior security consultant and P.E.Jp (Industrial Engineering, Comprehensive Technical Management) of the Consulting Department, NRI Secure Technologies, Ltd. His specialties include technology evaluation management and risk management in the information security field.

As a leading think tank and system integrator in Japan, Nomura Research Institute is opening new perspectives for the social paradigm by creating intellectual property for the benefit of all industries. NRI's services cover both public and private sectors around the world through knowledge creation and integration in the three creative spheres: "Research and Consulting," "Knowledge Solutions" and "Systems Solutions."

The world economy is facing thorough structural changes led by the dramatic growth of IT industries and the rapid expansion of worldwide Internet usage—the challenges of which require new concepts and improvement of current systems. NRI devotes all its efforts to equipping its clients with business strategies for success by providing the best in knowledge resources and solutions.

NRI Papers present selected works of NRI's 3,000 professionals through its worldwide research network. The mission of *NRI Papers* is to contribute new ideas and insights into business management and future policy planning, which are indispensable for overcoming obstacles to the structural changes in our society.

All copyrights to *NRI Papers* are reserved by NRI. No part of this publication may be reproduced in any form without the prior written consent of NRI.

Inquiries to: Corporate Communications Department
Nomura Research Institute, Ltd.
E-mail: nri-papers@nri.co.jp
FAX: +81-3-6660-8373