II. Research for Strengthening Information Security in the Business Sector

1. Promotion of Information Security to Support Investment in ASEAN and East Asia

1.1. Survey on Overseas Investment Intention and Information Security in Japan

1.1.1. Background and Purpose of the Survey

In recent years, overseas trade and investment (investment in overseas companies, local subsidiaries and their clients, outsourcing, etc.) by Japanese companies has been growing. Meanwhile, problems with information security by overseas trade clients and investment destinations have been reported. There is concern that the delay in responding to these problems may lead to barriers against overseas investment and business promotion in the future.

The Survey on Information Security in Overseas Trade and Investment was conducted with listed Japanese companies to understand the policies and responses to information security risks by overseas trade clients and the investment destinations of Japanese companies. These results were utilized to ascertain foreseeable appropriate information security environment at these overseas companies in the future.

This survey was conducted in part as a commissioned project from the Ministry of Economy, Trade and Industry in Japan but was conducted in close cooperation with the WG. Part of the results of this survey was reported in the first workshop as a contribution from Japan.

1.1.2. Survey Method and Subjects

The survey was conducted as shown in Table 1.1. All the companies listed on the first and second sections of the Tokyo, Osaka, and Nagoya Stock Exchanges (about 2,454 companies, duplications eliminated) were selected based on the *Japan Company Handbook 2009* (Toyo Keizai).

Table 1.1. Overview of the Survey

Target	Companies: Companies listed in the first or second section that make foreign investments (investments in overseas companies, establishment of joint ventures, overall transactions with overseas subsidiaries and their clients, and procurement from or outsourcing to overseas companies) Respondents: Persons in charge of general affairs departments, procurement departments, and information security departments who confirm, manage, and supervise the information security measures at overseas trade clients and investment destinations.
Period	Dec. 7, 2009 to Jan. 8, 2010
Supported by	MRI Research Associates, Inc.
Method	Mail survey
Number of distributed questionnaires	2,454 companies
Recovery rate	234 companies (recovery rate 9.5%)

The survey was conducted mainly on the following items.

- Impact of information security environment of overseas trade clients and overseas investment destinations on the intention to trade and the motivation to invest

- Items to value as information security measures of overseas trade clients and overseas investment destinations
- Measures to improve the information security environment of overseas trade clients and overseas investment destinations

1.1.3. Attributes of the Respondent Companies

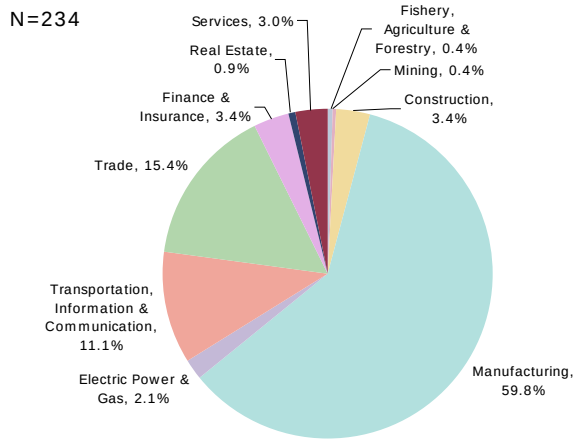
The number of effective responses to the survey was 234 (as of January 8, 2010). The following shows the attributes of the respondents.

(1) Industry Sectors of the Respondent Companies

The largest industry sector[6] of the respondent companies is manufacturing (59.8%), followed by trade (15.4%) and transportation, information, and communication (11.1%).

[6] We used the major industry classification defined by the Securities Identification Code Committee for the industry sectors in this survey. The classification is also used in the *Japan Company Handbook*. In subsequent analyses, manufacturing (only the manufacturing industry N = 140) and nonmanufacturing (all except the manufacturing industry N = 94) are mainly used for the classification, considering variations in the number of companies in each sector.

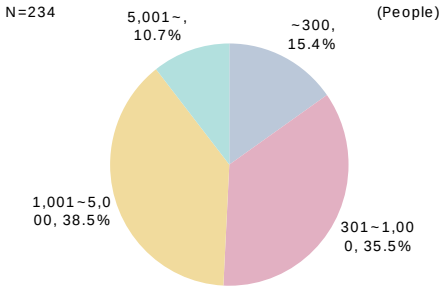
Figure 1.1. Industry Sectors of the Respondent Companies



(2) Number of Employees in the Respondent Companies

Nearly 85% of the respondent companies have 300 or more employees because listed companies were surveyed.

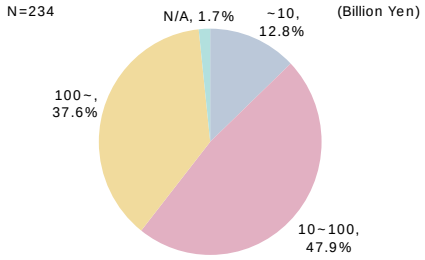
Figure 1.2. Number of Employees in the Respondent Companies



(3) Sales of the Respondent Companies

The sales amount exceeds 10 billion yen in 85% of the respondent companies and 100 billion yen in 37.6% of them.

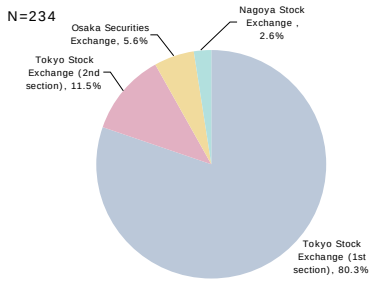
Figure 1.3. Sales Amounts of the Respondent Companies



(4) Stock Exchanges Where the Respondent Companies Are Listed

Eighty percent or more of the respondent companies are listed on the first section of the Tokyo Stock Exchange.

Figure 1.4. Stock Exchanges Where the Respondent Companies are Listed



1.1.4. Main Results of the Survey

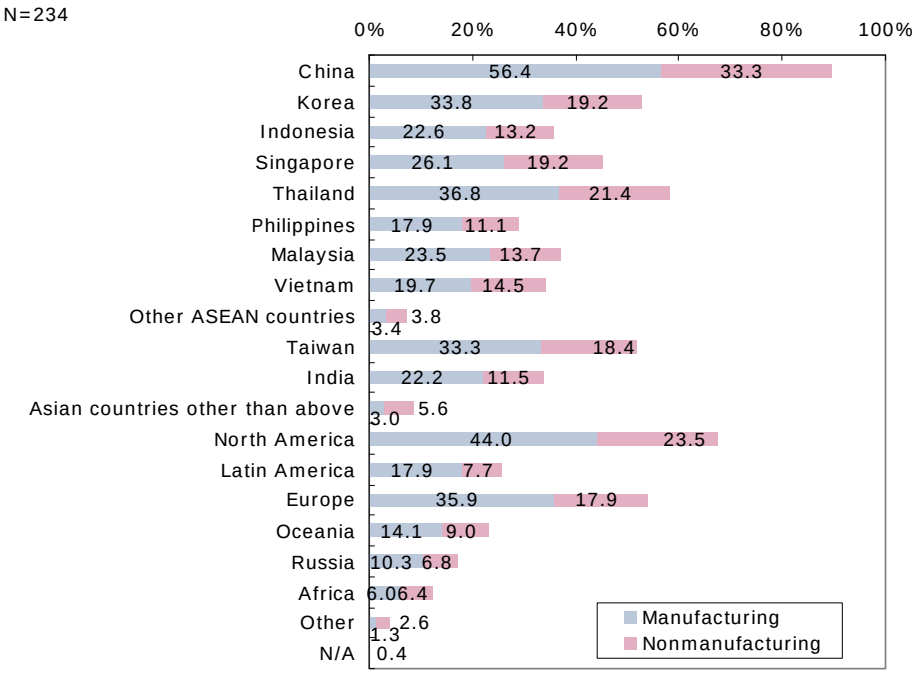
(1) Status of Overseas Trade and Investment by the Respondent Companies

a) Major Countries and Regions for Overseas Trade and Investment

The respondent companies are engaged in trade and make investments in Asia more than other regions. Nearly 90% of the respondent companies are involved in trade or investments in China, and 50% or more of them belong to the manufacturing sector.

South Korea, Thailand, and Taiwan are also major partners in Asia.

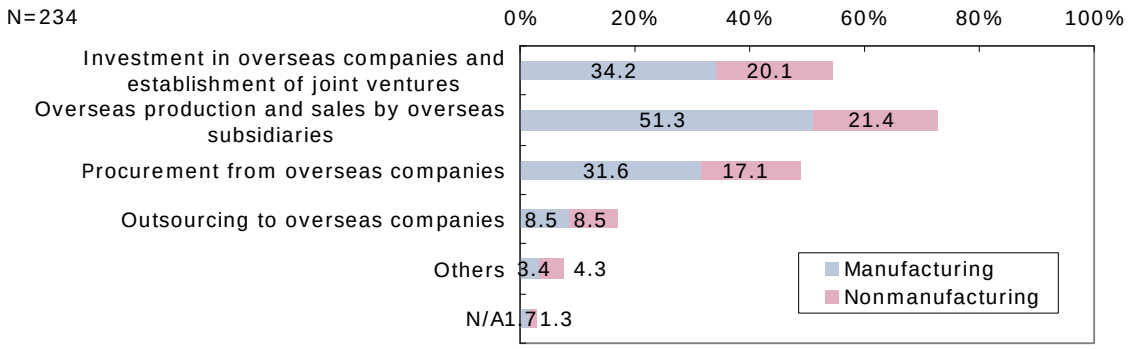
Figure 1.5. Major Countries and Regions for Overseas Trade and Investment



b) Types of Overseas Trade and Investment

"Overseas production and sales by overseas subsidiaries" is the most common type of overseas trade and investment (72.7%), especially in the manufacturing industry. "Outsourcing to overseas companies" is less common than other types, but equal in size in the two sectors.

Figure 1.6. Types of Overseas Trade and Investment



(2) Policy for Decisions on Overseas Trade and Investment

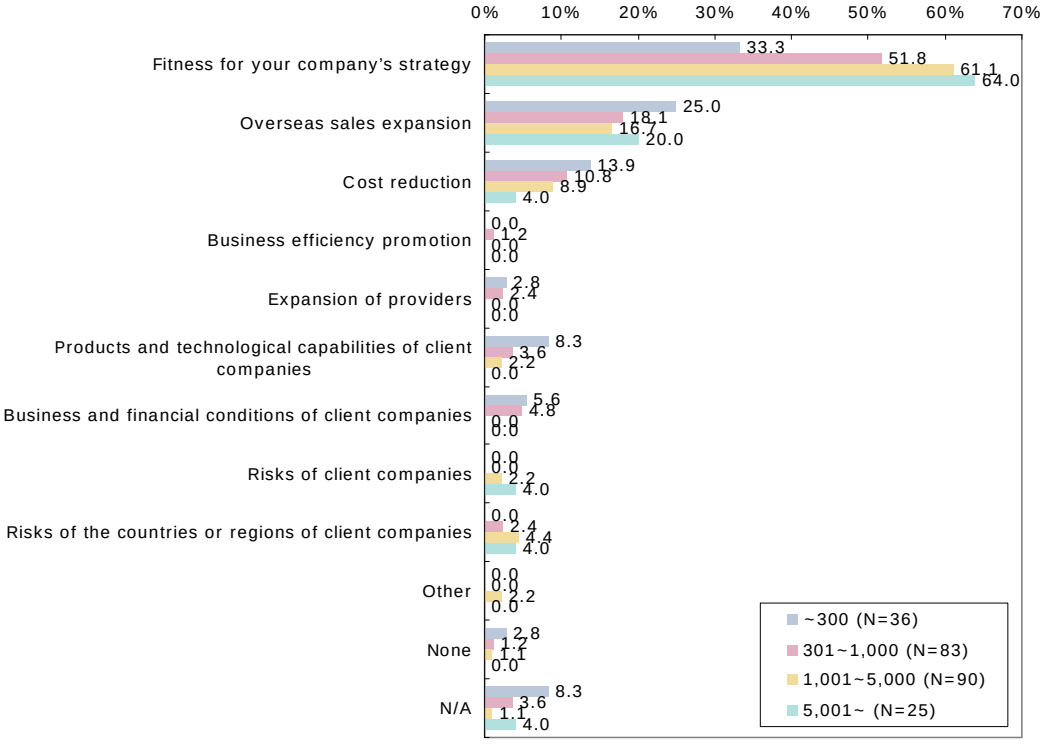
a) Major Considerations in Decisions on Overseas Trade and Investment

The respondent companies place highest priority on suitability to the company's strategy in decisions on overseas trade and investment. The tendency is stronger in companies with a large workforce, i.e., large-scale companies. Sixty-four percent of companies with 5,001 or more employees chose this item as the most important consideration.

Meanwhile, smaller-scale companies think much of overseas sales expansion. Twenty-five percent of companies with 300 or fewer employees chose this item as the most important consideration.

Overseas expansion by Japanese companies is often part of their business strategies. Large companies particularly attach great importance to this strategic aspect. Meanwhile, many small to medium companies give priority to sales expansion.

Figure 1.7. Major Considerations in Decisions on Overseas Trade and Investment (by Number of Employees)



b) Implementation of Risk Analysis in Decisions on Overseas Trade and Investment

Eighty percent or more of the respondent companies perform risk analysis in decisions on overseas trade and investment. The larger the company, the more likely it implements risk analysis. Among companies with 300 or fewer employees, 66.7% implement risk analysis, while the rate is 100% for companies with 5,001 or more employees.

The rate is 87.1% in the manufacturing industry and 78.1% in the nonmanufacturing industry. (We did not analyze by sector in detail because of the small number of companies in some sectors. See Figure 1.1. for reference.)

Figure 1.8. Implementation of Risk Analysis in Decisions on Overseas Trade and Investment (by Number of Employees)

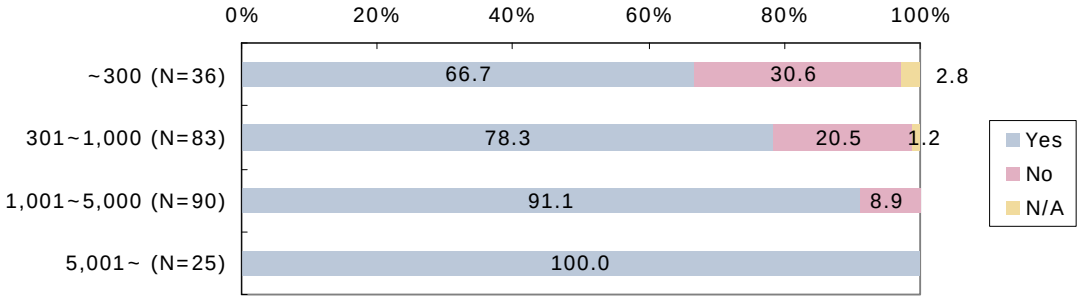


Figure 1.9. Implementation of Risk Analysis in Decisions on Overseas Trade and Investment (by Sector)

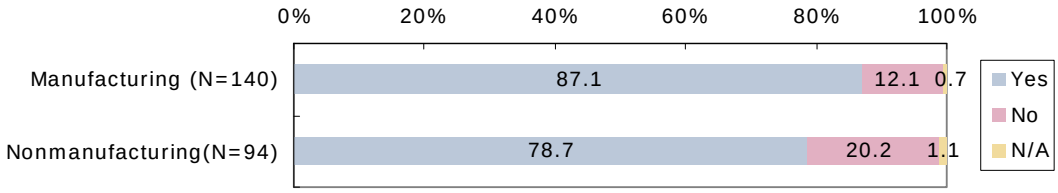
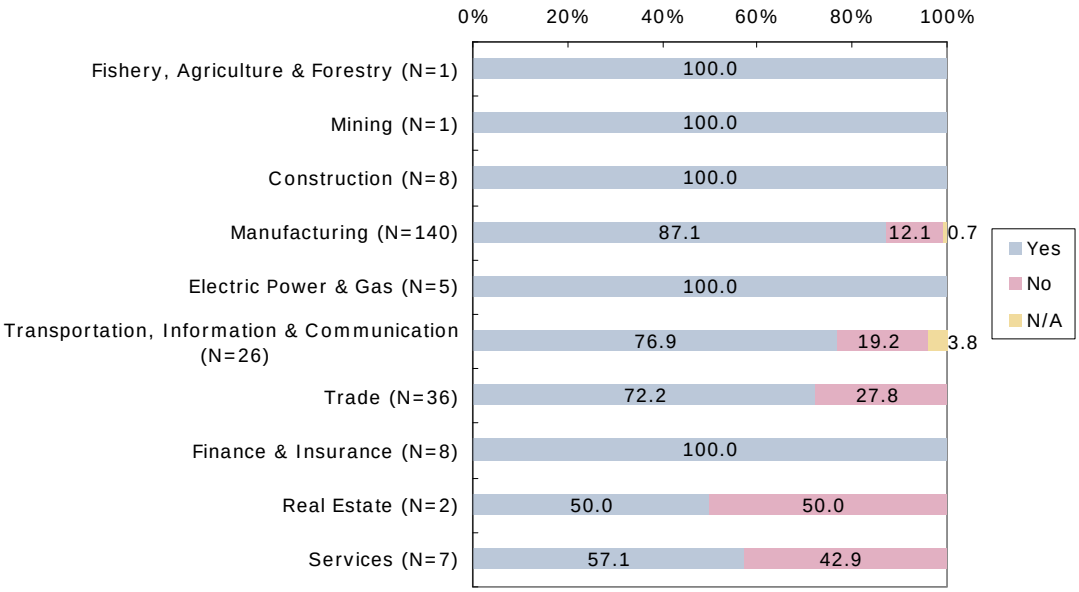


Figure 1.10. (Reference) Implementation of Risk Analysis in Decisions on Overseas Trade and Investment (by Business)



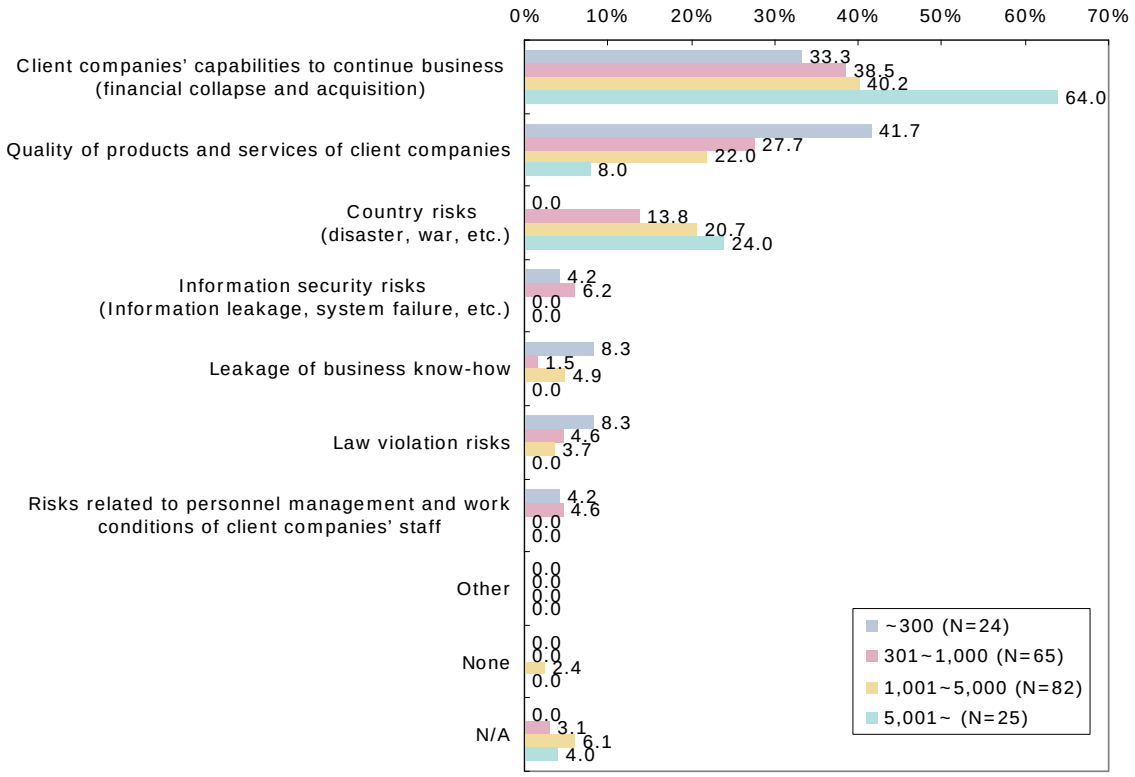
c) Risks Considered in Decisions on Overseas Trade and Investment

Here, we asked the companies that responded that they "perform risk analysis" in (2) about the most serious risk in making decisions on overseas trade and investment. The most serious risk for companies with 5,001 or more employees is "client companies' capabilities to continue business (financial collapse, acquisition, etc.) (64.0%). On the other hand, companies with 300 or fewer employees worry most about the "quality of products and services of client companies" (41.7%). Serious risks differ significantly depending on company size.

The results at (1) show that large companies often expand overseas as part of their business strategies. They give top priority to the business continuity of client companies to achieve their strategic goals. On the other hand, small and medium-sized

companies often expand overseas for greater profit rather than for their strategies. They think that the quality of risk of products and services is more important because it links directly to profit.

Figure 1.11. Risks Considered in Decisions on Overseas Trade and Investment



d) Presence of Global and Uniform Standards or Policies about the Information Security Risk in Overseas Trade and Investment

In the same way, we asked the companies that responded and "perform risk analysis" in (2) whether they have global and uniform standards or a policy about the information security risk in overseas trade and investment. The larger the company, the more likely it has standards or a policy. While 16.7% of companies with 300 or

fewer employees have standards, the rate rises to 48.0% for companies with 5,001 or more employees.

The ownership ratio is similar between the manufacturing industry (28.7%) and the nonmanufacturing industry (25.7%). For reference, in detailed classification, the ownership rate is higher in sectors such as financial and insurance (50.0%), construction (37.5%), and transportation, information, and telecommunications (35.0%) than manufacturing.

Figure 1.12. Presence of Global and Uniform Standards or Policies about the Information Security Risk in Overseas Trade and Investment (by Number of Employees)

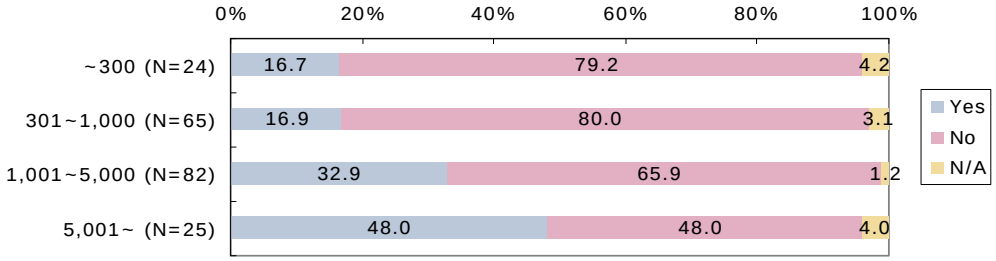


Figure 1.13. Presence of Global and Uniform Standards or Policies about the Information Security Risk (by Industry Sector)

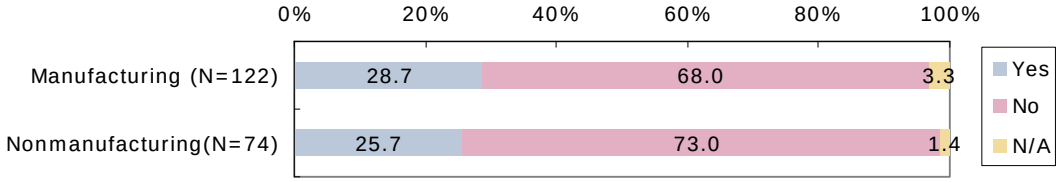
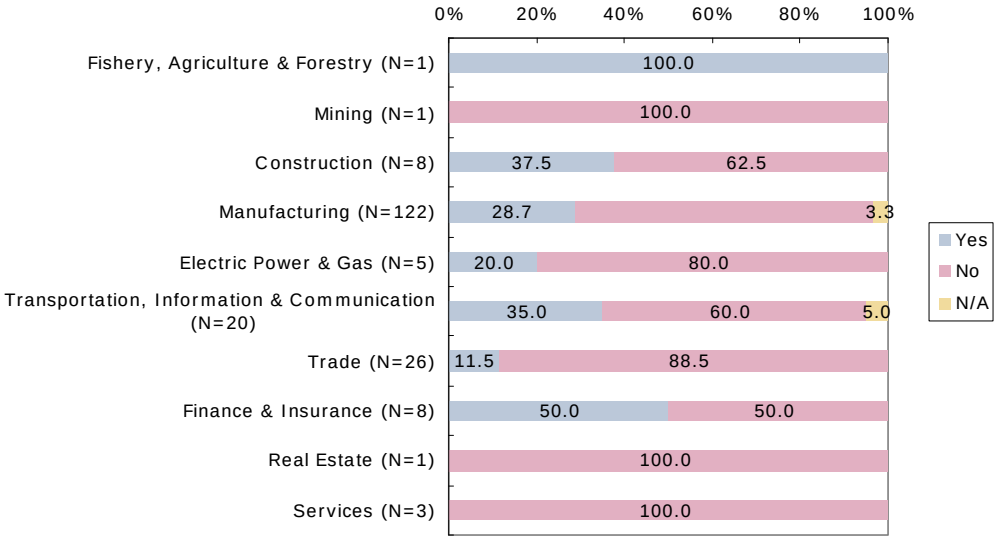


Figure 1.14. (Reference) Presence of Global and Uniform Standards or Policies about the Information Security Risk (by Business)



(3) Important Factors in the Information Security Environment of Overseas Trade Clients and Investment Destinations

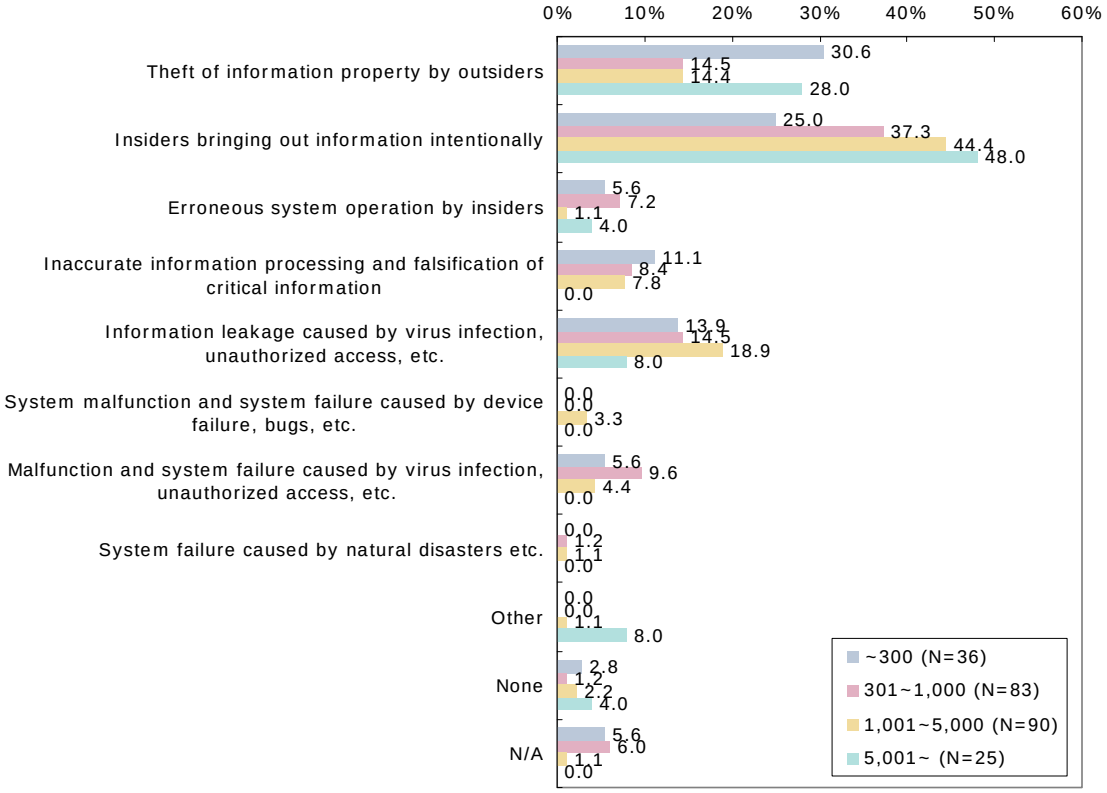
a) The Most Serious Information Security Risk at Client Companies

The greatest information security risk at client companies is "insiders bringing out information intentionally". The item was selected more often with the increase in company size, 48% for companies with 5,001 or more employees. On the other hand, "theft of information property by outsiders" was selected by 28.0% of companies with 5,001 or more employees and 30.6% of companies with 300 or fewer employees. In spite of these relatively high rates, in middle-sized companies with 300 to 5,000 employees, it is not highly recognized as a serious risk.

Because internal dishonesty cannot be prevented simply with technical measures for information security, large companies think it is a serious problem in spite of their

comparatively strong information security measures.

Figure 1.15. The Most Serious Information Security Risk at Client Companies



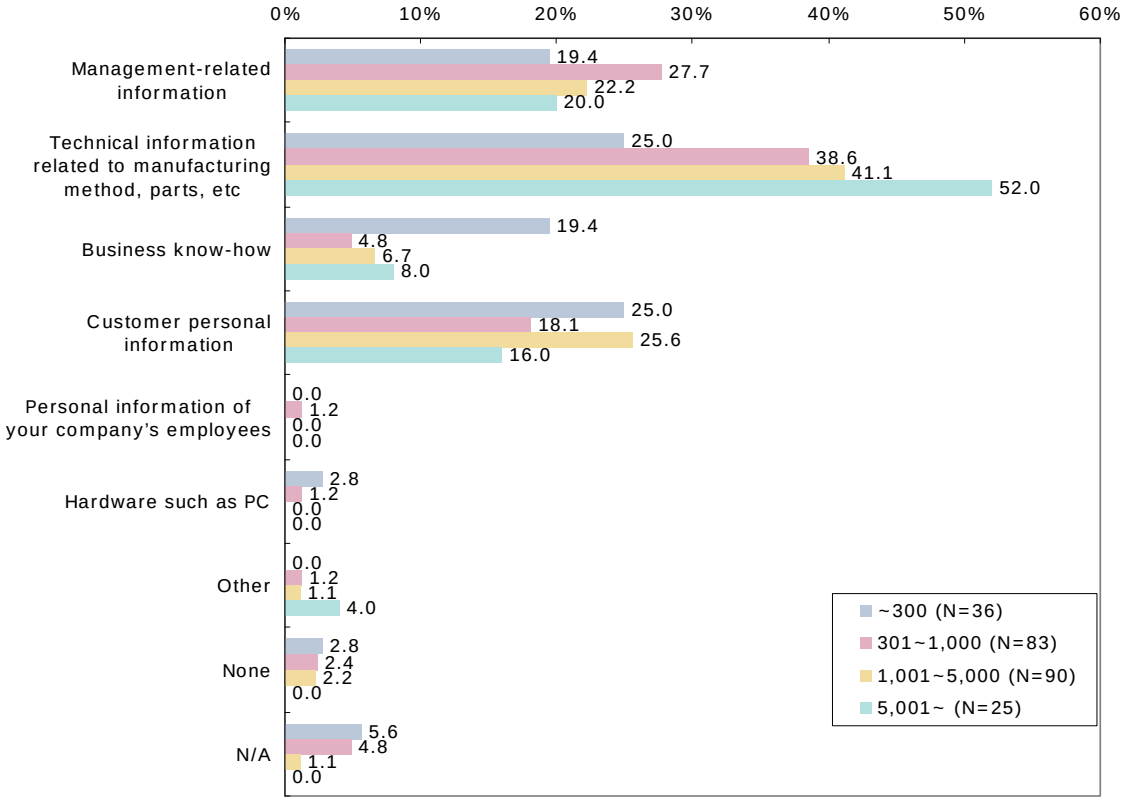
b) Properties to Protect with Information Security Measures at Client Companies

"Technical information related to manufacturing methods, parts, etc." is the most selected item as the properties that the respondent companies want to protect with information security measures at client companies. The need for protection increases with company size. This item was selected by 52.0% of companies with 5,001 or more employees.

"Business know-how" was selected by 19.4% of companies with 300 or fewer employees, which place a higher priority on the item than other companies.

As a whole, protection of technical information owned by Japanese companies is considered equally important. The results show that small and medium-sized companies have accumulated technical information as know-how.

Figure 1.16. Property to Protect with Information Security Measures at Client Companies

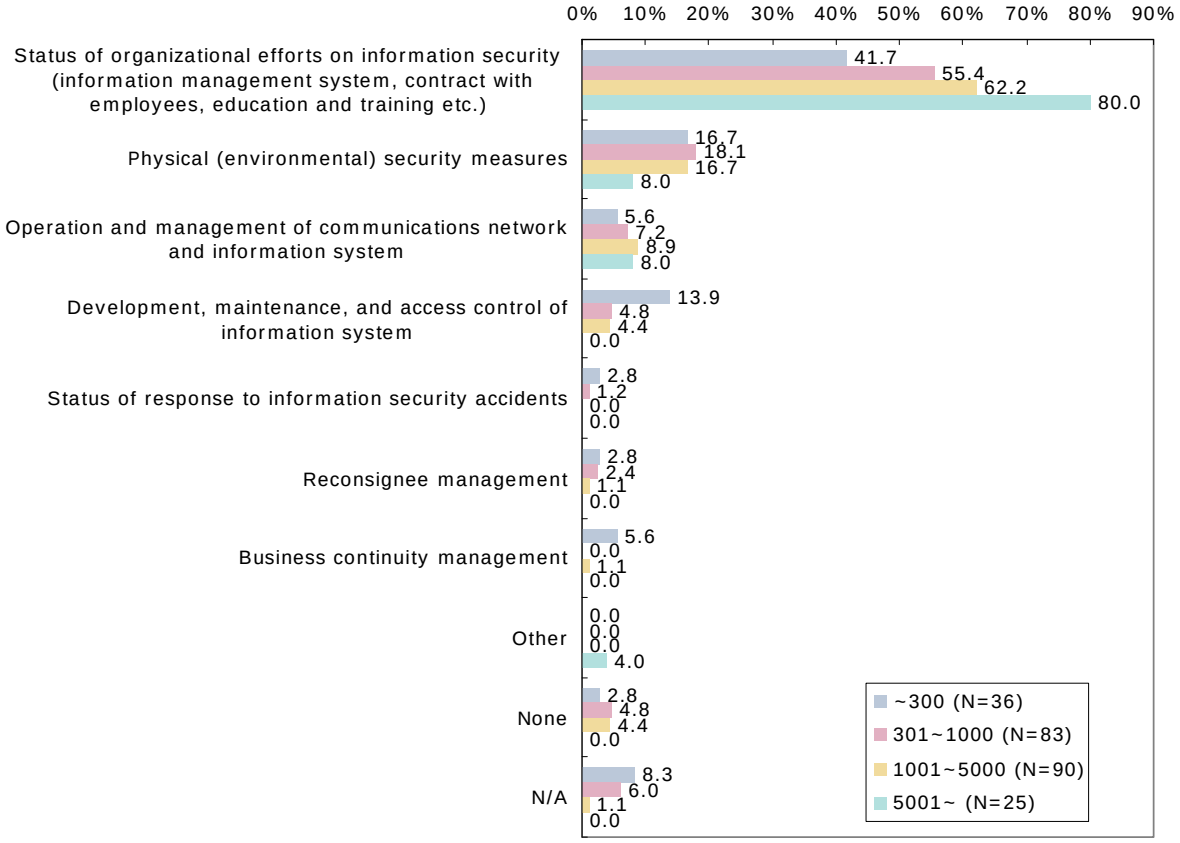


c) The Most Important Information Security Measures at Client Companies

"Organizational efforts on information security (information management system, contract with employees, education, and training)" were selected most often as the most important information security measures at client companies. The feature was selected by 80% or more of companies with 5,001 or more employees. Mistakes and

dishonesty by insiders were mentioned as serious information security risks at (1). They cannot be prevented simply with technical measures. Because organizational efforts clearly reflect the attitude of a company toward information security, they draw much attention from companies that make investment decisions.

Figure 1.17. Important Information Security Measures at Client Companies

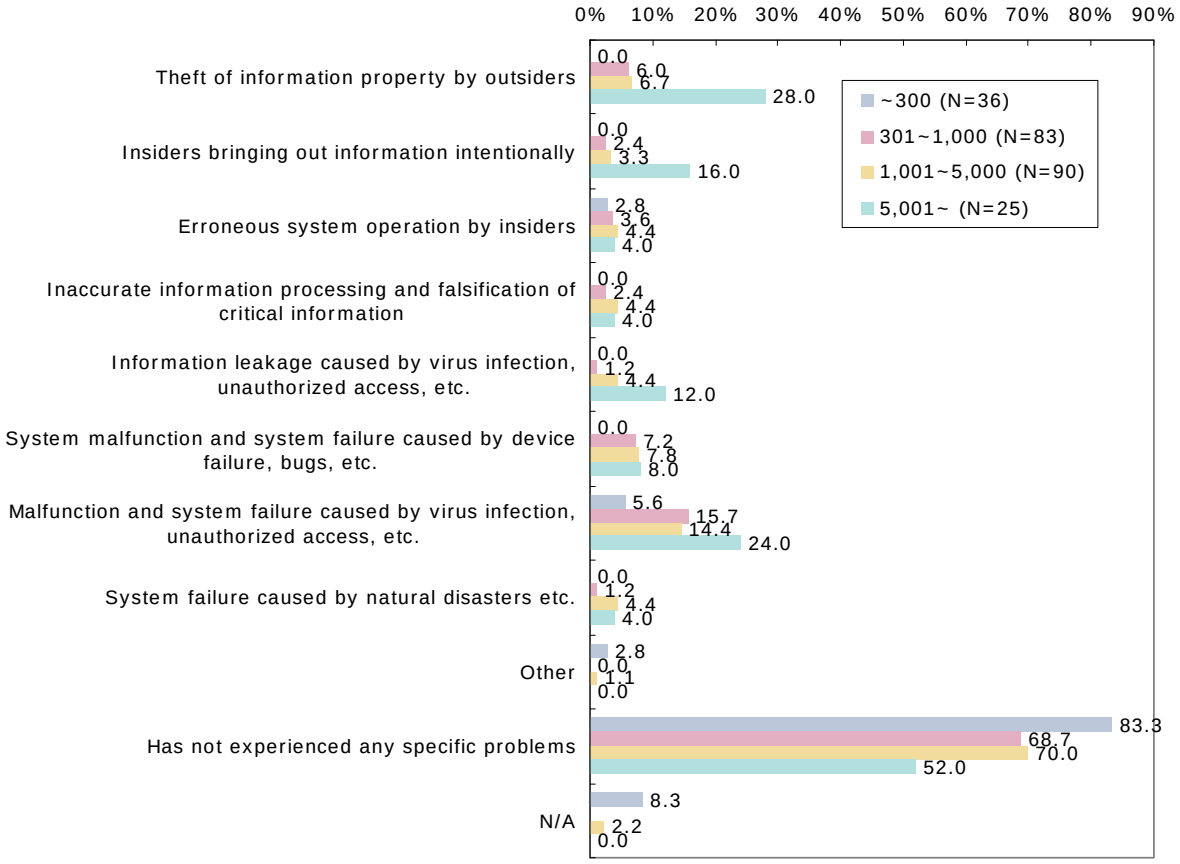


(4) Information Security Problems of Overseas Trade Clients and Investment Destinations

Most of the respondent companies answered that they have experienced no information security problems at overseas trade clients and investment destinations.

Some companies with 5,001 or more employees have experienced "theft of information property by outsiders" (28.0%) and "malfunction and system failure caused by virus infection, unauthorized access, etc." (24.0%). Experience with these problems may lead to greater awareness of information security risks.

Figure 1.18. Experience of Information Security Problems at Overseas Trade Clients and Investment Destinations



(5) Confirmation of Information Security Measures at Client Companies

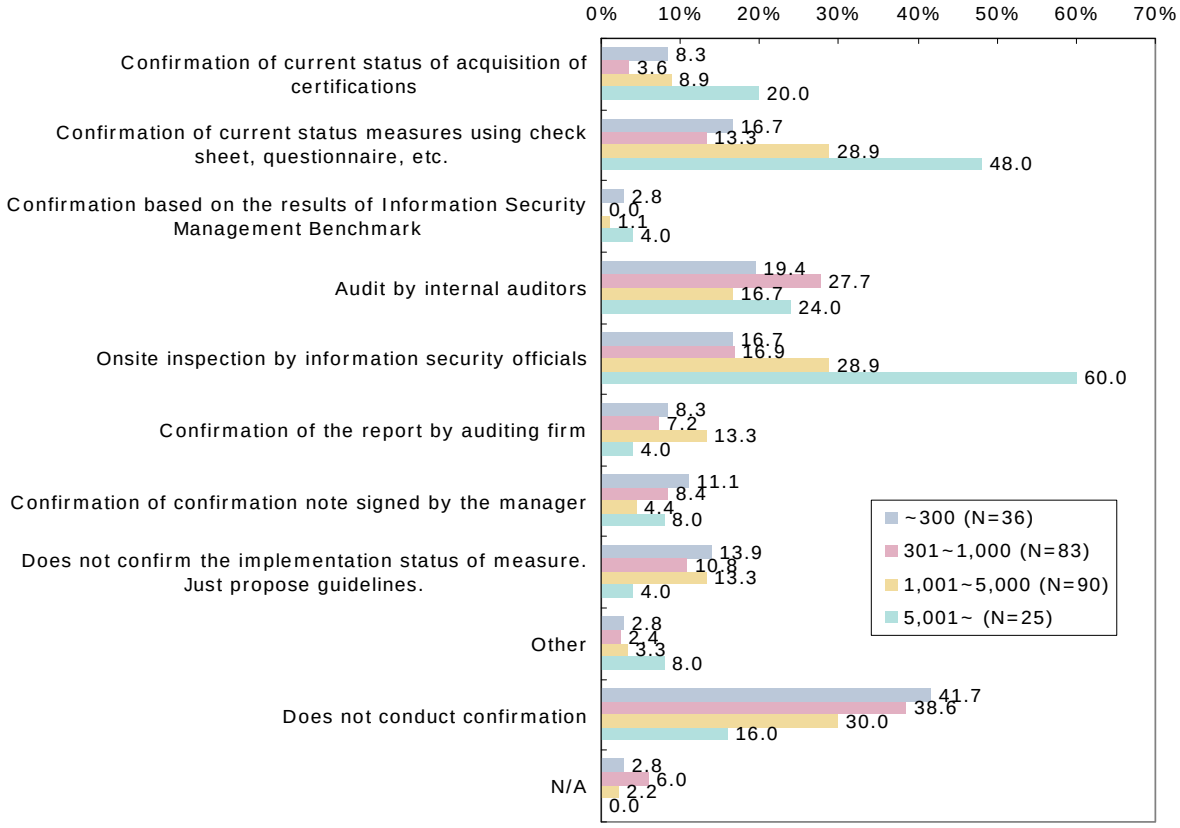
a) Confirmation of Information Security Measures at Client Companies

All kinds of methods are used to confirm the information security measures at client

companies. Companies with 5,001 or more employees often conduct "onsite inspection by information security officials" (60.0%) and "confirmation of current measures using check sheets, questionnaires, etc." (48.0%).

Companies with 300 or fewer employees most often "do not confirm the implementation status of measure, just propose guidelines" (41.7%). The attitude toward confirmation of information security measures and the resources for the confirmation are largely different depending on company size.

Figure 1.19. Confirmation of Information Security Measures at Client Companies

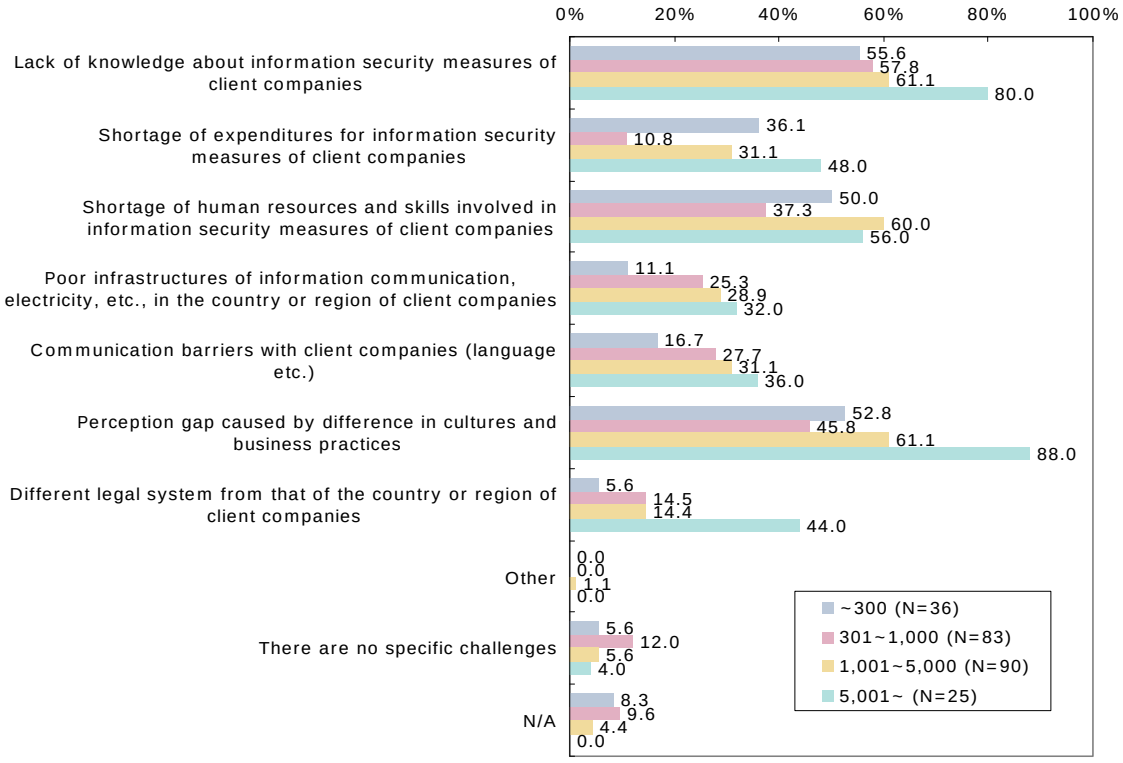


(6) Improvement of Information Security Environment at Client Companies

a) Challenges to Improvement of Information Security Environment at Client Companies

"Communication barriers with client companies (language etc.)" and "lack of knowledge about information security measures of client companies" are often selected as challenges to improvement of information security environment at client companies, particularly by 80% or more of companies with 5,001 or more employees. They also recognize a "different legal system from that of the country or region of client companies" as a challenge than other companies. This shows that the situations specific to a country or region hinder information security measures.

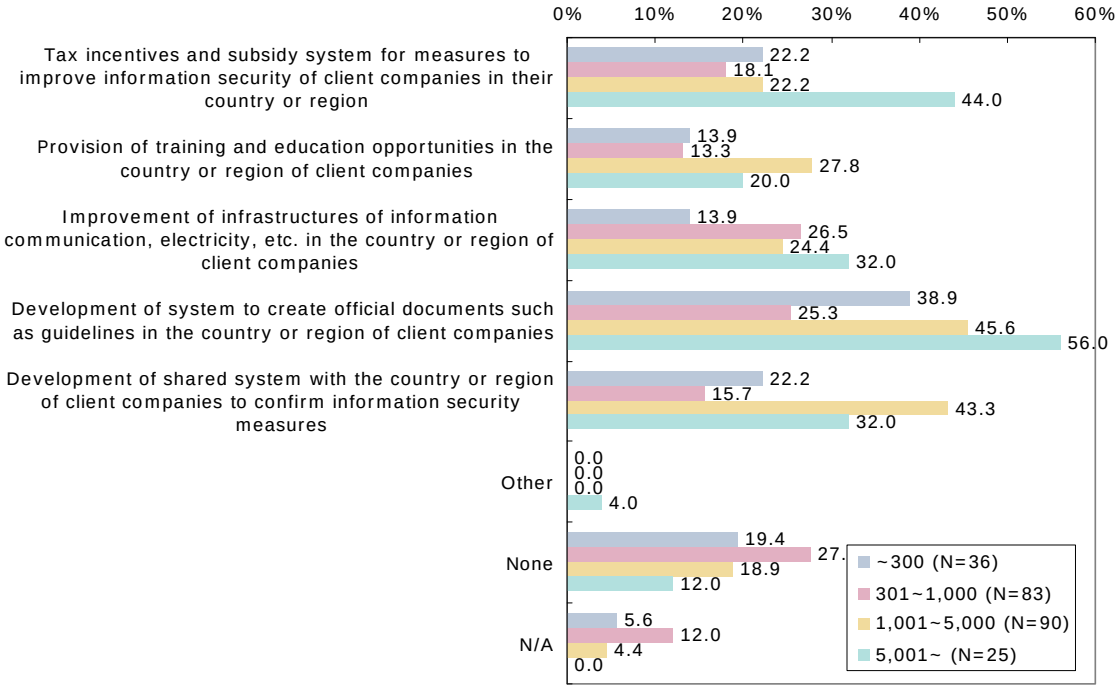
Figure 1.20. Challenges to Improvement of Information Security Environment at Client Companies



b) Requests of the Government for Improvement in the Information Security Environment in Overseas Trade and Investment

Requests of the government for improvement in the information security environment for overseas trade and investment differ depending on company size. Many companies with 5,001 or more employees request "development of a system to create official documents such as guidelines" (56.0%) and "tax incentives and a subsidy for measures to improve information security of client companies in their country or region" (44.0%). Middle-sized companies with 1,000 to 5,000 employees request "development of a system to create official documents such as guidelines" (45.6%) and "development of a shared system with the country or region of client companies to confirm information security measures" (43.3%). On the other hand, fewer requests were made by companies with 300 or fewer employees than other companies.

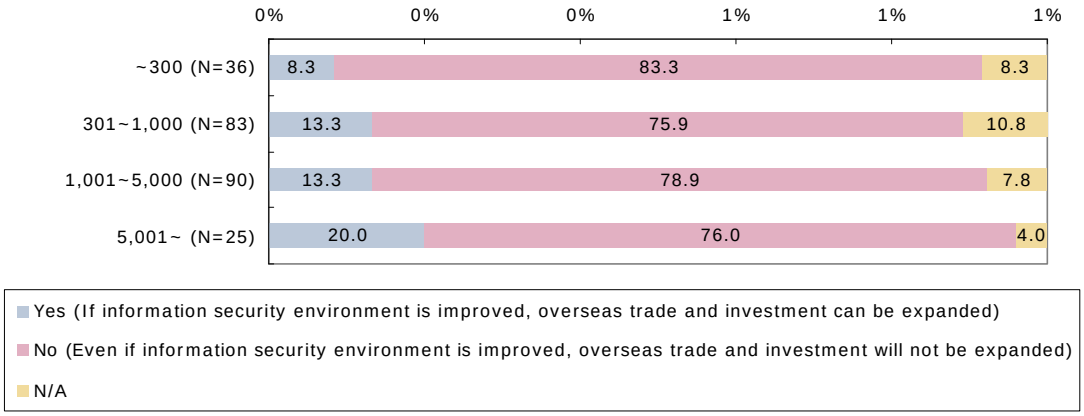
Figure 1.21. Requests to the Government for Improvement in the Information Security Environment of Overseas Trade and Investment



c) Information Security Environment for Overseas Trade and Investment and the Intention to Expand Overseas Trade and Investment in the Future

The intention to expand overseas trade and investment in the future when the information security environment of overseas trade and investment improves increases with company size. Among the companies with 5,001 or more employees, 20% respond that they intend to expand trade and investments.

Figure 1.22. Information Security Environment of Overseas Trade and Investment and the Intention to Expand Overseas Trade and Investment in the Future



1.1.5. Summary of the Survey Results

(1) Information Security in Making Decisions on Overseas Trade and Investment

Japanese companies conduct overseas trade and investment based on their business strategies. Suitability to their business strategies is the most important for decisions on trade and investment. The tendency is especially strong in large companies, most of which conduct risk analysis on decisions regarding transactions and investment. The business continuity of the client companies is an important factor in risk analysis. To promote their business strategy, companies make decisions on transactions and investments in consideration of the long-term view of client companies. Because companies in the manufacturing industry require time and large amounts of funds to prepare for business deployment, risk analysis is conducted more often in the manufacturing industry than in the nonmanufacturing industry.

On the other hand, comparatively small companies often think that immediate sales expansion in foreign countries is important. They emphasize the quality of the products and services provided by the business partners as the main criteria for decisions on overseas trade and investment.

At present, information security risks cannot be declared asa major factor in decisions on overseas trade and investment compared with factors directly linked to business. However, nearly half of all large companies with 5,001 or more employees have already established uniform standards and policies for information security risks, showing a willingness to regard information security as an element in the judgment of risk.

(2) Information Security Demanded from Client Companies

This survey shows that the information security risks about which Japanese companies are most worried at client companies are mistakes and dishonesty by insiders. Regarding security measures at client companies, Japanese companies think that organizational efforts, such as an information management system and education, are important. Large companies can ensure technical and physical security to some extent through investment. Therefore, implementation of the organizational efforts is the largest judgment criterion because it shows the policy and management system of a client company.

Information security measures at client companies are requested mainly to protect technical information, including production methods. In small and medium-sized companies, protection of technical information accumulated in the form of know-how is a challenge.

To confirm the status of information security measures at client companies, large companies with 5,001 or more employees generally send local staff to the site or use questionnaires and check sheets. Other companies seldom use these methods in their search for an effective confirmation method.

Nearly half of small and medium-sized companies conduct no confirmation. Many issues remain in promoting the confirmation of information security measures at client companies.

(3) Expansion of Overseas Trade and Investment with Improvement of Information Security Environment

This survey revealed that differences in culture and business practices between Japanese companies and client companies, rather than insufficient capital or human resources, is the issue for Japanese companies in the improvement of the information security environment at client companies or their country and region. To solve this issue, client companies should make information security efforts across the organization, and it is desirable to share the recognition between both sides of investment and trade. Therefore, Japanese companies request the government for efforts including guidelines for countries and regions of client companies to raise the awareness of information security and improve information security measures, in addition to the establishment of a common mechanism that can be used bilaterally to confirm these measures. In the last question on the survey, 13% of all companies and 20% of companies with 5,001 or more employees answered that improvement in the information security environment leads to the expansion of future overseas trade and investment. While globalization increases rapidly, the improvement in the information security environment is an urgent issue. Considering the situation of Japanese companies revealed by this survey, governments are expected respond to the issues and specific requests of Japanese companies quickly. In particular, immediate actions are desired in ASEAN and East Asia, the major trade and investment region for Japanese companies.

1.2. Survey on Overseas Investment Intention and Information Security in ASEAN and East Asia

1.2.1. Background and Purpose of the Survey

According to the experiment on utilization of the information security benchmark conducted by the WG last year, the companies in each ASEAN and East Asian country have stable needs. Though the number of samples in these surveys is small, the results show a stable trend, and it is expected that similar results will be obtained when the scale of the surveys is expanded.

Table 1.2. Needs for information Security Benchmark in ASEAN and East Asia[7]

	Yes	No	Reason (Comments)
Malaysia	86%	14%	Yes: It is an effective tool. No: Have own standards i.e. Cobit + homegrown standard.
Singapore	67%	33%	Yes: - It needs improvements in reducing repetitive questions, easier to understand questions in terms of grammar and construction, and the way it is structured. - To check your company's information security level No: - Concern over misuse and breaches of survey data, require higher management approval and support.
Thailand	NA	NA	- Some respondents are willing to use the Information Security Management (ISM) Benchmark to check the company's security level.
Vietnam	93%	7%	Yes: Free and easy-to-use. Effective tool for assessing the information security level. We can see improvements in information security through this benchmark.
China	83%	17%	No: The ISM Benchmark is too general, a more specific benchmark suitable to our company is needed.
Japan	NA	NA	
Korea	30%	70%	Yes: Possible referencing. Level comparison between the same fields is possible. Guidelines for improvement are required. Fast response to security management is possible. No: Self-measuring tool/checklist is already used. Not very flexible. No objective measure.

[7] ERIA Research Project Report 2008 No. 3-1, http://www.eria.org/research/y2008-no3-1.html.

On the other hand, considering the comments from each company, it is necessary to consider more specific needs and challenges, rather than restudying the need for an information security benchmark.

In order to clarify these needs and issues, the survey on the following items was conducted in six countries (Thailand, Singapore, Malaysia, Korea, Vietnam, and China).

- Clarification of the challenges regarding information security measures of local companies in the target countries.
- The survey on the need for an information security benchmark.

This survey was also conducted in part as a commissioned project by the Ministry of Economy, Trade and Industry in Japan but was conducted in close cooperation with the WG. Part of the results of this survey was reported in the second workshop as a contribution from Japan.

1.2.2. Survey Method and Subjects

The survey was conducted mainly through interviews by telephone with a combination of e-mail correspondence where necessary.

The survey items were based on the survey conducted on Japanese companies (outlined in 1.1.) for the purpose of comparison and covered much of the same material. Due to restrictions arising from the interview survey method, the number of questions was reduced and aggregated into 15 questions. Specifically, they consisted of items to clarify the following points:

- Impact of information security environment of overseas trade clients and overseas investment destinations on intention to trade and the motivation to invest
- Items to value as information security measures of overseas trade clients and

overseas investment destinations

- Measures to improve the information security environment of overseas trade clients and overseas investment destinations
- Requests for governments

As for the first item, since the interviewee in this survey was not responsible for overseas transactions, it was an indirect survey item.

The subjects of the survey were from companies that met the following conditions and were introduced by members of the WG.

- Companies engaged in overseas trade
- Companies aware of information security (mainly information communication industry, service industry, and manufacturing industry)

We received introductions from the WG members for 14 companies in a total of six countries, and all 14 companies were contacted. Of the 14 companies, we received the cooperation of 11 companies from a total of six countries and conducted the interviews.[8] The actual interview was conducted by the Mitsubishi Research Institute and WIP Japan on consignment from the Ministry of Economy, Trade and Industry in Japan.

1.2.3. Summary of the Survey Results

The results of the interview survey are shown in Table 1.3. From these results, the following characteristic topics were extracted:

[8] One company answered in writing.

- Of the ten companies[9], seven were large corporations[10].
- Of the ten companies, four were in the IT or communications industry and the remainder consisted of three companies in manufacturing, three companies in trade and distribution, and one company in the service industry.
- Of the eleven companies, five had global standards or policies regarding information security risk. These five companies were all large corporations, and looking at only the large corporations, five out of seven of the companies had global standards or policies. Of the remaining two companies, one company's global transactions were mainly involving goods procurement, which was why they did not have a global standard or policy. (Q5)
- As for the information security risk being considered, though there were differences in the points being focused on by each company, they considered almost all of the risks we provided as examples. The same trend was seen in the information security risks that are considered related to transactions. (Q6)
- The trends for priority level of the assets to be protected differed significantly among the companies. This is considered to be due to the differences in business industry and category. (Q7)
- Regarding the classification of the importance of information assets, ten out of eleven companies responded that they conducted classification. We also found out

[9] Excluding one company which has not given its profile.

[10] Large corporations here refers to companies with 300 or more employees or sales of 300 million yen or more (shown as LARGE in the table), and those companies smaller than that are referred to as small and medium-sized businesses (SMB in the table). As a matter of convenience, affiliates of global companies were treated as large corporations regardless of their size. The basis of 300 employees or 300 million yen is the definition for small and medium-sized companies in Japan. However, in Japan, the 300 million yen is for capital, not sales. In this survey, we did not research capital, and so the definition is based on the somewhat loose assumption that capital and sales are basically the same, that is that the stockholder asset turnover rate is approximately 1. The effect of this assumption is negligible and, therefore, has no affect on the conclusions of this survey.

that other information security measures were implemented by a large percentage of these companies. (Q8)

- As for the information security measures that should be emphasized for overseas business partners, the responses varied significantly. On average, control of IT system (d.), organizational management (a.), business continuity management (g.) and network security (c.) were comparatively valued. (Q9)
- Three companies responded that they experienced problems with information security with their overseas business partners. All three of these companies responded that this affected the business with the overseas business partner in question. This shows that when an information security issue arises, it can affect the business between the companies. (Q10)
- As for the methods used to confirm the information security measures implemented by business partners, five out of eleven companies utilized a self-check sheet. Five companies also responded utilizing third party audits. Other examples included, audits conducted by the company and the use of Information Security Management System (ISMS) authorization. On the other hand, when asked about the methods required by business partners to show their own information security, seven out of eleven companies responded that they had submitted a self-check sheet in the past. We can see that even concerning overseas transactions, the use of self-check sheets is becoming more common. (Q11)
- Regarding information security regulations, we found out that companies are being affected not only by domestic regulations but also by those overseas like the Sarbanes-Oxley Act (SOX Act) in the United States. (Q14)
- When asked about what they expect from the government, eight out of eleven

companies responded that they would like governments to formulate standards or guidelines for information security in overseas transactions. Additionally, six out of eleven companies expected the development of a shared method for measuring information security levels including common check sheets. (Q15)

In interpreting these results, it should be noted that the number of samples was small, and the sample population was biased. In other words, we cannot say that the results above are significant statistically. However, we were able to see one side of the picture, the side of a particular group in the target countries, companies that have global transactions and have a certain level of interest in information security.

Table 1.3. Result of Survey on Overseas Investment Intention and Information Security in ASEAN and East Asia

(1/10)

	No.	1	2	3	4	5	6
	Country	Thailand	Singapore	Malaysia	Malaysia	Malaysia	Malaysia
	Type of industry	NA	Telecom, Networking service	Supplier, Defence	Service, Consulting	Supplier, Telecom	Supplier, Aviation
	Size of business	NA	LARGE	SMB	LARGE (Subsidiary of global company)	LARGE	LARGE
Q1	**Major countries and regions with which your company is engaged in overseas trade and investment**	ASIA: Cambodia, Myanmar, Indonesia, Vietnam South Africa: Egypt Australia: Australia, New Zealand Middle East:, Bahrain, Algeria, Iran, Oman	Global – AMERICAS, EMEA and APAC including Japan; less the countries which UN has imposed sanctions on	Australia, Europe and ASEAN countries.	China and India	United Kingdom and Turkmenistan	Germany and United Kingdom
Q2	**Type of overseas trade and investment** **a) Investment in overseas companies and establishment of joint ventures** **b) Overseas production and sales by overseas subsidiaries** **c) Procurement from overseas companies** **d) Outsourcing to overseas companies** **e) Other**	b	a, b, c, d, e (provide outsourcing services to MNC)	a, b, c, d, e (JV with foreign companies on security system, procurement of parts and system with the rest)	a	a, c, e (Providing specialized services to overseas companies)	c
Q3	**Name of the department which is engaged in confirmation and management/supervision of information security measures involving overseas trade clients and overseas investment destinations**	CSB (Corporate Strategy and Business Development)	Legal and compliance, and Global Security	IT (Information Technology)	Risk Management Unit and Corporate Support Services – IT Unit	Operation	All done by interviewee himself, because “the company is a small set-up with only about 20 personnel, and there are only a few departments in company".
Q4	**Is risk analysis performed in making decisions on overseas trade and investment**	Yes	Yes	Yes	Yes	Yes	No
	If yes, kind of risks concerned about: **a) Client companies’ capabilities to continue business (financial collapse and acquisition)** **b) Quality of products and services of client companies** **c) Country risks (disaster, war, etc.)** **d) Information security risks (Information leakage, system failure, etc.)** **e) Leakage of business know-how** **f) Law violation risks** **g) Risks related to personnel management and work conditions of client companies’ staff** **h) Other**	a, c, f, g	c→h (local regulatory requirements and law)→f→a→d→e→b→g	a, b, c, d, e, f, g (Priority ranking of Information security risks: 3rd, after country risks and law violation risks, in this order)	a, b, c, d, f, h (Corporate Governance, Financial risk)	a, b, c, d, e, f (Priority of risks concern for Information security risks: 3rd, after country risks and leakage of business know-how, in this order)	(Reason: All business partners are established co’s. Also, procurement is by L/Cs – so co. not subjected to much risks.)

Q5	**Has global and uniform standards or a policy on information security risks**	No	Yes	Have Non Disclosure Agreement with our partners. (does have a checklist, but declined to give citing company's nature of business (national defence)	Yes - General IT controls	No (Do not have check-list)	No. (Reason: Company's oversea business is procurement of goods and trading only, and its on proven/off the shelf products. Do not have check-list.)
Q6	**Kind of information security risks concerned about** **a) Theft of information property by outsiders** **b) Insiders bringing out information intentionally** **c) Erroneous system operation by insiders** **d) Inaccurate information processing and falsification of critical information** **e) Information leakage caused by virus infection, unauthorized access, etc.** **f) System malfunction and system failure caused by device failure, bugs, etc.** **g) Malfunction and system failure caused by virus infection, unauthorized access, etc.** **h) System failure caused by natural disasters etc.** **i) Other**	a throuth h	a through h (failure to comply with local regulatory requirements and laws)	Protects against intentional or accidental attempts to deny legitimate users access to information or systems. Confidentiality covers the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use. (Violation of confidential information by staff and client (the Armed Forces)	a, d	i (Leakage of financial model)	No intellectual property to lose. Minimum security involved (due to nature of business).
	Kind of information security risks concerned about in client companies	a, c, d	All 9 items are applicable to both 'interviewee's company' and 'client companies'	a, b, c, d, e, f, g, Unauthorized export of technical data, Commercial-in-Confidence Information to reproduce, redesign, reverse engineer or manufacture any products or equipment of the disclosing party, Safekeeping of Commercial-in-Confidence Information.	a,d	b	a, b, d, e, f, g, h
Q7	**Kind of properties desire to protect with information security measures?** **a) Management-related information** **b) Technical information related to manufacturing method, parts, etc** **c) Business know-how** **d) Customer personal information** **e) Personal information of your company's employees** **f) Hardware such as PC** **g) Other**	0	d→b→a	a→b→c	a, c, e	c, d, f	a, c, d, e, f

Q8	**If classifying and managing company's assets (manpower, facilities, media, information, etc.) according to the order of importance**	Yes	Yes	Yes	Yes	No	Yes
	Have set rights to control third parties' access to its servers and networked computers	Yes	Yes	Yes	Yes	No	Yes
	If the user rights' settings regularly updated	Yes	Yes	Yes	Yes	No	Yes
	If users always obtain the system administrator's permission before installing a software application on a computer or server	No	Yes	Yes	Yes	Yes	Yes
	If a sufficient test is performed when installing new software	Yes	Yes	Yes	Yes	No	No
	If servers' applied software programs and security equipment systems patched on a regular basis	Yes	Yes	Yes	Yes	Yes	Yes
Q9	**What are valued as information security measures in client companies a) Status of organizational efforts on information security (information management system, contract with employees, education and training etc.) b) Physical (environmental) security measures c) Operation and management of communications network and information system d) Development, maintenance, and access control of information system e) Status of response to information security accidents f) Reconsignee management g) Business continuity management h) Other**	a, c, g	c→a→g	b→g→d	a, d, g	d, e, h (Ensuring non-approved external PC devices are brought in and connected to the network)	d, e, h (Ensuring non-approved external PC devices are brought in and connected to the network)
Q10	**Have ever experienced information security problems in client companies that influenced your company**	No	Yes (differing views on criticality of patch/vulnerability management)	Yes (declined to give examples citing security reason)	No	No	No
	If yes, have information security troubles influenced the concerned business relations with client	NA	Yes (response time/turnaround time to address concerns had escalated to SLA conflicts and disagreement)	Yes (declined to give examples citing security reason)	NA	NA	NA

Q11	**How the information security measure of client companies are confirmed** **• Certification of ISMS (Information Security Management)** **• Confirmation of the report by auditing firm** **• Self-check sheet** **• Other**	Certification of ISMS	all the three mentioned	• Maintenance of data integrity • Ensuring Company's security policy is maintained. • Regular visit by client company to access the running of company's security policy	• Confirmation of the report by auditing firm • Self-check sheet	• Other (By talking to IT department Manager/Senior executives in clients' organization)	• Other (ISO 9001)
	How the level of information security measure presented to client companies **• Certification of ISMS (Information Security Management)** **• Confirmation of the report by auditing firm** **• Self-check sheet** **• Other**	Certification of ISMS	all the three mentioned	• Self-check sheet • Other (Documentation of the risk assessment process and procedures assists in ensuring consistency and completeness as well as accountability)	• Confirmation of the report by auditing firm • Self-check sheet	• Other (At present we have not experienced such a request by any customer)	• Other (signing of Non-Disclosure Agreement)
Q12	**Kind of matters related to information security are stipulated in the agreement with client companies** **a) Use, storage, taking out, erasing, and destruction of confidential information** **b) Reconsignment of operations related to confidential information** **c) Provision of training opportunities for employees handling confidential information** **d) Physical security** **e) Control of access to confidential information** **f) Operations to respond to audit** **g) Response to accidents (intervention in investigation of client companies, agreement on compensation, etc.)** **h) Other** **i) Not stipulated**	i	a through h (demonstrate compliance to local regulatory requirements and law)	a through h (definition of commercial-in-confidence information, liability for disclosure, protection, impermissible uses, no rights granted, permitted disclosures, return or destruction of commercial-in-confidence information, legal actions and government regulations, relationship between the parties, dispute resolution)	a, e, f	i	e, h (signing of Non-Disclosure Agreement)
Q13	**Kind of statutory and regulatory requirements-- both domestic and foreign-- on information security which the company identifies in oversea trade and investment**	NA	local central banking requirements, Electronic Transaction Act, Stock Exchange acts, computer mis-use acts, SOX, Basel, HIPPA, privacy acts, export controls	Dispute resolution shall be subject to and construed in accordance with the laws of country both foreign and local.	Local : Communication and Multimedia Act - Guidelines on Management of IT Environment by Central Bank of Malaysia - Digital Signature Act - FRS 139	None at present	Via contractual obligation

Q14	**Knowledge of any information security initiatives that your government is doing**	Computer Crime Act., ISMS Standard	promotion of ISO 27000 standards and adoption of these standards where applicable, participation in the drafting/commenting of the standards via ITSC (www.itsc.org.sg)	Yes, through the government initiative in formulating The National Cyber Security Policy. Exposed the National Cyber Security outline that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects.	1.Implementation of National Cybersecurity Policy - Capability building and Acculturation - Vulnerability assessment to critical information infrastructure - ISMS implementation to al critical sectors 2. Common Criteria scheme 3. Trustmark Scheme	There are a lot of training courses developed by governmental bodies to educate business IT users. There is a government body (NISER) set up to monitor a whole range of IT security risk.	Do not know of any.
Q15	**Request for the government in order to improve information security environment in overseas trade and investment** **a) Tax incentives to improve information security** **b) Provision of training and education opportunities** **c) Improvement of IT infrastructures** **d) Development of standards or guidelines** **e) Development of shared mechanism to confirm information security level, including common check sheet**	b, e	a, b, c, d, e	b, f, e	a, b, c	a, b, c, d, e	c, d
-	**additional comments**	NA	One real-life example by interviewee: The adoption of international security standards. Being a global company, we have encountered clients who do not comply to international standards, e.g. China. They have their own and there are grey areas. No encryption allowed in the country and we cannot fulfill our contractual obligations. All governments should encourage the adoption of international standards as a baseline to facilitate a common understanding.	Comment by interviewee: Laws are already in place, only lacks supervision and enforcement on the authorities/government's part. Government should improve on this area.	NA	Comment by interviewee: Feels contented with what the authorities have done up to now as regards the information security environment, especially with the already set up of the government body, NISER (refer Q14) to monitor it.	Comment by interviewee: Hopes for a cheaper, faster and more reliable data circuit within Malaysia and to servers overseas.

	No.	7	8	9	10	11
	Country	Korea	Vietnam	Vietnam	China	China
	Type of industry	Service, Internet	Food	Manufaturing, Service (Design)	Manufacturing, Communication	Manufacturing, IT
	Size of business	LARGE	SMB	SMB	LARGE	LARGE
Q1	**Major countries and regions with which your company is engaged in overseas trade and investment**	Japan / Asia Pacific Region	America, EU, Canada, Japan (From 1984, but the business relation was interupted recently)	Import-The Netherlands, America, Japan Export-Japan, Hong Kong, Malaysia	all over the world, including England, France, Sweden in Europe, U.S., India and even Africa	all over the world, including U.S., Germany, England, Japan, Korea, Taiwan, Hong Kong and some emerging markets like Russia and India
Q2	**Type of overseas trade and investment** **a) Investment in overseas companies and establishment of joint ventures** **b) Overseas production and sales by overseas subsidiaries** **c) Procurement from overseas companies** **d) Outsourcing to overseas companies** **e) Other**	a	c (Importing chemicals from EU, Importing technological machines e (Exporting its products to America, EU, Canada, Japan)	c, d	b	b
Q3	**Name of the department which is engaged in confirmation and management/supervision of information security measures involving overseas trade clients and overseas investment destinations**	Global Information Security (Information Security Policy Establishment, Technical Risk Assessment, User Awareness Training, Security Solutions Operation)	There is no specilized department as above. But Sales deparment and Market department and an IT employee work together. The interviewee said "the information security management is bad in this company and it doesn't know any company that can help them to to improve the situation".	The Department of Accounting and General Affairs and Practical research department work together.	Committee of Information Security Management which is in charge of information security in regard to the operation of the company	IT operation & Maintenance department is in charge of the information security, standard and purchase of products of the entire company
Q4	**Is risk analysis performed in making decisions on overseas trade and investment**	Yes	Yes	Yes	Yes	Know nothing about it and does not participate in that activity
	If yes, kind of risks concerned about: **a) Client companies' capabilities to continue business (financial collapse and acquisition)** **b) Quality of products and services of client companies** **c) Country risks (disaster, war, etc.)** **d) Information security risks (Information leakage, system failure, etc.)** **e) Leakage of business know-how** **f) Law violation risks** **g) Risks related to personnel management and work conditions of client companies' staff** **h) Other**	b→a→f→d→g→e→c→h (Human Resource)	b, c, d, e, f, g	a, b, d, e, g	b, d, e	NA

Q5	**Has global and uniform standards or a policy on information security risks**	Yes (does have a checklist, but cannot disclose)	No	No	Yes (but cannot disclose)	Yes (handled by the business department and is not accessible to the interviewee)	
Q6	**Kind of information security risks concerned about** **a) Theft of information property by outsiders** **b) Insiders bringing out information intentionally** **c) Erroneous system operation by insiders** **d) Inaccurate information processing and falsification of critical information** **e) Information leakage caused by virus infection, unauthorized access, etc.** **f) System malfunction and system failure caused by device failure, bugs, etc.** **g) Malfunction and system failure caused by virus infection, unauthorized access, etc.** **h) System failure caused by natural disasters etc.** **i) Other**	a through h	a through i (if clients' employees are qualified enough)	a through i (mouse, electricity problem)	b	There are in-house trainings about information security, front end, back end, and the contents involved in the trainings cover all kinds of problems.	
	Kind of information security risks concerned about in client companies	a through h	a through h	a through h	b	d	
Q7	**Kind of properties desire to protect with information security measures?** **a) Management-related information** **b) Technical information related to manufacturing method, parts, etc** **c) Business know-how** **d) Customer personal information** **e) Personal information of your company's employees** **f) Hardware such as PC** **g) Other**	c, d, e	c→f→e	a→b→c	b→c→a	b→c→d→a→f	

Q8	**If classifying and managing company's assets (manpower, facilities, media, information, etc.) according to the order of importance**	Yes	Yes	Yes	Yes	Yes	
	Have set rights to control third parties' access to its servers and networked computers	Yes	No	No	Yes	Yes	
	If the user rights' settings regularly updated	Yes	Yes	Yes	Yes	Yes	
	If users always obtain the system administrator's permission before installing a software application on a computer or server	Yes	Yes	Yes	Yes	Yes	
	If a sufficient test is performed when installing new software	Yes	No	Yes	Yes	Yes	
	If servers' applied software programs and security equipment systems patched on a regular basis	Yes	No	Yes	Yes	Yes	
Q9	**What are valued as information security measures in client companies a) Status of organizational efforts on information security (information management system, contract with employees, education and training etc.) b) Physical (environmental) security measures c) Operation and management of communications network and information system d) Development, maintenance, and access control of information system e) Status of response to information security accidents f) Reconsignee management g) Business continuity management h) Other**	b, d, g	a, c, d	a	a, c, d	b→a→d	
Q10	**Have ever experienced information security problems in client companies that influenced your company**	No	No	Yes	No	No	
	If yes, have information security troubles influenced the concerned business relations with client	NA	NA	Yes	NA	NA	

Q11	**How the information security measure of client companies are confirmed** **• Certification of ISMS (Information Security Management)** **• Confirmation of the report by auditing firm** **• Self-check sheet** **• Other**	• Confirmation of the report by auditing firm • Self-check sheet	• Self-check sheet • Other (Company profile)	• Confirmation of the report by auditing firm • Self-check sheet	• Confirmation of the report by auditing firm • Certification of ISMS • Other (conduct quality check towards client companies, ask for relevant certificates)	know nothing about what measures are taken for confirmation	
	How the level of information security measure presented to client companies **• Certification of ISMS (Information Security Management)** **• Confirmation of the report by auditing firm** **• Self-check sheet** **• Other**	• Confirmation of the report by auditing firm • Self-check sheet	• Self-check sheet • Other (Company profile)	• Confirmation of the report by auditing firm • Self-check sheet	• Confirmation of the report by auditing firm • Report authenticated by third party	all the three mentioned, other (auditing report by the interviewee's own company, evaluation by the third party, relevant qualifications)	
Q12	**Kind of matters related to information security are stipulated in the agreement with client companies** **a) Use, storage, taking out, erasing, and destruction of confidential information** **b) Reconsignment of operations related to confidential information** **c) Provision of training opportunities for employees handling confidential information** **d) Physical security** **e) Control of access to confidential information** **f) Operations to respond to audit** **g) Response to accidents (intervention in investigation of client companies, agreement on compensation, etc.)** **h) Other** **i) Not stipulated**	a, c, d, e, g	b, c, e	a, c, d, g	a, b, g	a through g	
Q13	**Kind of statutory and regulatory requirements-- both domestic and foreign-- on information security which the company identifies in oversea trade and investment**	Sarbanes-Oxely Act, Payment Card Industry Data Security Standard, Other local compliance requirements Laws and regulations do not discourage business; the interviewee recognizes those as, "things to keep in mind and remember all the time upon dealing with other companies."	None	There is no statutory requirements on information security. The company negotiates and comes to agreements with its clients about requirements. No further information has been released.	relevant legal monitoring laws in each country, protection for users' data in each country, and laws related to information security management	There must be some relevant laws and regulations, however, the interviewee knows nothing about the specific names.	

Q14	**Knowledge of any information security initiatives that your government is doing**	Nothing in particular	It is heard that the government is establishing Department of information security which is in the national security campaign about information). But the governemt still doesn't know what kind of information and support that enterprises want to receive.	The government has not given any security initiatives on information securitty.	Know a little about it. For example, the regulations related to the supervision of information contents and status of network operation, etc.	know nothing about it	
Q15	**Request for the government in order to improve information security environment in overseas trade and investment** **a) Tax incentives to improve information security** **b) Provision of training and education opportunities** **c) Improvement of IT infrastructures** **d) Development of standards or guidelines** **e) Development of shared mechanism to confirm information security level, including common check sheet**	d	b, c, d, e	a, b, d, e	d	a, d, b	
-	**additional comments**	Comemnt by interviewee: Laws, regulations, and institutions need to be enriched, supplemented, and concretized. It is not that there is no development of standards or guidelines right now; however, creating more of those do not necessarily enhance efficiency. I do not expect the government to create more and more standards or guidelines: Rather, what I think is necessary is that the government optimizes and makes the standards and guidelines perfect, by putting itself in company's shoes.	The government should run national program on information security for companies that cost little fee or free.	NA	NA	NA	

1.3. Status of Information Security Measures of Companies in ASEAN and East Asia

Based on the results of II. 1.1. and 1.2. , we will discuss the issues in formulating the Common Information Security Management (ISM) Benchmark.

(1) General Statement

Even if the difference in investigation methods or in the population is considered, the results of the investigation intended for Japanese companies and that for other countries show a very similar trend. Under the wave of rapidly progressing globalization, we assume that the difference in the industry structure in Japan and other countries is negligible from the viewpoint of information security, or at least that the difference is rapidly decreasing.

We think the above-stated situation gives positive grounds for the formulation of the Common ISM Benchmark. In ASEAN and East Asia, the relationship among companies is not hierarchical or static like that of an orderer and an order-receiving party, but it has been strengthened as equal partners. This indicates that the importance of bi-directionally common communication is growing for risk communication with respect to information security. As a tool for such risk communication, we think it would be possible to find meaning in the Common ISM Benchmark.

(2) Items that Should be Included in the Common ISM Benchmark

In the study targeting Japanese companies, a significantly higher percentage of responses regarding the items emphasized for information security measures

implemented by business partners were for organizational measures compared with other items. This shows that, for Japanese companies, a certain level of technological measures has already been implemented, and so the emphasis is placed on confirming how these measures are being managed. On the other hand, in the study targeting the companies from other countries, though organizations are of course emphasized, other physical measures were also emphasized. These differences between industries cannot be ignored.

If we consider the items that should be included in the Common ISM Benchmark based on these results, we can see that it is necessary to select a balanced mix of questions so that it can be used more widely rather than focusing on specific items. Additionally, it is ideal that there be room for customization, such as adding optional items depending on the country.

Additionally, the Common ISM Benchmark can be used not only with business partners but also to confirm the situation of your own company, and therefore, the items should be balanced accordingly.

(3) Needs for the Common ISM Benchmark

In both the survey results for Japanese companies and those for all other countries, the highest percentage of responses for the type of measures or policies the companies wanted from the government was the formulation of standards and guidelines. The second highest response was the development of a shared method for measuring information security levels including checklists.

From these results, we can ascertain that the potential needs of companies in ASEAN and East Asia for the Common ISM Benchmark and the common question list

it is based on are high. Our next challenge will be how to provide a Common ISM Benchmark that responds to these potential needs.

2. Concept and Value of Common ISM Benchmark

The vision statement drafted by the WG the previous year provides the objective of the Common Information Security Management (ISM) Benchmark, and the goal statement presents the ideal shape of the Common ISM Benchmark.

Our Vision:

A Common ISM Benchmark contributes to industries and governments by building and promoting a trustworthy economic partnership that encourages more foreign direct investment (FDI) and business outsourcing in the Asian region.

Goals:

- The Common ISM Benchmark provides acceptable and comparable indicators of the information security management level of organizations.
- As a comprehensive risk communication tool, the Common ISM Benchmark enables organizations to improve their sense of information security through visualization of the risks.

2.1. Objective of Common ISM Benchmark

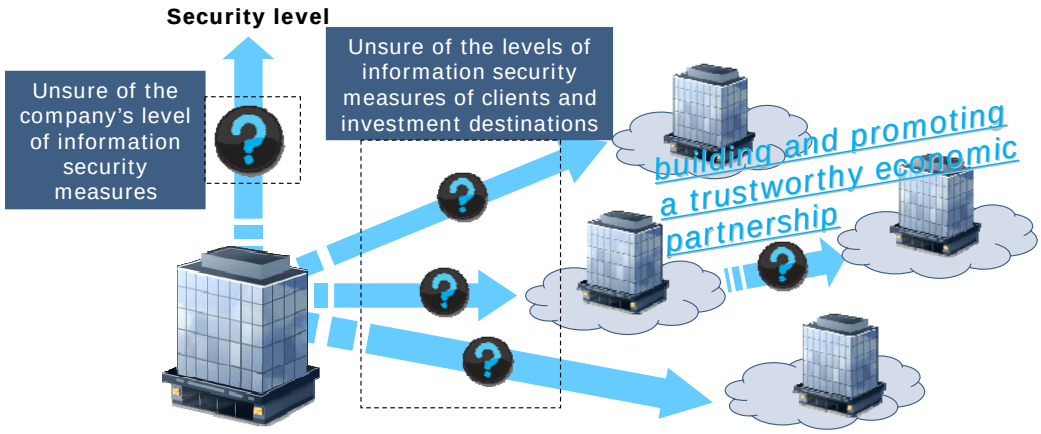
The objective of the Common ISM Benchmark is *building and promoting a trustworthy economic partnership* as was stated in last year's vision statement, and to realize this, the following information security issues the companies in ASEAN and East Asia face should be resolved.

- Do not know which security level to adopt for information security measures and how to measure such levels

- Difference in awareness of information security measures, including information management between customers/clients
- Communication/cultural gap on information security caused by the diversity in ASEAN and East Asia

Figure 2.1. is a diagram of these issues.

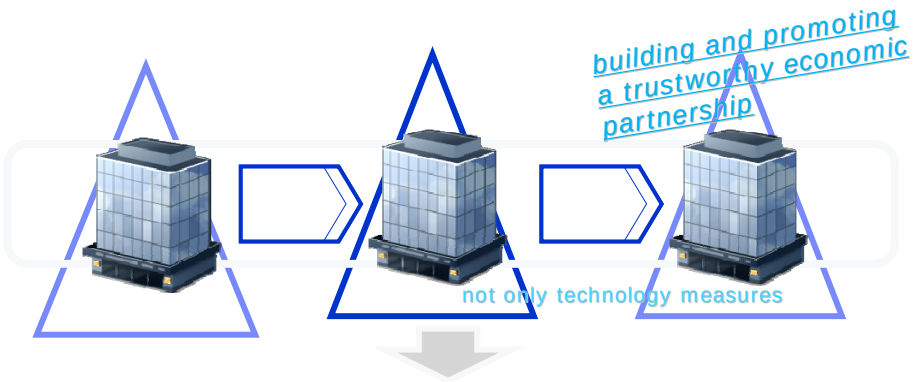
Figure 2.1. Information Security Issues for Companies in ASEAN and East Asia



The Common ISM Benchmark should contribute to resolving these issues.

The important thing here is that the groups of companies that comprise the value chain of companies in the region are able to share important proprietary information and divide the operations among themselves while providing value to end consumers. This means that each company in the region that is part of the value chain should achieve the same level of information security management; otherwise, it will not be possible to share proprietary information and achieve highly efficient operations.

Figure 2.2. Information Security Management within a Value Chain



Every company in the chain needs to establish security management to reduce and maintain risks under an allowable level

2.2. What Common ISM Benchmark Should Be

What should the Common Information Security Management (ISM) Benchmark be like? The answer is the three keywords: acceptable, comparable, and risk communication tool from last year's goal statement.

These three keywords are defined as follows:

Acceptable

- Easy to understand and to use for all participants, especially for business executives
- Reasonably detailed, but not too complicated

Comparable

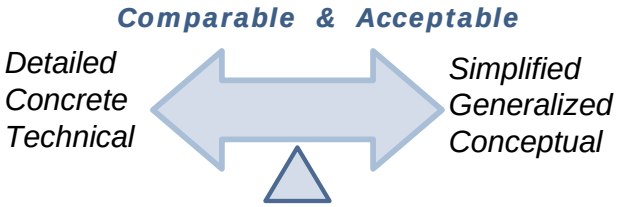
- Common questions for any geography, any industry, regardless of organization size
- Not depend on specific technology implementation

Risk communication tool

- Express high level risk status by checking Information Security Management actually implemented
- MECE (Mutually Exclusive and Collectively Exhaustive)

To design a Common ISM Benchmark that meets these requirements, it is necessary to achieve a balance between comparability and acceptability. That is, when one pursues comparability, the number of common questions increases and the contents become more specific; however, this goes against the basic rule of acceptability. If we consider server massage block (SMB), which accounts for a significant majority of the companies, it is obvious that there is a certain restriction on comparability.

Figure 2.3. Desirable Design of the Common ISM Benchmark



We should also consider who will be using the Common ISM Benchmark and for what purpose. The Common ISM Benchmark emphasizes the use within the value chain, such as supply chain management (SCM), but is not limited to this. The main use methods and anticipated users are the following:

Companies aiming to confirm their own level of information security measures

Main use methods:

- Application as a self-awareness tool and risk communication tool
- Available for small and medium-sized companies as well as major companies
- Comparison of their level with those of other companies

Anticipated users:

- For executives: Know your company's position within the industry and verify your understanding of risk
- For business owners: Satisfy business partner requirements
- For business process managers: Understand the current status by control area and department and develop plans to upgrade the levels

Companies aiming to confirm the levels of information security measures of their clients and investment destinations

Main use methods:

- Confirmation of the status of information security measures with clients and investment destinations
- Application as a common language with clients and investment destinations

Anticipated users:

- For commissioning company/investing companies: Understand the status of information security measures of commissioned companies and utilize the Common ISM Benchmark as a basis (item/level) to agree on required information security measures
- For commissioned companies/investee companies: Report the status of information security measures to commissioning companies in a single way and call attention to their own level of measures

2.3. Relationship to Existing Standards

The purpose of this section is (1) to evaluate the benchmark against existing standards; and (2) identify possible framework, scheme, and challenges for standardization of the Common Information Security Management (ISM) Benchmark.

2.3.1. Relationship to Existing Standards

One of the objectives of the Common ISM Benchmark is to provide a system of assurance for service acquirers or buyers of services/products, i.e., organizations who are outsourcing their business or IT processes to external providers, or using suppliers of components, products, or services to support its business. To meet this objective, considering the target community of organizations, and the nature of the organizational relationships involved, the information security standards that covered the following scope should be leveraged:

1. Help organizations to set up a system of governance for information security management;
2. Best practices guidance on information security controls in general;
3. Best practices guidance on information security controls relating to outsourcing and related services (or business operations/processes); and/or
4. Best practices guidance on the use of third party services, either for security-specific purposes or supply of other products or services (such as manufacturing or development work).

Given the limited time and resources allocated for this section of the research, the study was limited to information security standards developed and published by the

International Standards Organization and International Electrotechnical Commission Joint Technical Committee 1, Subcommittee 27 (ISO/IEC JTC 1/SC 27).

Table 2.1. lists the information security standards identified and the mapping to the above scope:

Table 2.1. List of ISO/IEC Standards Related to Information Security Management and Outsourcing

Standard	Title	Scope
ISO/IEC 27001	Information Security Management Systems - Requirements	1
ISO/IEC 27002	Code of Practice for Information Security Management	2
ISO/IEC 27036	Guidelines for Security of Outsourcing (2nd Working Draft)	3
ISO/IEC TR 14516	Technical Report – Guidelines on use and management of Trusted Third Party (TTP) services	3, 4
ISO/IEC 15945	Specification of TTP services to support application of digital signatures	3, 4
ISO/IEC 29149	Technical Report – Best practices on the provision of Time Stamping Services (PDTR)[11]	3, 4

[11] A PDTR is a proposed draft technical report two stages from being published formally by ISO/IEC.

ISO/IEC 27001 is a specification for a management system, which is a certifiable standard. Organizations that implement an information security management system based on this standard can be certified to conformance by an accredited certification body to gain formal recognition globally. ISO/IEC 27001 promotes a management system approach, using the Plan-Do-Check-Act (PDCA) cyclical processes to manage information security risks in an organization. A formal information security risk assessment process is required as part of the PDCA cycle.

ISO/IEC 27002 is a best practice guide that specifies a total of 133 controls in 39 control requirements covering 11 areas (also known as clauses, categories, or domains) that organizations may use in accordance with the findings of the risk assessment step from the ISO/IEC 27001 PDCA process to manage related information security risks. ISO/IEC 27002 defines the objective of information security as "to minimize risks and impacts to business while maximizing business opportunities and investments and to ensure business continuity". The standard includes two groups of controls based on essential legislative requirements or considered common practice for information security. The following are controls considered essential to an organization from a legislative point of view, depending on the applicable legislation:

1. Data protection and privacy of personal information
2. Safeguarding of organizational records
3. Intellectual property rights

The following are controls considered common practice for information security, which include the following:

1. Information security policy document
2. Allocation of information security responsibilities

3. Information security awareness, education, and training
4. Correct processing in applications
5. Vulnerability management
6. Business continuity management
7. Management of information security incidents and improvements

ISO/IEC 27036, which is currently under development, at its second working draft stage, may take another 18 to 24 months or more before it becomes a published standard. This standard is developed to provide more in-depth guidance to support organizations in implementing ISO/IEC 27002 information security controls related to suppliers of outsourced services. The standard aims to address the security of outsourcing comprehensively from a risk management perspective. The security requirements provided in this standard are based on a generic and commonly accepted view of processes involved in an outsourcing lifecycle. The current draft further includes two annexes, providing a list of key risks for consideration in the risk assessment process, and additional guidance on control objectives, controls, and implementation guidance to supplement the controls provided in ISO/IEC 27002.

ISO/IEC TR 14516, ISO/IEC 15945, and ISO/IEC TR 29149 are technical standards specifically developed for trusted third party (TTP) organizations provide security services relating to the implementation of a Public Key Infrastructure (PKI). While the general framework and processes may apply to outsourcing service providers, the major sections of the standards are only applicable to TTP organizations specific to the security services (e.g., time-stamping services in the case of 29149) targeted by the respective standard.

Figure 2.4. Relationships of Standards, from Management Systems to Technical Requirements

Figure 2.4. shows the relationships between the above-described standards, from management systems to more specific technical requirements.

In addition to the above standards, ISO/IEC JTC 1/SC 27/WG 4 is currently having a study period on "Supply Chain Security Controls". The study period will evaluate the relationship of ISO/IEC 27036, the study period proposal, and the work of ISO/TC 8 on ISO/IEC 28001 and ISO/IEC 28002. The latter two standards are specific to supply chain security management requirements:

Table 2.2. List of Supply Chain Security Management Standard Developed by ISO/TC 8

Standard	Title	Scope
ISO/IEC 28001	Security management systems for the supply chain—Best practices for implementing supply chain security, assessments and plans—Requirements and guidance	3, 4
ISO/IEC 28002	Resilience in the Supply Chain: Requirements with Guidance for Use	3, 4

In terms of security, the ISO/IEC 2800x standards include requirements for physical protection, personnel security, and goods and conveyance security, in addition to information security.

2.3.2. Consistency with Existing Standards

The study in section 2.3.1 above established that there are in fact a number of ISO/IEC standards that may be leveraged by service providers and suppliers to ensure the security of information in their respective organizations.

Using these standards and understanding as a baseline, we evaluate the current Information Security Management (ISM) Benchmark in five areas, namely, coverage, focus, depth, quality, and assurance.

(1) Coverage

The current ISM Benchmark focuses on the requirements and best practices specified in ISO/IEC 27002. The 25 questions used in the ISM Benchmark represent a subset of the 133 controls in the ISO/IEC 27002 standard, covering the following areas:

1. Organizational approach to information security, including policy requirements
2. Physical security countermeasures
3. Operation and maintenance controls over information systems and communication networks
4. Information system access control, including security countermeasures for development and maintenance phases
5. Information security incident response and business continuity management (BCM)

The distillation of the 133 controls to 25 questions aims to focus only on the above five areas that are deemed more important by the designer, and to reduce the time required for respondents to complete the benchmark questions. However, this approach assumes that these five areas (covered by the 25 questions) are sufficient and adequate for all service providers, covering all the information security concerns of the service/product acquirers. This underlying assumption (which has not been explicitly stated) may not be true in the actual environment.

The ISO/IEC 27002 was developed essentially as a standard to support the implementation of the ISO/IEC 27001 ISMS approach. It calls for the use of risk assessment as a fundamental technique to understand organizational information security needs before embarking on selecting and implementing controls. It also discusses about other risk response options, besides the risk mitigation (or treatment) approach detailed in ISO/IEC 27002. The use of ISO/IEC 27002 in the current ISM Benchmark does not take into considerations these essential requirements, and therefore is not consistent with the objectives of the standard.

As a result of the distillation, the outcome of the benchmark, comparing many organizations from different industries based on their answers to a single set of 25 questions, may have several side effects as discussed in the subsections that follow.

(2) Focus

There are many different types of service and products providers in the industry, delivering services and products are unique to the needs of the specific industry. In addition, the information security requirements for different industry will also differ, in terms of priorities and focus. For example, in the healthcare industry, personal privacy

identifying information (PII) is given the greatest focus and care, whereas in the financial industry, transaction integrity is often the prime focus, followed by systems availability and information confidentiality.

The current ISM Benchmark was not designed with this in mind and, therefore, cannot provide questions specific to the concerns of each industry category. In essence, the 25 questions, which are generic in nature, may gather some information, but not sufficient to provide greater understanding of the respondent's organization information security profile (which closely align with business needs).

As described in section 3.3.1., there are existing standards developed for specific TTP and manufacturing suppliers. These standards could not be leveraged as such, given that the industry profile of the respondent organization is not identified in the benchmark questions.

(3) Depth

The generic nature of the 25 questions does not allow for more detailed information to be clearly identified about the respondent organization and its security practices. Furthermore, the design of the question was such that they are generally one-off, in that the answer is not evaluated to determine further questions that need to be answered, and the response is accepted as provided.

(4) Quality

A number of questions asked for appropriate countermeasures, which are subjective, in which their selection would depend on many factors, based around the risk identified, and the risk culture of the organization.

The quality of the respondent's answers to such questions depends on whether the respondent is a practicing information security professional with an understanding of the question and the issues and concerns involved.

A respondent, for example, may take it that observing one or few of the many examples of *appropriate countermeasures* as an indication that the practice is in place in the organization, whereas the question assumes all countermeasures given in the examples are essential.

Two different respondents from the same organization may therefore provide different answers to such questions.

(5) Assurance

The current approach accepts the answers from the respondents as-is, without a mechanism for validation of the responses. On top of this, the questionnaires are not designed to support the need for assurance or validation.

There are also no questions that look for evidence of controls in practice (but just asked whether they are there), which does not allow the evaluator to check for consistency in the answers or provide leading indicators of compliance with specific requirements.

2.3.3. Possible Framework, Plan, and Challenges for Standardization of Common Information Security Management (ISM) Benchmark

We propose a framework based on the approach used in the Singapore Standard (SS) 493:2001 – Security Standards Framework, and the ISO/IEC 15408 – Evaluation criteria for IT security standards.

In accordance with SS 493, the information security controls and requirements should be aligned to the security services the organization needs as part of its business. Security services include confidentiality, integrity, availability, accountability, and privacy services. To ensure consistent coverage and appropriate depth, focus, and quality of the questions used, the Common ISM Benchmark should include a set of questions designed to profile the respondent's organization and identify the security services essential for the service acquirer to gain confidence (assurance).

The varied needs and priorities of the different industry and security services would result in a slightly different set of questions to determine their risk profile and the current information security status of the respondent. These questions (specific to the respondent's organization) represent the functional security requirements of the organization in question.

To gain assurance, we need to establish the assurance requirements of the service acquirers. A plan with different levels may be used and selected by the service acquirers based on the level of confidence that the acquirer's organization needs from the service and product providers.

As discussed at the ERIA workshop in February 2010, the following assurance level may be used:

1. Level 1 – Self-check questionnaire similar to the current approach; this level offers very weak assurance for the plan involved.
2. Level 1V – Validated self-check, which may involve another user or professional in the community to perform selected validation of the responses provided, but not all responses. By performing such a validation, we gain more confidence in the integrity and accuracy of responses and, therefore, increase the assurance provided.
3. Level 2 – Independent third party assessment, involving a comprehensive assessment based on the responses in the ISM Benchmark, and generating additional questions to gain an understanding and confidence in the organization's benchmark results.
4. Level 2V – Validated third party assessment in which the work of the third party is crosschecked by another professional or security organization.
5. Level 3 – Certified and validated third party assessment, which closely mirrors the ISO/IEC 27001 approach, with the exception that the evaluation is more focused on the industry concerned with more coverage (on all relevant standards, not just ISO/IEC 27002) and depth as identified from the risk profile and industry category involved.

The combination of the functional requirements and assurance requirements above is in line with the security evaluation approach described in ISO/IEC 15408, which is also known as the *common criteria scheme*. While the details do not include such elements as the Protection Profile, Security Target, and Target of the Evaluation, the approach of ensuring consistent coverage, focus, depth, quality, and assurance supports the scalability needs and allow for such a scheme to more accurately and effectively

measure and benchmark small and medium enterprises.

At the Tokyo workshop, there were also discussions regarding the different level of functional requirements, similar to the idea of having different levels of assurance requirements. The functional levels could potentially be developed based on the four areas used in the above evaluation of the current ISM Benchmark, namely, coverage, focus, depth, and quality. Additional resources are necessary in order to expand the proposal and provide more details on the functional and assurance levels discussed in this subsection.

3. Common ISM Benchmark and Related Issues

3.1. Part to be Developed in Common and the Part to Be Localized

Following the objectives of the WG,

- promote further business outsourcing and foreign direct investment in ASEAN and East Asia.
- motivate each company to understand the importance of information security measures and take action.

The Common Information Security Management (ISM) Benchmark was developed by the WG members to serve this purpose. In this year's WG, we discussed the common questions to be used by all countries as a common part of the Common ISM Benchmark and decided on the 27 questions provided in 3.2.2.

Through the deliberations outlined in 3.2.1., the common questions were accepted by all members for use by the member countries. It will be the tool to provide acceptable and comparable indicators of the information security management level of organizations that will promote further business outsourcing and foreign direct investment. All the questions used in the Common ISM Benchmark should be the same and should cover all the important issues emerging in the ISO/IEC 2700X standards.

The part to be developed after using the Common ISM Benchmark will occur when the ISO/IEC 2700x is updated; the Common ISM Benchmark should be updated and serve as the reference. The Common ISM Benchmark should be reviewed by experts and the WG members involved in this project. The Common ISM Benchmark in this paper can be identified as Common ISM Benchmark, version 1.0. However, if it does

not cover all domains in ISO/IEC 2700x, then it should be improved in the future.

The WG finished research on the Common ISM Benchmark. The Common ISM Benchmark will now be compared with local benchmarks in each of the members' countries. There are some differences in the questionnaires. Some countries' benchmarks have unique issues. There are some differences in their systems, system environment, system development, and system culture. There are many reasons, and the importance of their IT policy is such that they should add some details to the local benchmark, such as security awareness and a business continuity plan. The local benchmark can help them achieve greater awareness of IT security, which is important. However, all of the WG members agree that they should have the Common ISM Benchmark for self–evaluation and comparisons with other WG member countries. This will fulfill the objective of this WG. The local benchmark should be based on the Common ISM Benchmark.

3.2. Common Questions

3.2.1. Process of Selecting Common Questions

The following is the process used to deliberate the common questions.

(1) Discussions on the Method for Determining the Common Questions

In the first workshop, the WG studied existing benchmarks ordinarily used in the member countries of Japan, Korea, and Malaysia. After some discussion, the Japanese and Korean benchmarks were selected as the main idea for developing the Common Information Security Management (ISM) Benchmark.

Table 3.1. Japanese and Korean Benchmarks

Name	Country and Organization	Overview
Information Security Management Benchmark (ISM Benchmark)	Japan (Information-technology Promotion Agency IT Security Center)	A self-assessment tool to visually check the level of the company's security measures by responding to questions about the company profile and security countermeasures. The ISM Benchmark was based on the management measures (133 items) of JIS Q 27001:2006 Appendix A, which is an ISMS authorization standard. The 25 questions regarding measures for information security were used in the current deliberations. (Reference URL) http://www.ipa.go.jp/security/english/benchmark_system.html (Questions regarding the company profile: 15 questions, questions regarding measures for information security: 25 questions, total of 40 questions)
Information Security Assessment Tool for SMEs Questionnaire	Korea (Korea Information Security Agency)	An evaluation tool for information security measures for small and medium-sized businesses. (No. of questions: 30 questions)

(2) Create a Mapping Sheet

With the cooperation of the members and concerned parties in Japan and South Korea, a mapping sheet was created using the two questionnaires selected in (1). With this mapping sheet, we could see which items were included in both questionnaires, which items had parts in common with other items, and which items were found in only one of the questionnaires. As for each item, a simple explanation was provided regarding the contents. A column was provided for responses as to whether the item should be included as a common item and the reason for the choice.

(3) Primary Selection of Questions by the WG Members

The mapping sheet was distributed to the WG members for review. The members evaluated and scored the importance of all questions on the mapping sheet. The members selected the questions and identified which should remain in the Common ISM Benchmark based on their expertise and experience under the condition that the questionnaire should refer to the ISO/IEC 2700x standards and serve the objective of the ERIA.

The members and concerned parties in Japan collected all the scores submitted by members and put them in a table to prepare for the second workshop.

(4) Final Selection of Questions

In the second workshop, the open session was set. The members shared their experience and openly discussed all the questions. Then the members selected 27 common questions.

The selections were made based on the following policy:

- The questions were determined by consensus. (In the primary selection, those items for which a large number of members agreed to inclusion as common items were automatically added, and for those for which there was no consensus, individual discussions were held.)
- The questions were kept as simple and easy to understand as possible.
- Detailed explanations were included as examples.
- The answer choices for the questions were not deliberated.
- The final number of questions was to be about 30 questions (a maximum of 35 questions).
- For each question, we did not discuss the phrasing of the questions and only determined the following:
    - Which question to adopt
    - Which questions to combine
    - Keywords and details to add to the questions

As a result of the deliberations, the final 27 questions were determined. (Questions that were a combination of multiple questions were counted as one item.) Vigorous discussions were held regarding each question, but much of the discussion focused on the implementation of risk assessment, which was proposed by a member. In the discussion, the opinions voiced included statements such as “risk assessment is essential to information security measures and should be included in the questions,” “risk assessment should be conducted as a precondition of information security measures and should not be included in questions regarding the implementation of measures but instead should be included as an explanation,” and “won’t there be

companies that will be daunted by items regarding risk assessment (especially at the beginning of the questionnaire)?" Finally it was determined that an explanation of the positioning of risk assessment and information security measures will be provided as a note, and the item will be added as one question item.

(5) Documentation and Finalization of the Questions

Based on the questions determined in (4), the members and concerned parties in Japan created a draft of the wording for each question. This draft received approval from the WG and was formulated as the final common questions. Refer to 3.2. for the common questions formulated by the WG.

After the members agree on all issues that appear in the Common ISM Benchmark, the members propose the model to review the Common ISM Benchmark in the future by using the same process as the first developed Common ISM Benchmark.

3.2.2. Common Questions

Table 3.2. shows a list of the common questions.

Table 3.2. List of the Common Questions

No.	Common Questions
Q1 Organizational approaches to information security	
Q1-(1)	**Does your company have any policies or rules for information security and implement them?** (It is important to establish policies/rules based on your company's business and operational risk, rather than just applying a simple copy of a sample or template. To ensure the enforcement of those policies and rules, you need to improve the understanding of policy/rules among employees as well as collaborators and encourage them to comply with policy/rules, check the state of implementation, and review those policy/rules on an as-needed basis.)
Q1-(2)	**Does your company evaluate dangers and vulnerabilities regarding the security of vital information assets within your organization in deciding security rules and countermeasures?** (Such procedure is named "risk assessment". It is important to establish procedures for information security risk assessment and review the risk and countermeasures regularly for implementing cost-effective and efficient countermeasures.)
Q1-(3)	**Does your company have an organizational framework which includes the management to promote information security as well as compliance with law and rules?** (To build a framework to promote information security, it is important for the management to exercise their leadership and clearly state the responsibilities assigned, for example, to the division or person in charge of information security. It is also important for you to have a clear, full understanding of legislation, standards, and regulations that should be followed in doing your business.)
Q1-(4)	**Are the key information assets (i,e., information and information systems) classified based on their level of importance? And are there any rules and documented procedures to manage such assets based on their level of importance?** (To manage information assets in an appropriate manner, those assets should be classified into multiple groups based on their level of importance; rules and documented procedures should be established to manage such assets; and a person in charge of information management should be assigned.)

Q1-(5)	**Does your company exercise appropriate security measures to protect key information (including personal data and confidential information) in each phase of the information life cycle, including acquisition, creation, utilization, saving, exchange, provision, deletion and disposal?** (Appropriate information management includes clarifying operational procedures (e.g., labeling and disposal of important data) and the person responsible for the operation, limiting the number of operators who can perform a specific operation, recording operational history, and checking operations. These tasks need to be implemented regardless of whether the operation is performed manually or by means of information systems.)
Q1-(6)	**Are information security requirements included in your company's written contract, which is exchanged when you outsource your business operation or information system management to a contractor?** (These requirements should be satisfied to prevent information leakage, loss of data, or misuse of information and information systems, etc.)
Q1-(7)	**Does your company make clear to its employees (including temporary staff) security obligations, which include, for example, nondisclosure agreements signed when they enter or leave your company?** (To ensure that everybody within the company satisfy information security requirements, the company needs to assign a person responsible for it and to conduct clear succession of duties in case of personnel changes, to make clear the rules to be followed, and to let everybody know about them.)
Q1-(8)	**Does your company give its employees (including management and temporary staff) security education and training regularly to teach them the company's approaches and associated rules regarding information security?** (It is important to regularly provide all the employees with security education and training that cover security requirements, prohibited matters, information security threats and countermeasures, and how to prevent, or respond to security incidents, etc.)
Q2 Physical (Environmental) security controls	
Q2-(1)	**Does your company implement security countermeasures required for the rooms, buildings and sites where you want to improve security?** (Countermeasures include separating such sites from outside using a gate, wall, or access control devices, keeping access logs, and setting up alarm devices or fire prevention device. It is necessary to assign employees who maintain those facilities and devices. It is important to divide such area into multiple sections (e.g., a delivery-and-receipt room, a working area for outside contractors) from the aspect of security.)
Q2-(2)	**Does your company formulate and enforce any security-related rules for the people**

	moving in, or moving out of your company, including clients, vendors, common carriers, and cleaners? (More people than you imagine can visit your company. It is important to establish security rules that should be followed by the visitors and to keep visitors' log.)
Q2-(3)	**Are the important information equipment and wires/cables placed correctly and set up in safety so that they are protected against natural and man-made disasters?** (Safety placement and setup refer to placing information equipment and wires/cables in a safe place so that they are protected against unauthorized access and tapping, putting wires/cables underground or under floor, and installing devices and systems in a safe place so they are protected against natural disasters (e.g., water leakage, fire, earthquake).)
Q2-(4)	**Does your company handle in an appropriate manner important documents, mobile PCs, and removable storage media (e.g., CD-ROM)?** (Appropriate management refers to lockable filing cabinets, taking printed documents away from printers or other output devices immediately, breaking up storage media for secure disposal, and keeping a log or diary of your use and disposal, etc. Important documents include information-system-related documents as well.)
Q3 Operational controls for information systems and communication networks	
Q3-(1)	**Does your company protect in an appropriate manner information systems and data that are used in the actual operational environment?** (Appropriate protection refers to separating the development and test systems from the actual operational systems, implementing change control, restricting the use of actual data in the development systems etc.)
Q3-(2)	**Does your company implement security countermeasures required for information system operation?** (Appropriate security countermeasures include developing operational manuals, operating in accordance with the established rules and procedures, monitoring the state of implementation, keeping and regularly checking security logs etc.)
Q3-(3)	**Does your company have documented procedures for the backup of vital business data and related systems, and implemented them?** (Scheduled and systematic data backup is very important, as the backup data supports quick recovery from data loss, system failure or incident. If you fail to back up vital business data and related systems on a regular basis, you cannot restore such data in the event of system failure etc, which may result in serious adverse effect on your business.)
Q3-(4)	**Does your company take countermeasures against malware (e.g., computer viruses, Worms, Trojan horses, Bots, Spyware)?** (Countermeasures against malware include installing antivirus software, regularly updating pattern files, and applying security patches)

Q3-(5)	**Does your company take any countermeasures to mitigate vulnerabilities of the information systems used in your company?** (Appropriate countermeasures include configuring your system in consideration of information security, applying security patches, conducting version management and change management, and removing sample applications from the company's internal servers.)
Q3-(6)	**Does your company take appropriate protective measures (e.g., encryption) for data being transferred across communication networks as well as data stored on a public server?** (Appropriate protective measures include the use of Virtual Private Network (VPN), Secure Sockets Layer (SSL) or other secure protocols.)
Q3-(7)	**Does your company implement appropriate security countermeasures to protect storage media such as mobile PCs, USB memories, CD-ROMs, floppy disks, etc. in case of the loss, theft or other incidents of such media?** (Mobile PCs, USB memories, and other storage media can be used not only in your office but other areas (e.g., public spaces outside your company, remote offices, and users' homes). When such media is taken out, there is a higher risk of being stolen or lost, compared to when used in your home or office. Taking this into account, you need to implement appropriate countermeasures.)
Q4 Access control and security countermeasures for development and maintenance phases	
Q4-(1)	**Does your company perform appropriate user ID management, including adequate user identification and authentication, to restrict access to information (data) and information systems?** (Appropriate user ID management includes reviewing user IDs on a regular basis to remove unnecessary ones, restricting the use of shared IDs and folders, and forbidding the use of simple passwords.)
Q4-(2)	**Does your company implement appropriate access controls for information (data), information systems and business applications, including granting users adequate access rights for such resources?** (Appropriate access controls include restricting access to information (data) and information systems using the different levels of access privileges, limiting functions that can be used by each user, and reviewing access rights granted to users.)
Q4-(3)	**Does your company implement appropriate access controls for the company's networks?** (Appropriate network access controls include separating networks and conducting authentication for an access from outside your company. In using Wireless LAN, it is important to have an established access policy and to use an authentication scheme. In case

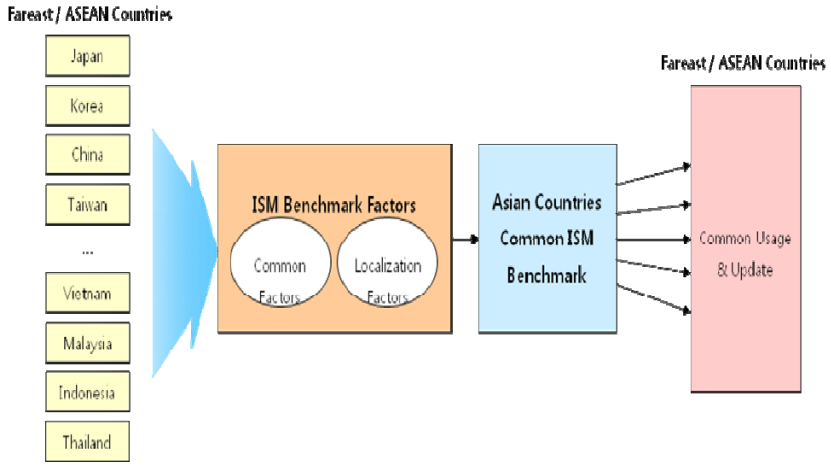
	of necessity such as electronic approval or e-commerce transaction data, you may consider using encrypted communication tunnel with VPN or other methods.)
Q4-(4)	**Does your company define security requirements for business application development and satisfy them in the design and implementation phases?** (Regardless of developing a system internally or outsourcing the system development to a contractor, security requirements should be included in the company's system specifications; the system should be designed and developed properly to avoid the creation of vulnerabilities; thorough system tests should be conducted so that vulnerabilities do not remain unfixed.)
Q4-(5)	**Does your company perform security controls for the selection and purchase of software products and/or the development and maintenance of systems?** (If your company is outsourcing to a contractor the selection and purchase of software products and/or the development and maintenance of systems, please answer this question from the aspect of whether your company can check the contractor's implementation status of security controls.)
Q5 Information security incident response and BCM (Business Continuity Management)	
Q5-(1)	**Does your company take appropriate measures against information system failures?** (Appropriate measures include applying system redundancy, performing system backups, keeping operational logs, clarifying procedures to be followed when a system failure occurs, concluding service level agreements with the service providers.)
Q5-(2)	**Does your company have written rules and procedures for security incident responses that describe how to act in a quick-and-appropriate manner when such incidents occur?** (To respond quickly and appropriately to security incidents, you need to examine steps that should be taken against such incidents, put the result of the study into writing, make concerned parties know about it, develop a telephone tree for emergency communications, and secure resources (including human resources) and equipment required. Incident response action should be documented and kept on files for future reference.)
Q5-(3)	**Does your company have a company-wide framework for BCM（Business Continuity Management) for the case of system down?** (The organization needs to prepare for a possible system down, such as by establishing procedures for manually performing the tasks implemented by the systems, and securing a place, resources, and equipment for conducting such activities. It is also important for the organization to educate and train its employees so they can manually implement those tasks.)

3.3. Framework and Challenges for Implementation

3.3.1. Open Accessibility to Each Country's Benchmark

Currently, there are very few Information Security Management System (ISMS) solutions for organizations with limited resources (time, money, manpower) in Asian countries. Some Asian countries and regions such as Korea, Japan, and Taiwan also developed benchmark tools. The level of e-readiness for those organizations is now increasing, and those organizations face the same security risks as large ones in the Internet environment. Those smaller-sized organizations represent the heart of the overall economical power in Asia. For small and medium-sized organizations, the ISM Benchmark is no longer a rich man's privilege—it is simple, affordable, and doable. Policymakers are interested in two factors: measurable and comparable tools. A common benchmark is necessary to reduce the effort of development and maintenance, to share information, and to level-up Asian countries information security. In order to develop a common benchmark, the tools developed and operated are actually based on international standards (IS). Thus, consideration of each country's benchmark items already in operation and consensus by Asian countries for their own views are the most efficient ways to create a common benchmark for Asia. It may become a de facto standard in Asian region. The idea of a consensus on a common benchmark is illustrated as follows:

Figure 3.1. Process of Developing a Common Benchmark for Asian Countries



In this figure, ISM Benchmark factors are dived into two parts: one is common factors selected by participants from each country and the other is localization factors based on each country's own environmental, infrastructural, cultural, and linguistic factors. A combination of common factors and localization factors is one of the best ways to adapt each country's situation, such as differences in IT levels, definitions of SMEs, and online and offline accessibility.

In the operation process, we must think about two important factors for data reliability: one is a method for securing the data (security of diagnosis data), and the other is a way to achieve data reliability (in order to use them as statistic data). These factors take into account when each county uses a common benchmark tool. Some other factors to consider during operation are data, analysis, and language. Where do we locate the data – central or local? Data stored locally is recommended for each country's security level (guidelines requested). Analysis of the ISM Benchmark may be centralized (optional) for updates, maintenance, and comparisons. Language and style are other important factors in each country. These are adapted by each country in

cooperation with the original tool developer. Based on the Common ISM Benchmark, the IT level of enhancement of security is estimated in the near future.

3.3.2. Challenges for Implementation of Common ISM Benchmark

In order to achieve our vision and goals for the Common Information Security Management (ISM) Benchmark that we offered in the last research and let the Common ISM Benchmark play its role, some challenges to implementation should be faced and overcome. These challenges are as follows:

(1) A Dependable Entity is needed to Develop, Operate, and Maintain the Common ISM Benchmark System.

If we want the Common ISM Benchmark to serve the organizations in Asia, an application system should be developed. The application system should be operated via the Internet for free access by Asian organizations.

It is not nearly enough if we only complete the development of the Common ISM Benchmark system, an entity is also needed to install, operate, and maintain the system during operation. As an information system, various unexpected problems, such as software bugs, hardware faults, malware, network attacks, and human error may occur during operation that can cause business interruption. An operator should be assigned to deal with these problems.

The Common ISM Benchmark system should also be upgraded constantly to correct bugs, improve capabilities, and extend functions so that it will be better able to meet the needs of its users.

In addition, funds for application development, operation, and maintenance, as well

as server hosting, Internet communication, and other necessary expenses are also a problem. The application is built not for profit definitely, so we have to find funds to support its operation.

Like the Japan ISM Benchmark system run by Information-Technology Promotion Agency (IPA), we should choose a dependable entity to run the Common ISM Benchmark. To deal with this challenge, we propose that ERIA establish sustaining funds for implementation of the Common ISM Benchmark system, including development, operation, and maintenance of the system. The entity that develops and operates the benchmark application would be chosen by ERIA through outsourcing, and the object of outsourcing should include the following:

- Benchmark application development.
- Benchmark application operation and maintenance
- Server hosting
- Application security

(2) Each Country would worry about the Sensitivity of the Collected Data under the Common ISM Benchmark System.

Information security issues have become more sensitive in every country, especially the government sector nowadays, and in particular data security. Every country's government sector would be quite cautious about data collection by an Internet application like the Common ISM Benchmark system unless the system operates independently.

The Common ISM Benchmark system will collect many kinds of data concerned with security from many organizations in many countries, and the collected data will be

analyzed by the entity that operates the system. The result of the data analysis may be sensitive and unexpected use would be a cause for concern by many countries even the users of the system.

To deal with this challenge, our proposals are as follows:

- The goal of the Common ISM Benchmark should be clearly announced to every country and every user. In particular, is the benchmark will only be used in the business sector not the government sector. The benchmark is not mandatory but a recommendation decided by the organization as to whether to use it.
- The entities that develop and operate the system would be chosen by ERIA through independent public means.
- The impartiality of the implementation of the system should be ensured and made known to the public.
- ERIA should formulate a policy to avoid abuse of the collected data with a pop-up warning before the user enters the system.
- The implementation of the system should be monitored and audited by a third independent party.

(3) How many Organizations would Actually Use the Common ISM Benchmark System in Asia?

Most organizations know other information security management tools well, like ISO/IEC 27001, OCTAVE, and some domestic information security management tools (e.g. China Classified Protection of Information Security (CPIS), also named as Multilevel Protection Scheme (MLPS)). For example, in Japan, 3,378 organizations

have earned ISO/IEC 27001 certification as of January 2010.[12] In China, more than 30,000 organizations have implemented CPIS up to now.

By comparison with those tools mentioned above, the Common ISM Benchmark system is a new arrival. Organizations do not know about the Common ISM Benchmark or the benefits it will bring. So it would take a long time to make the Common ISM Benchmark system known by Asian organizations.

On the other hand, we are not sure the Common ISM Benchmark will be competitive with those tools mentioned above for Asian organizations. After all, it has not been widely used by Asian organizations, so we are also not sure whether the function of the Common ISM Benchmark system will actually meet the needs of users.

If no organization uses the Common ISM Benchmark system, our efforts will come to nothing. To deal with this major challenge, we propose that the following:

- The Common ISM Benchmark should be broadly promoted on the Internet, in every country, and among each international organization (e.g. ASEAN, ASEAN+1, ASEAN+3, ASEAN+6, APEC, etc.).
- The difference between the Common ISM Benchmark and other information security management tools should be distinguished and explained to users.
- The function and effectiveness of the Common ISM Benchmark system should be improved and strengthened constantly.

(4) How can We Provide Organizations Further Solutions to Each Item of the Common ISM Benchmark?

We ask organizations around 30 questions about information security protection in

[12] Data source: www.iso27001certificates.com.

the Common ISM Benchmark but do not provide solutions to these questions at this time. Most organizations can answer the questions but do not know how to correctly solve the problem. There is no doubt that understanding the security weaknesses and determining the security level are not the organization's ultimate objective.

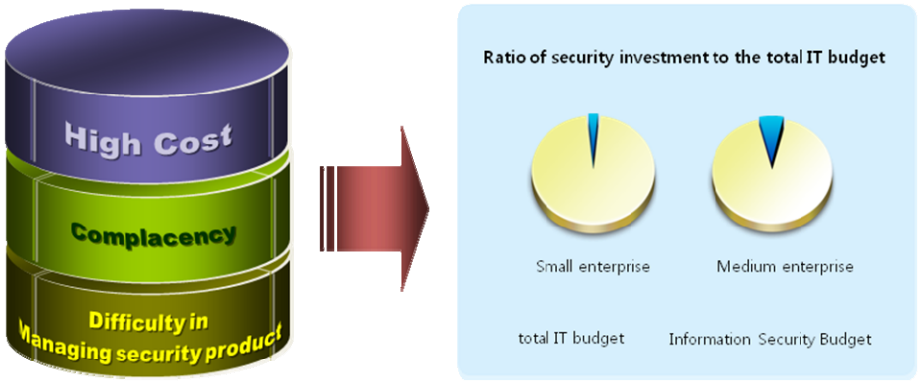
By providing recommendations and solutions to each item of the Common ISM Benchmark, we can achieve our vision and goal. So we propose that further research be conducted on how organizations should address security risks described in the Common ISM Benchmark.

3.3.3. Country-Specific Issues (Korea)

Challenges for Implementation of Common ISM Benchmark in Korea

In Asia, many enterprises are small and medium sized. In small and medium-sized enterprises (SME), introduction to security measures is not the first priority. The construction of infrastructure, website development, and ordinary operation may be much more important in the budget than security product installation. The CEO's lack of concern about security is another obstacle to the introduction of security products and budget increments. These obstacles are illustrated in Figure 3.2.

Figure 3.2. Major Obstacles to Security Product Introduction

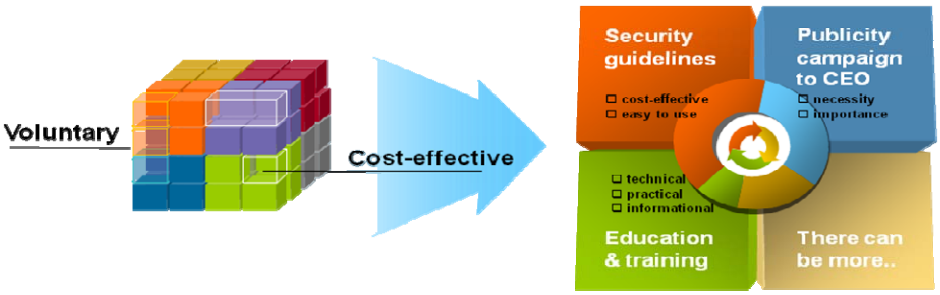


Source: Korea Internet & Security Agency (KISA).

In order to overcome the problems mentioned above, new direction and action plans for security guidelines and self-assessment tools were introduced by the Korean government, Korea Communication Commission (KCC). The aim is to enhance the security level of SME with voluntary and cost effective security measures. Security awareness, security goals, and easy to use guidelines are three major factors. The

concepts of the directions are illustrated as follows:

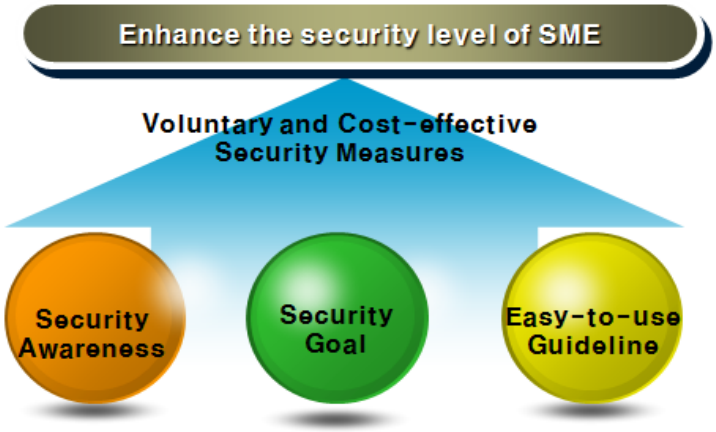
Figure 3.3. Direction of Action Plans in Korea



Source: Korea Internet & Security Agency (KISA).

Security guidelines take into account the security requirements for each component of IT infrastructure type, security levels, and assets. Based on the guidelines and action plan, an Information Security Management System (ISMS) Benchmark tool was developed by Korea Internet & Security Agency (KISA) for self-assessment of each company's level of security. Using voluntary and cost-effective security measures, the SME can enhance the security level.

Figure 3.4. IT Level Enhancement (Benchmark Tool + Guideline)



In Korea, the Korea Internet & Security Agency (KISA) is in service with ISMS Benchmark since 2002. A total of 77 companies acquired certification under the ISMS Benchmark by the end of 2009. KISA's ISMS Benchmark questionnaire is called the Information Security Assessment Tool for SMEs Questionnaire and contains 57 items. Test results are provided in a table in a simple and easy-to-understand presentation. Test results are provided along with suggestions for improvement and solutions on the security holes detected. The test, available at KISA's website (http://www.kisa.or.kr), consists of a series of multiple-choice questions that may best be answered by someone familiar with a company's information system like an IT officer, chief information officer (CIO), or chief executive officer (CEO).

The items are categorized as follows:

- Information infrastructure: 10 questions
- Reliance on Information Systems
    - Reliance on computer systems: 6 questions
    - Information system reliance assessed through impact of security incidents: 6 questions
- Security Readiness
    - Policy and organization: 6 questions
    - System management: 15 questions
    - System maintenance and security response: 3 questions
    - Protection of data: 3 questions
    - Physical environment: 3 questions

KISA's ISMS Benchmark is developed under the ISO standards of the 27000 series. An example of the certificate of the ISMS Benchmark is shown in Figure 3.5.

Figure 3.5. KISA's ISMS Benchmark Certificate

Certificate Number :

CERTIFICATE
of Information Security Management System

Name of Organization :
Name of Representative :
Address :
Scope of Certification :
Period of Validation :

This is to certify that the above mentioned organization is compliant to the assessment standard for Information Security Management System certification in accordance with Article 47, Paragraph 1 and 4 of 「Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.」, and Article 50, the Enforcement Decree of the Act.

Date of Issuance :

Signed by :

Hee-Jung Kim, President of Korea Internet & Security Agency

인증번호 :

정보보호관리체계 인증서

상호 또는 명칭 :
대 표 자 :
소 재 지 :
인증의 범위 :
유 효 기 간 :

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제1항 및 제4항, 같은 법 시행령 제50조에 따라 위와 같이 정보보호관리체계를 인증합니다.

발행일 :

한국인터넷진흥원장

Source: Korea Internet & Security Agency (KISA), http://isms.kisa.or.kr/isms/jsp/isms_7010.jsp.

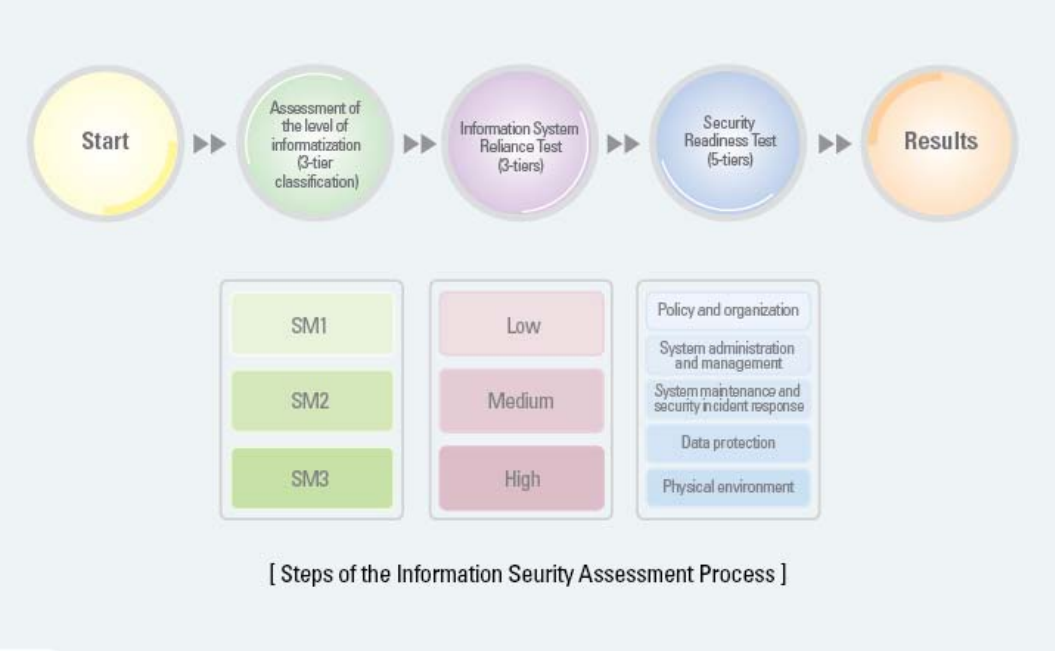
The company of accreditation can use the logo of ISMS mark in its product. The logo is shown below:

Figure 3.6. Logo of ISMS Certificate

Source: Korea Internet & Security Agency (KISA), http://isms.kisa.or.kr/isms/jsp/isms_7010.jsp.

The overall procedure for the ISMS process is shown in Figure 3.7.

Figure 3.7. Process for ISMS Benchmark



Source: Korea Internet & Security Agency (KISA).

The steps for the ISMS Benchmark are explained as follows:[13]

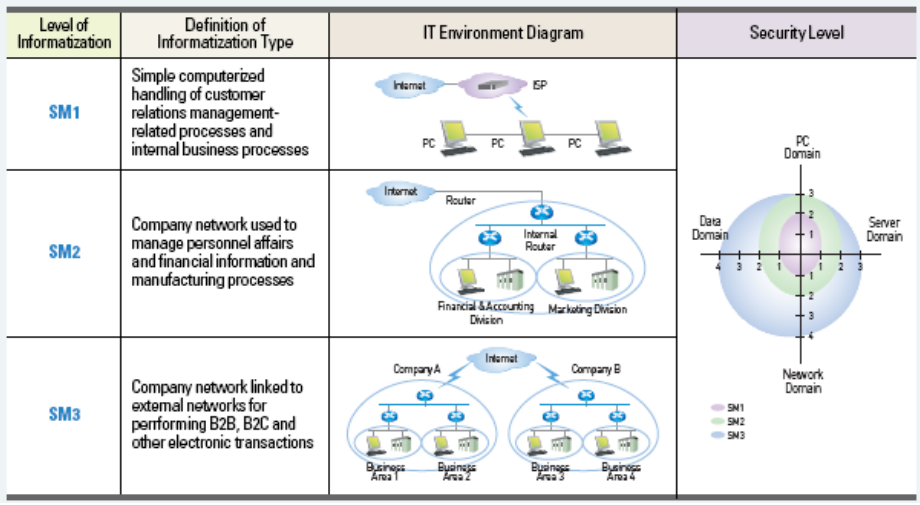
Step 1: Assessment of the Level of Informatization

The first step in the assessment process consists of determining the level of informatization of the company. Small and medium-sized enterprises are classified according to a three-tier classification system (SM1, SM2, SM3). Each of the three classifications corresponds to the size of IT assets; IT assets handled by SM3 systems, for instance, are larger than the SM1 or SM2 system, and the level of security needed is higher. The definitions for each of the three types of informatization and the

[13] Korea Internet & Security Agency (KISA), http://isms.kisa.or.kr/isms/jsp/isms.jsp.

respective security requirements are provided below.

Figure 3.8. Definition of Informatization Types and Related Security Requirements[14]



Step 2: Information System Reliance Test

Companies belonging to the same informatization type can, nevertheless, differ from each other in terms of the sensitivity of information assets, impact of a security incident on business operation, and reliance on external information systems. Hence, to determine the appropriate target security levels, the assessment classifies companies according to the level of reliance on informatization systems into three types: low, medium, and high.

Step 3: Security Readiness Test

Next, the assessment measures the level of security in five areas: policy and

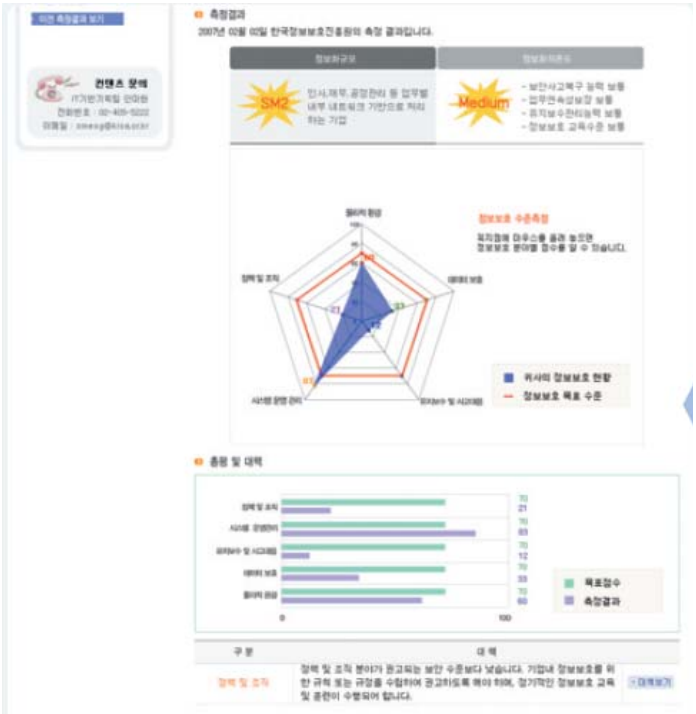
[14] SM: Small and Medium, B2B: Business to Business, B2C: Business to Consumer.

organization, system administration and management, system maintenance and security incident response, protection of data, and the physical environment. It is during this stage that the adequacy of implemented security solutions is assessed, and any areas needing improvement are identified.

Step 4: Result Reporting

This is the final step in the evaluation where the user is presented with a test report. Bar graphs and radial diagrams used in the report give users a snapshot of the level of security readiness of their company's information system. For any vulnerabilities detected, companies are referred to security solutions detailed in the information security guidelines for small and medium-sized enterprises, also available on KISA's website.

Figure 3.9. Test Report



3.3.4. Country-Specific Issues (Vietnam)

Challenges for Implementation of Common ISM Benchmark in Vietnam

This report presents country-specific issues by implementing the Common Information Security Management Benchmark (Common ISM Benchmark or the ISM Benchmark) in the business sector in Vietnam. In order to summarize the findings in this report, a survey on the trial use of the ISM Benchmark was conducted from December 2008 to February 2009 to obtain opinions and feedback from 14 selected Vietnam enterprises of different sizes and in different industries. Moreover, two other companies engaged in overseas trade had been selected for 15 interview questions in February 2010. Although the sample size of the survey was small, we studied the need for the Common ISM Benchmark and possible issues by implementing the ISM Benchmark, which can be seen from actual companies regarding the country's specific issues.

The survey results showed that the major information security challenges for enterprises in Vietnam are the lack of a legal basis for information security, lack of security policies, lack of information security awareness, lack of professional security personnel, lack of security training, inadequate investment in security, and insufficient implementation of information security countermeasures.

Based on the study of the survey results and the current status of information security in Vietnam, essential issues and challenges for implementing the ISM Benchmark in Vietnam can be identified as follows:

- What is the key driver for the successful implementation of the ISM Benchmark?
- How can the ISM Benchmark be successfully deployed?
- How can the ISM Benchmark better meet the demands of companies?

・ How to realize the mutual reorganization of different companies and organizations in Vietnam by maintaining the Common ISM Benchmark?

In the following paragraphs, we will discuss these specific issues and try to point out the possible countermeasures for successful implementation of the ISM Benchmark.

(1) Key Driver for the Successful Implementation of the ISM Benchmark

a) Legislation Environment

Vietnam is in the process of gathering information to make proposals for amendments to its laws regarding information security. The growth of information security issues has prompted legislatures to take action. Extending the rule of law into cyberspace is a critical step in creating a trustworthy environment for implementation of the ISM Benchmark.

To address information security matters in Vietnam, Vietnam Emergency Response Teams (VNCERT) were established in 2005 as a government agency under the Ministry of Post and Telematics (called the Ministry of Information and Communications since 2007) to be responsible for all national information security activities in the country.

Existing laws are likely to be unenforceable with respect to cybercrimes. There is still no assessment of the status of current laws to determine whether they are sufficient to combat cybercrimes. Lack of legal protection means that businesses must rely solely on technical measures to protect their information systems themselves.

With the contribution of VNCERT, the Vietnamese government has recently issued a number of decrees and regulations relating to information security, such as Direction 03/2007/CT-BBCVT for information security on the Internet, Decree 64/2007/ND-CP for secure information communication technology (ICT) applications, Decree

97/2008/ND-CP for Internet regulations in order to replace the obsolete Decree 55/2001/ ND-CP, Decree 90/2008/ND-CP for an anti-spam measure, Joint-Circular 06/2008/ TTLT-BTTTT-BCA for protecting the information infrastructure, and Decision 58/2008/BTTTT and Decision 59/2008/BTTTT for implementing the PKI structure and Root CA system in Vietnam. However, effective law enforcement is complicated by the nature of cyberspace, and there is still deficient practical deployment of laws. Many of the other necessary legal documents are underway.

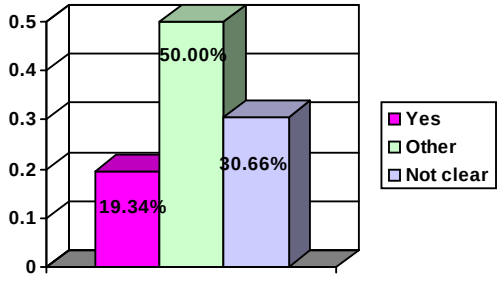
On the other hand, few information security specific events and program initiatives of the government have been conducted in recent years including establishment of Vietnam's Information Security Association (VNISA), annual organized National Security Day, and Vietnam Security World, as well as several workshops on information security.

At the macro policy level, at the beginning of 2010, a significant plan came into effect, namely the Prime Minister's Decision 63/QD-TTg (dated 13 January 2010) approving the 2010-2015 Master Plan for National Information Security and Vision for 2020. This first National Master Plan for Information Security covered four key objectives including: (1) IT applications for e-government and e-business; (2) Nation critical information infrastructure; (3) Laws, regulations, policies on cyber security; and (4) Human resources development for cyber security.

With the efforts of VNCERT, the Department of Science and Technologies under Ministry of Information and Communications, and Ministry of Science and Technologies of Vietnam, several IT security standards have been developed and adopted including TCVN-7562 (adopted from BS7799), TCVN-27001 (ISO/IEC 27001), TCVN-15408 (ISO/IEC 15408). However, very few organizations have received

Information Security Management System (ISMS) certification based on ISO/IEC 27001 until now. According to a survey by VNCERT in 2008, only 19.34% of companies expect to obtain ISMS 27001, 60% expect other standards, more than 30% do not know of any standard (see Figure 3.10.). This figure reflects the deficient awareness of information security standards and the deficient deployment of standards.

Figure 3.10. Percentage of Companies Expecting to Use ISO/IEC 27001



In conclusion, the ISM Benchmark can be only successfully implemented with the support of the government through legislation and enforcement.

b) Consensus on the Common ISM Benchmark

Various opinions, both in the business sector and in government, have been given regarding the issue of IS management. There is a broad consensus among companies and organizations as to the kinds of measures that should be undertaken by organizations. A Common ISM Benchmark for IS assessment is a basic necessity. The answers of 14 companies in the survey from December 2008 to February 2009 showed evidence of the need for an ISM Benchmark. All of the companies in this study (14/14) thought that a Common ISM Benchmark was urgently needed.

However, in order to successfully implement the ISM Benchmark, stronger requirements, obligations, and recommendations should be addressed by information

security laws and regulations. Enforcement of existing laws and regulations should be synchronized with improvements to the IT infrastructure and increased awareness by the community. To promote the adoption of a Common ISM Benchmark, there is a need to include various stakeholders, including relevant government agencies, industry associations, and enterprises in the implementation of such an ISM Benchmark.

In the case of Vietnam, VNCERT could be the representative entity for developing and implementing the ISM Benchmark because an objective evaluation for organizations is needed. VNCERT is now in charge of a public awareness improvement program and responsible for all national information security activities. VNCERT is nationwide recognized as an agency for national information security governance management. Therefore, VNCERT is a unique agency that on behalf of the government has the right to host local survey data, can protect the collected survey data on a local national server, and could legally share local survey data between various stakeholders according to the policy of ERIA.

(2) How can the Information Security Management (ISM) Benchmark be Successfully Deployed?

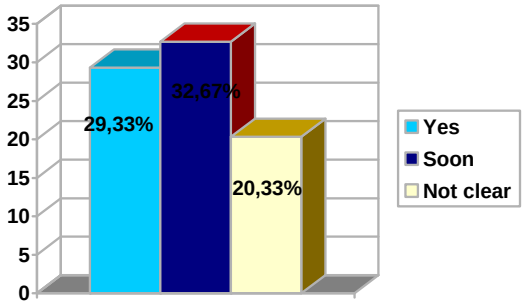
a) Improving Information Security Awareness for the Business Sector

Leaders of companies recognized the importance of the protection of their information assets, but they are not always aware of how to implement specific countermeasures. In line with this issue, many companies do not know how to deal with the specific items in the regulations and standards related to information security issued by the government.

According to various surveys, the findings reflected the fact that many enterprises

still have not taken enough countermeasures in preventing or tackling attacks. Many companies did not invest enough in incident response procedures and security policies. Among 400 responding organizations, only 29.33% had implemented a security policy, 32.67% wanted to have one soon, and 20.33% did not know of a security policy (Figure 3.11.). Fifty-two percent of companies showed a lack of awareness by users and 43% of companies indicated a lack of awareness within the organization.

Figure 3.11. Percentage of Companies with a Security Policy



Due to the lack of awareness of information security, many companies are not committed to IS countermeasures nor do they allocate the necessary resources (budget, personnel, instruments, regular software patches).

For successful adoption of the ISM Benchmark, an awareness improvement program for the business sector should be implemented beforehand, in order to raise awareness of the need and the benefits of the ISM Benchmark through the following:

- Check the company's IS level;
- Identify the problem domains with regard to information security;
- Obtain advice on necessary information security measures;
- Identify the deficiencies and the areas for further improvement;

- Compare the information security level to the average;
- Report the IS level to clients and customers.

For awareness improvement programs, funds should be provided annually regarding development of propagation documents, translation into the Vietnamese language, maintenance of the local server, and other expenses.

Specific ISMS training should also be provided for company personnel. The lack of personnel responsible for information security by business had been indicated in the results of a survey conducted in recent years. According to a survey of 400 companies in 2008, approximately one-half of the companies (44% in the whole country, 38.4% of companies in the south, 48.5% of companies in the north) had no personnel responsible (either direct or indirect) for information security. There was no Information Security Management System (ISMS) training for those persons (See Figure 3.12.).

Figure 3.12. Percentage of Companies Having Personnel Responsible for IS

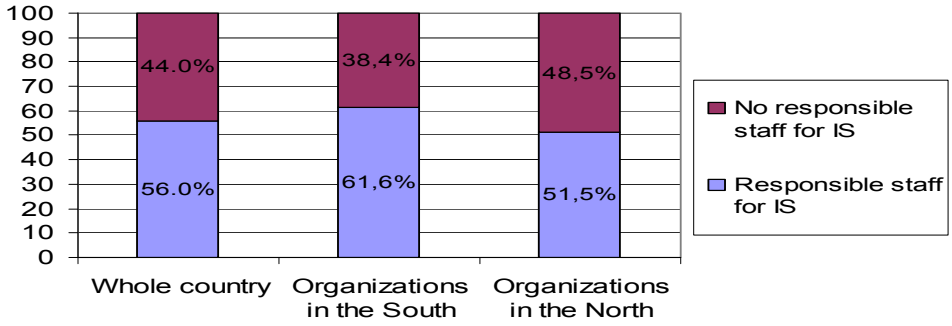
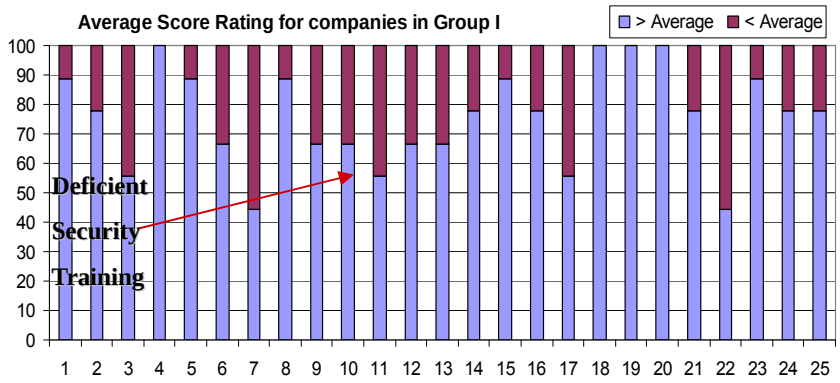


Figure 3.13. presented the average score rating for 25 questionnaires conducted by an IPA[15] survey from December 2008 to February 2009. The survey results also showed a deficiency in security training (See Figure 3.13.).

[15] http://www.ipa.go.jp/security/english/benchmark_system.html.

Figure 3.13. Column 3 Presents the Average Score Rating for Security Training



For adoption of the ISM Benchmark, annual training programs should be provided to improve the level of awareness of employees on the use of the ISM Benchmark and necessary ISM measures within the company.

b) Customization and Local Language

According to the survey of 14 companies from December 2008 to February 2009, almost all were of the opinion that the ISM Benchmark is an effective, and easy-to-use tool. However, some respondents thought that this self-diagnostic was still general and did not include detailed explanations on practical use. They wanted to have additional questionnaires, functions, and information on the assessment results.

Further development of the ISM Benchmark for national use had been suggested including the following:

- Add some country specific questions for further analysis;
- Provide additional information and hints on the output results;
- Support local servers for collecting local survey data from companies and for comparing within the domain;
- Translate into the Vietnamese language.

In order to customize and translate the ISM Benchmark, funds for further development should be provided and further investigation of the practical application of the ISM Benchmark should be carried out.

c) Regular Updating and Improving the ISM Benchmark

A comprehensive feedback learning mechanism can be seen as a critical challenge for the ISM Benchmark. Monitoring the outcome of enterprise processes supports the critical feedback loop required for producing better services from the ISM Benchmark in the future. This learning/feedback mechanism should be a fundamental characteristic. The functionality and affectivity of the ISM Benchmark should be regularly maintained.

d) Annual Assessment

By conducting assessment with the ISM Benchmark, companies often raise the following questions: Is the company more secure now than it was last year? Are we spending too little or too much? Which of our security investments are producing the most cost-effective results?

Companies want to conduct regular benchmark studies in order to establish a performance baseline upon which improvements can be made and measured. If benchmarking is not conducted on a regular basis, it may happen that the best practices initially implemented will no longer be deemed competitive in subsequent years. Customer and business satisfaction should be conducted at least annually to determine the levels of end-user satisfaction and identify areas of improvement.

(3) How can the Information Security Management (ISM) Benchmark Better Meet the Demands of Companies?

By implementing the ISM Benchmark, the following questions may arise regarding the need for information security by companies:

- How well can the ISM Benchmark assess company's information security measures?
- Does the ISM Benchmark reflect needs of companies in assessing the information security level?

Based on the trial use of the ISM Benchmark for 14 companies, the common response was that the questions covered all aspects of organizational, technical, physical, environmental, and human security measures in a good balance. The ISM Benchmark covered five essential sections of IS corresponding to the basic requirements of IS management at a high level. It reflected the rapid changes in the IS environment of the organizations. Basically, the existing functions of the ISM Benchmark already met the needs of companies for IS level assessments. The assessment process was simple with several tips and hints for answering the questions and provided quick graphical output results.

Nevertheless, several respondents suggested the addition of country specific questions for further analysis. They wanted additional information on the output results and more hints for answering the questions using the detailed checklists. For instance, from the question on organization policy, they wanted detailed hints on specific policies regarding information protection, incident response, etc.

One possible solution may be to provide a multiple checklist for the answer. Assessment results will offer more information on deficient countermeasures and more

hints for improving deficient security issues.

On the output results of the ISM Benchmark, companies should be able to understand the security weaknesses and obtain recommendations for solutions to each question regarding the corresponding security measures in order to develop procedures to overcome the information security deficiencies.

(4) How to Realize the Mutual Reorganization of Different Companies and Organizations in Vietnam by Maintaining the Common Information Security Management (ISM) Benchmark?

At the national level, more obligatory requirements on protecting infrastructure and building secure business environments are necessary. A number of programs in relation to the first National Master Plan should be implemented, including (1) infrastructure protection for both public and private sectors; (2) building a secure environment for developing IT applications and services; (3) further developing and implementing laws and regulations for information security; and (4) developing and implementing training and awareness improvement programs.

It is necessary to systematically build a coordination mechanism for mutual information checking between companies by developing a common check sheet and establishing auditing firms. The ISM Benchmark should provide a common check sheet and a way to check the supplier's IS level and to report the IS level to/from different clients. The national authority of the ISM Benchmark should provide a shared medium and mechanisms for confirming the IS level of business partners.

(5) Conclusion

The report pointed out several issues, challenges, and some countermeasures for implementing the Common ISM Benchmark in Vietnam. We believe that stronger law enforcement with obligatory requirements and detailed recommendations will be the key driver for successful implementation of the ISM Benchmark. More awareness improvement programs for leaders and employees of companies on the benefit of ISM Benchmark as well as necessary ISM measures should be provided nationwide. Further development and research on the ISM Benchmark should be taken in order to localize the ISM Benchmark and to regularly update the ISM Benchmark to meet the demands of the business sector in Vietnam. A local agency should be chosen for the customization, operation, and maintenance of the ISM Benchmark for the mutual acceptance of companies on the common check sheet as the result of the Common ISM Benchmark. In this way, we would be able to build a more secure infrastructure and secure environment for the business sector in Vietnam.

3.3.5. Country-Specific Issues (Malaysia)

Challenges for Implementation of Common ISM Benchmark in Malaysia

The Information Security Management Benchmarking (ISM Benchmarking) tool is a new application in Malaysia, and a lot of effort and consistence pursuance is expected for it to be accepted by the targeted users. Most organizations in the country use the ISO 27001-Information Security Management System (ISMS) for information security. Therefore, the use of the ISM Benchmarking tool at the national level is considered an ambitious project as the concept and the application needs to be accepted by all relevant organizations in the public and private sectors.

The tool is intended to assist small and medium-sized enterprises (SME) to gauge the information security status among other organizations within their business sectors. This is because SME tends not to have dedicated programs and resources on information security, and with 99% of the total business establishment in Malaysia in this category, it is clear that promoting the use of such a tool will be a major task. However, the tool can also be used by corporate organizations for the same purpose

This will require many engagement activities to make potential users understand and accept the use of the ISM Benchmarking tool. However, after all the efforts, there is no guarantee that the organizations will use the application.

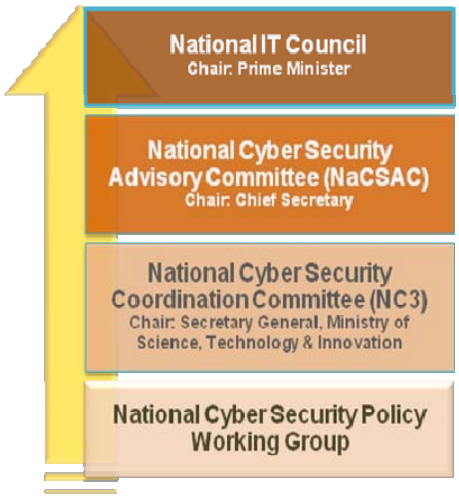
Some of the challenges that need to be considered in the implementation of the ISM Benchmarking tool in Malaysia would be as follows:

(1) Stakeholders' Support

Policymakers in the country need to involve in preliminary engagement activities in order to make this group understand why the Information Security Management (ISM) Benchmarking tool needs to be used. It is imperative to make the policymakers understand the objective of the tool and the benefit it will bring to the country. This is to obtain the necessary stakeholder support from across the ministries and agencies that have authority over users.

In introducing the ISM Benchmarking tool, it is recommended to approach the stakeholders in the committees involved in the implementation of Malaysia's National Cyber Security Policy (NCSP). These committees oversee the initiatives of information security in Malaysia, especially cyber security since the year 2007. The committees, as shown below, consist of members from various ministries and agencies. Each committee is represented by the different management level.

Figure 3.14. Cyber Security Committees in Malaysia – Reporting Structure and Members



1. Malaysian Administrative, Modernization and Management Planning Unit
2. National Security Council, Prime Minister's Dept.
3. Attorney General's Office. Prime Minister's Dept.
4. Chief Government Security Officer's Office, Prime Minister's Dept.
5. Ministry of Science, Technology & Innovation
6. Ministry of Defense
7. Ministry of Foreign Affairs
8. Ministry of Energy, Green Technology & Water
9. Ministry of Finance
10. Ministry of Information Communication & Culture
11. Ministry of Transportation
12. Ministry of Home Affairs
13. Central Bank of Malaysia
14. National Water Services Commission
15. Malaysian Communication & Multimedia Commission
16. Energy Communication
17. Security Commission Malaysia
18. CyberSecurity Malaysia

Starting from the bottom, the National Cyber Security Policy Working Group consists of eight (8) groups. Each group represents the respective policy areas as follows:

1. Effective Governance
2. Legislative & Regulatory Framework

3. Cyber Security Technology Framework
4. Culture of Security and Capacity Building
5. Research and Development Towards Self Reliance
6. Compliance and Enforcement
7. CyberSecurity Emergency Readiness
8. International Cooperation

These working groups implement the action plans of the NCSP. In addition, new initiatives are also formulated at this level to accomplish the task provided by the action plans and to accomplish the objectives of the policy.

The working groups report to the National Cyber Security Coordination Committee (NC3), which is chaired by the secretary general of the Ministry of Science, Technology and Innovation (MOSTI) and comprises senior management from the respective ministries and agencies. The NC3 spearhead the implementation of the NCSP and cyber security initiatives in Malaysia. In this committee, cyber security agendas formulated by the working group are tabled and reviewed. It is decided in this committee if the agendas tabled are in line with the NCSP. If such agenda falls within the NC3 purview, then it will be endorsed for implementation.

However, if the NC3 is of the opinion that such an agenda needs a higher mandate, then it is brought to the National Cyber Security Advisory Committee (NaCSAC), which is chaired by the chief secretary to the government. This committee, consisting of the highest level of officers in the respective ministries and agencies, provide an advisory role on the implementation of the NCSP. All cyber security agendas at the national level and that need a higher mandate will be presented here for endorsement. Other agendas that have been approved by the NC3 are also presented for information

and support from this committee.

Finally, all major cyber security agendas are brought to the National IT Council, which is chaired by the Prime Minister. With the acceptance and endorsement at this level, the agenda will become a national initiative to be implemented by all public and private sectors in the country.

Therefore, it is highly recommended that the implementation of the ISM Benchmarking tool in Malaysia receive the support of these committees, as it will facilitate the acceptance and implementation of the tool. The implementation needs to be synchronized among the regulators through the issuance of directives to the organizations under their respective purview.

(2) Ownership of the Information Security Management (ISM) Benchmarking Tool

Acceptance and endorsement of the committees overseeing the implementation of cyber security initiatives in the country provide the mandate to start the journey to reach out to users. Such activities will need a champion, and we recommend that the implementation of the ISM Benchmarking tool be coupled with the NCSP under MOSTI. CyberSecurity Malaysia, as an agency under the purview of this ministry and currently implementing the NCSP, shall be mandated to carry the responsibility to implement this tool along with the NCSP.

This will provide a custodian for the ISM Benchmarking tool in Malaysia. Due to the sensitivity of the data that will be collected, the ISM Benchmarking tool should be operated and maintained locally by a trusted local party. It is expected that it would be a stumbling block if the tool were managed by foreign parties because the users would be very reserved in revealing any information about their organization information

security status. This is also true if the database of the ISM Benchmarking tool can be accessed by foreign parties under the pretext of information sharing. When maintained locally, it will allow the tool to be upgraded constantly according to local needs and the local information security environment.

With the mandate given by the NCSP committees, CyberSecurity Malaysia will spearhead the implementation by coordinating efforts among the various stakeholders. It is foreseen that high level meetings, discussions, and workshops need to be conducted to educate and provide awareness and understanding to the stakeholders about the ISM Benchmarking tool. These stakeholders will be the ministries and agencies that have regulating powers that will be able to provide directives to the relevant organization under their purview to use the tool.

The initial task is to develop an implementation framework, which provides focus on outreach activities. Formulation of such a framework will be done through discussions and workshop sessions with the stakeholders before being forwarded to NC3 for endorsement. The outreach activities formulated are to ensure a systematic approach in educating the users about the ISM Benchmarking tool.

The functionality and the effectiveness of the tool will be improved and strengthened constantly by the custodial body, which is to be CyberSecurity Malaysia.

(3) Reaching Users

Just like the implementation of the NCSP or any other national initiatives, awareness has to be provided to users in the field. When the implementation framework is developed by stakeholders, it needs to be shared with the public and private sectors of the county.

The awareness programs should first target top management of the organizations that will eventually lead to a top down approach in the implementation of the ISM Benchmarking tool. It is common that many management teams do not put information security as a priority, especially among the Small and Medium-sized Enterprise (SME), and thus there is no proper allocation of a budget. This resulted in a lack of support and training for those who are in the information security area.

In reaching out to users, information security requirements can be encouraged by incorporating the ISM Benchmarking tool in contracts and agreement with vendors or suppliers.

It is also necessary that other countries within the region implement the ISM Benchmarking tool at the same time. This will show to users that the use of the tool is a regional initiative where inter-country platforms can be set up to exchange implementation experiences.

The objective of the ISM Benchmarking tool should be clearly transmitted to users to make them understand that it will be used for measuring the information security level of an organization. This will assist chief information officers (CIO) in determining the weaknesses of information security within their organizations to be addressed immediately. In addition, the results of the ISM Benchmarking tool can be used in considering business partnerships and in contracting as it indicates the level of information security of an organization.

The awareness of the ISM Benchmarking tool can be done through seminars, conferences, and dialog sessions. This can be specific events and sessions conducted to provide awareness of the tool or other information security events. In addition, materials such as guidelines on the use of the tool should be printed and made available

to users. Websites simulating the *how to* of the ISM Benchmarking tool and a general explanation will further accelerate the understanding of users. To provide more in-depth knowledge, workshops and focus group discussions need to be conducted.

The outcome of the ISM Benchmarking tool should be made clear to users to gain maximum appreciation. Evaluation of the information security status of an organization should be portrayed as a good thing that provides a positive impact on the organization's image and current standing within the respective sectors.

(4) Target Group

Since the proposed approach is to go through NCSP committees, the initial target group for the ISM Benchmarking tool will be the Critical National Information Infrastructure (CNII) of Malaysia. Although the tool is meant for all organizations in the country, especially the SME, using the CNIIs as a starting point will provide encouragement as there is already a mechanism in place for information security initiatives. The NCSP has the objective of ensuring that the CNII of the country is protected against cyber threats. It has ten (10) sectors as follows:

1. Defense and Security
2. Transportation
3. Banking and Finance
4. Health Services
5. Emergency Services
6. Energy
7. Information and Communication
8. Government
9. Food and Agriculture
10. Water

These sectors are regulated by members of the NCSP committee. Therefore, directives can be issued to the organizations within the respective sectors via the regulators for the use of the ISM Benchmarking tool.

The engagement for the initiative can be done using the public-private cooperation (PPC) platform provided by the NCSP Effective Governance Thrust. This is because the CNII of the country is complex and interdependent and supported by both the public and private sectors. The PPC in Malaysia are categorized into two as follows:

1. Formal PPC

   The working relationship between the public and private sectors is institutionalized with clear lines of reporting between the public sector leads and their respective private CNII under their jurisdiction. They are required to conform and comply with specific legislation, policies, laws, rules, and procedures.

2. Informal PPC

   Informal PPC is not institutionalized as there is no specific legislation required of the cooperation. There are informal PPCs in operation based on standard practices, social interaction, and community interest.

With the PPC platform, the following can be done in implementing the ISM Benchmarking tool:

a) Exchange of Information

Information exchange and interaction among both the public and private sectors can be done to ensure concerted efforts and prompt action to implement the use of the ISM Benchmarking tool.

b) Outreach and Awareness

The success of nationwide use of the tool will depend upon the effectiveness and extent of coordinated awareness and outreach programs to reach all public and private

organizations. Awareness of the importance and benefit of using the ISM Benchmarking tool and their impacts to organizations and the nation as a whole should be intensified. The awareness program must be an ongoing exercise to educate and in the long run inculcate the culture of information security into every organization.

c) Co-formulation of the Use Policies

Traditionally, it has always been the government sector that plans and develops policies. However, it must be recognized that there is much knowledge about information security successes and challenges based on experience, skills, research findings, products and services, and dealing with different target groups residing in both the public and private sectors. The synergistic values of co-formulation of the ISM Benchmarking tool use policies through open-minded deliberations and consensus building will help to ensure buy-in and successful adoption from all parties involved.

d) Sharing of Resources

The organizations require knowledgeable and skilful professionals in information security to really appreciate the ISM Benchmarking tool. These resources are scarce but they are available within some public or private sectors. The mechanism for sharing knowledge about the tool can be done through hands-on capacity building or structured training programs on goodwill or on a not-for-profit basis.

e) Research and Development

There is a need to customize the ISM Benchmarking tool for localization. The tool provides the information security status of an organization mainly the SME. However, it can be customized to provide useful information to the policyholders, which can be unique to Malaysia. One such function that can be created is the

dashboard indicating the information security status of the CNII. This was the original intention of CyberSecurity Malaysia in 2006 when the ISM Benchmarking tool was on trial by the Information-technology Promotion Agency of Japan (IPA)

The CNIIs are mainly major corporate companies, such as Telekom Malaysia Berhad (Communications service provider), Tenaga Nasional Berhad (Utility Company), hospitals, banks, and many others. Presently, cyber security initiatives of the country through the NCSP are focused on the critical services and system of the CNII. The ISM Benchmarking tool is not limited to such systems only but is applicable to the entire organization. Therefore, it can provide a health reading on information security for management of the respective organization.

As mentioned earlier, the ISM Benchmarking tool is applicable to all organizations but the introduction into the Malaysian community can start via the country's CNII. It can be expected that the use of this tool will finally reach the small and medium-sized enterprises. For example, the government sector outsources activities for development, hardware, software technical support, and training to small and medium-sized business organizations. As the CNII sees the positive outcome and impact of the tool, it is assured that the requirement will be passed to business partners such as the consultants, vendors, and suppliers of the CNII organizations. These partners are mostly the small and medium-sized business entities that represent a major part of Malaysia's industry sector.

(5) Data Accuracy

The accuracy of the data provide by the organizations is foreseen as another challenge in using the ISM Benchmarking tool. Reluctance to share sensitive

information, such as the status of information security within the organization and vulnerabilities, is both understandable and challenging. Many organizations from both the public and private sectors still consider information such as this as confidential and are concerned about the reputational damage that the ISM Benchmarking tool may cause.

As the society become more aware of information security, protecting information has assumed greater importance in organizations especially within the CNII. Therefore, it is expected that the entities, especially government and government linked organizations, will not want to participate or would modify the data to hide the true status of their information security. This can be overcome by providing anonymity. Anonymity should be guaranteed to protect the privacy of users. In line with this, policies and guidelines need to be developed to ensure the data are not abused.

The principle of sharing takes into consideration the need to protect individual sensitive and proprietary information. The sharing of information will be the pillar to the successful implementation of the ISM Benchmarking tool for the benefit of both the public and private sectors. However, given the right level of confidence, education, and appropriate confidentiality, organizations might be willing to share more information.

(6) Local Applications/Tools

The existence of local applications/tools that have similar functions to the ISM Benchmarking tool can be considered a push factor for not using the tool. The Malaysian Administrative Modernization and Management Planning Unit (MAMPU) developed a tool for information security risk assessment for the public sector. The

tool is called the Malaysian Public Sector Information Security High Level Risk Assessment Guide (HiLRA), which provides a high level indicator of the information risk an organization faces.

This application is based on the domains of the MS27001 ISMS and is very similar but more detailed compared to the ISM Benchmarking tool. In applying the ISM Benchmarking tool to the country's environment, it must be harmonized with HiLRA to avoid duplication.

(7) Funds

Funding the development and customization of the ISM Benchmarking tool will be provided by the government through the implementing agency, CyberSecurity Malaysia. The outreach and awareness program for the tool should be joint responsibilities by both the public and private sectors as they are the benefactors of the tool.

Therefore, it is imperative that budgets are allocated by all relevant organization for the awareness programs. For CyberSecurity Malaysia, since it is a government agency, the government should allocate funds for the operation and maintenance of the tool and the database servers and to conduct centralized workshops, meetings, and seminars.

(8) Enforcement and Audits

The NCSP promotes compliance and enforcement. This promotion is to ensure that any directives and guidelines by the NCSP committees are complied with by the CNII organizations. It is foreseen that the working group managing this promotion will be responsible for ensuring compliance and conducting audit on the use of the ISM Benchmarking tool by users.