Information Security Measures Benchmark (ISM-Benchmark)

Ms. Yasuko Kanno, Chief Advisor,
IT Security Center, Information-technology Promotion Agency (IPA)
Japan

Abstract

This paper presents introduction of Japan's ISM-Benchmark including its background, concept and outline, significance and future direction.

The ISM-Benchmark is a web-based self-assessment tool to visually check where the level of the user company's security measures resides by responding questions about company profile and 25 items of security measures. The ISM-Benchmark can be used in information security measure development and operation phases to improve information security.

This tool was developed and released by IPA in August 2005 and by March 2008, the number of its users had exceeded 13,000. It is contributing to raise Japanese enterprises' information security level to a great extent and has achieved high recognition.

1. Background-Why do we need the ISM-Benchmark?

Information security is said to be one of the business challenges that should be addressed by enterprises. This is because value of information held by enterprises has been increasing and enterprises are required to ensure compliance with regulations and laws pertaining to information security. Moreover, if an information security incident occurs within a company, not only does it endanger the company's existence, but may affect society as a whole. Therefore, in addressing information security issues, enterprises should establish security measures with social responsibility in mind, following the basic principles of "preventing yourself from being victimized by a security incident" and "If you encounter a security incident, strive to minimize the extent of damage."

But in reality, it seems difficult for many enterprises, particularly small- and medium-sized enterprises (SMEs), to implement appropriate information security measures. According to the "Report of Research Group on Corporate Information Security Governance," released by the Ministry of Economy, Trade and Industry(METI) in March 2005, the following three factors are impeding information security measures from being implemented: "Risks involving information security incidents are not clarified and it's difficult for enterprises to make sound investment decisions on information security", "Existing information security measures and approaches are not directly tied to corporate value" and "the need to ensure business continuity is not fully understood." To solve these problems, the following three items were developed and released.

1) ISM-Benchmark
2) Information Security Report Model
3) Guideline for the Development of Business Continuity Plan

2. What is the ISM-Benchmark?

The ISM-Benchmark is a self-assessment tool to visually check where the level of the user company's security measures resides by responding questions about company profile and 25 items of security measures. IPA developed the web-based self-assessment tool based on the

concept of METI and released the system on the IPA's web site in August 2005.

Officially it is called **Information Security Measures Benchmark** and you can understand this tool also as **Information Security Management Benchmark**, as it helps your organization to build Information Security Management System by going through the questions about security measures which include managerial, personnel, technical and physical controls.

There is a variety of self-assessment tools in this world. There are also some web-based tools that allow users to answer questions on their Websites and show the users' scores. Although the ISM-Benchmark has above mentioned characteristics, the big difference from those tools is that it enables users to compare their company's scores with ideal scores or those of other organizations using thousands of real-life assessment records of ISM-Benchmark.

In general, Benchmark is something that is used as a standard by which other things can be measured. Benchmarking is also known as a method to improve the organization's management by establishing a standard, determining the organization's level by making comparisons with the best practices and making up deficiencies detected. The ISM-Benchmark applies this method to information security measures.

To conduct diagnosis, the ISM-Benchmark requires users to answer questions on its Website. Part I consists of 25 questions regarding information security countermeasures and Part II contains 15 questions about corporate profile. When the 40 questions are answered, diagnostic outcome and recommended approaches are displayed.

For the ISM-Benchmark, user companies (or user organizations) are classified into three groups (see Table 1), based on the Information Security Risk Index (hereafter referred to as 'Risk Index'). Risk Index indicates risks to which organization is being exposed. Risk Index is calculated based on several factors, including the number of employees, sales figures, the number of critical information held and so on. Categorizing organizations into three groups supports organizations in establishing information security measures based on their level (high, medium, or low) and determining reasonable security expenses.

As a diagnosis outcome, the following items are displayed (See Figure 1):

(1) A scatter chart that shows your company's position in the group;
(2) A radar chart that shows implementation status of 25 security measures;
(3) Scores for the 25 questions.

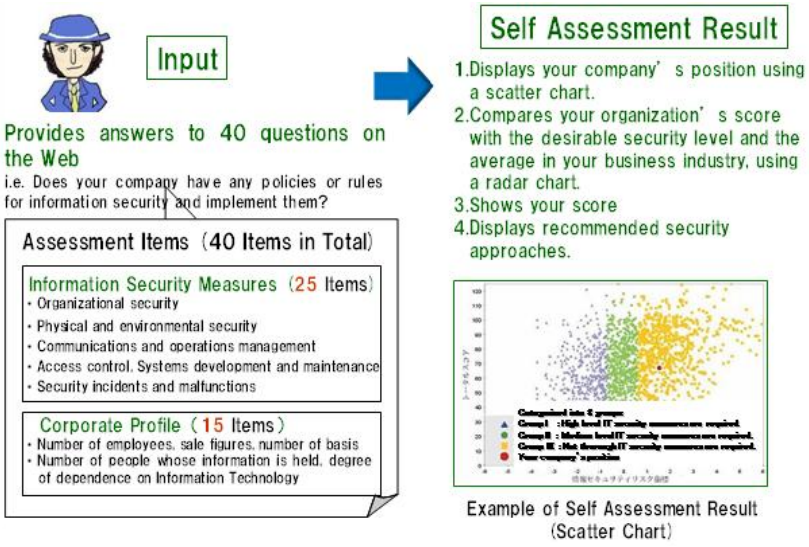


Figure 1 Input and Output of ISM-Benchmark

Table 1 Classification According to Risk Index

Type	Characteristics
Group I	High level IT security measures are required
Group II	Medium level IT security measures are required
Group III	Not thorough IT security measures are required

3. 25 questions and 146 tips

Regardless of group, all the organizations to be diagnosed need to answer 25 information-security-related questions (see Table 2) on the following one-to-five scale: (1) No policy or rule has been established (2) Only some part of it is implemented (3) Implemented but the state has not been reviewed (4) Implemented and the state reviewed on a regular basis (5) Implemented enough to be recognized as a good example for others. The highest score is 125 points with each question giving 5 points at best.

Table 2 ISM-Benchmark List of Evaluation Items

1. Information Security Policy
2. Security Organization
3. Categorization of Information Assets
4. Handling of Information Assets
5. Outsourcing Contracts
6. Employee Contracts
7. Security Training
8. Physical Security
9. The Third Party Access
10. Safe Installation
11. Documents and storage media
12. Security in operational environment
13. Security for IT system operation
14. Countermeasures against Malware
15. Measures for Vulnerability
16. Measures for Communication Networks
17. Prevent Theft or Loss of Media
18. Access Control - Data
19. Access Control - Applications
20. Network Access Control
21. Security in System Development
22. Security Management of Software
23. Measures for IT system failure
24. Incidents Handling
25. Business Continuity Management

1	The management is not aware of its necessity or **no rule and control has been established** even though they are aware of its necessity.
2	The management is aware of its necessity and they are proceeding to **formulate and disseminate the rules and controls**, but only some part of them is implemented.
3	**The rules and controls have been established with the approval of the management, and they are disseminated and implemented company-wide,** but the state of implementation has not been reviewed.
4	The rules and controls have been established under the leadership and approval of the management, and **they are disseminated and implemented company-wide with its status reviewed on a regular basis** by the responsible person.
5	In addition to those described in item 4 above, **your company has improved it to become a good example for other companies** by dynamically reflecting the changes of security environment.

Figure 2 Answers on a one-to-five scale that reflect the degree of maturity

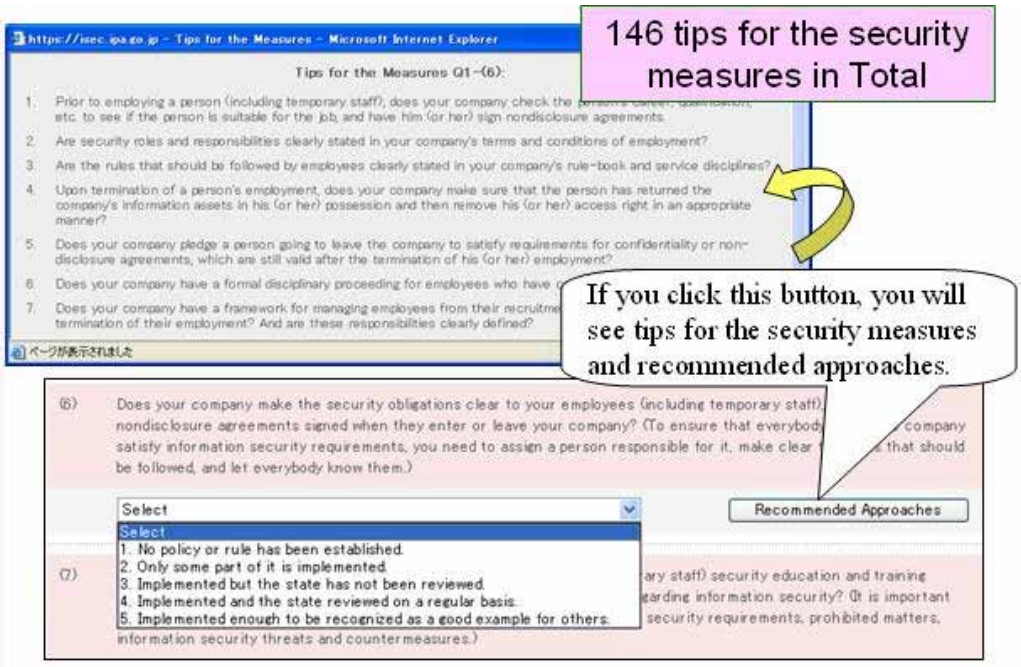


Figure 3 How to check the 146 security tips

Table 3 Controls: ISO/IEC 27001 vs. ISM-Benchmark

ISO/IEC 27001:2005 Annex A		**ISM-Benchmark** (Section Titles and Questions/Tips)		
Information Security Management Domain(Clauses title)	Number of Controls	Section Title		
1. Security Policy	2	1. Organizational Approaches to Information Security		**7**
2. Organization of Information Security	11			50
3. Asset Management	5			
4. Human Resource Security	9			
11. Compliance	10			
5. Physical and Environmental Security	13	2. Physical (Environmental) Security Countermeasures		**4**
				22
6. Communications and Operations Management	32	3. Operation and Maintenance Controls over Information Systems and Communication Networks		**6**
				33
7. Access Control	25	4. Information System Access Control and Security Countermeasures during the Development and Maintenance Phases		**5**
8. Information Systems Acquisition, Development and Maintenance	16			25
9. Information Security Incident Management	5	5. Information Security Incident Response and BCM (Business Continuity Management)		**3**
10. Business Continuity Management	5			16
11 Clauses	133	5 Sections	Number of Questions	**25**
			Number of Tips	146

25 questions in Part I were derived from 133 security measures in Annex A of ISO/IEC 27001:2005, which is the ISMS Certification Criteria. These questions cover information security measures that should be implemented by organizations, including organizational, physical, technical controls. By using the ISM-Benchmark, you can check your organization's approach

to information security more easily than using the ISMS conformity assessment. The ISM-Benchmark provides 146 tips for 25 security measures. These tips can be used to perform more detailed assessments. You can see these tips and recommended approaches while you are in the middle of self-assessment (See Figure 3).

The questionnaire consists of 5 sections, each of which has 3 to 7 questions. Table 3 is a mapping table for security measures in ISO/IEC 27001, Annex A and evaluation items in the ISM-Benchmark.

3. Assessment Result

Using assessment result, you can check your organization's score and compare it with that of other organizations. For comparison, a radar chart and a scatter chart are displayed to allow you to check where the level of your organization resides. The basis of these comparisons is diagnosis data that was collected through the self-assessments performed by other organizations using the ISM-Benchmark.

Self-assessment results contain the following items:

1. Scatter Chart – shows the distribution of all the companies and your position.
   - Presents two types of distribution: all (in three groups) or organization-size-based.
   - Allows you to compare your organization's position with other companies.
   - Allows you to compare your organization's current position with past two positions.
2. Radar Chart – allows you to compare your score with that of others from four different angles.
   - Group-based Comparison – comparing your score with that of others in the same group which is classified based on the information risk index.
   - Organization-size-based Comparison - comparing your score with that of others in the same group which is classified based on the size of the organization.
   - Industry-based Comparison - comparing your score with that of others in the same group which is classified based on the business industry.
   - Time series Comparison - comparing your organization's current position with past two positions.
3. Frequency Distribution and T-score of Your Total Score.
4. Self-Assessment Results in PDF format – allows you to save and print it as a reference material.
5. Score List.
6. Recommended Information Security Approaches.

Scatter chart shows which group your company belongs to and where the level of your company's security measures resides (See Figure 4). Scatter chart presents two types of distribution: all (in three groups) or organization-size-based. In either case, organizations are separated by three colors, based on their Risk Index.

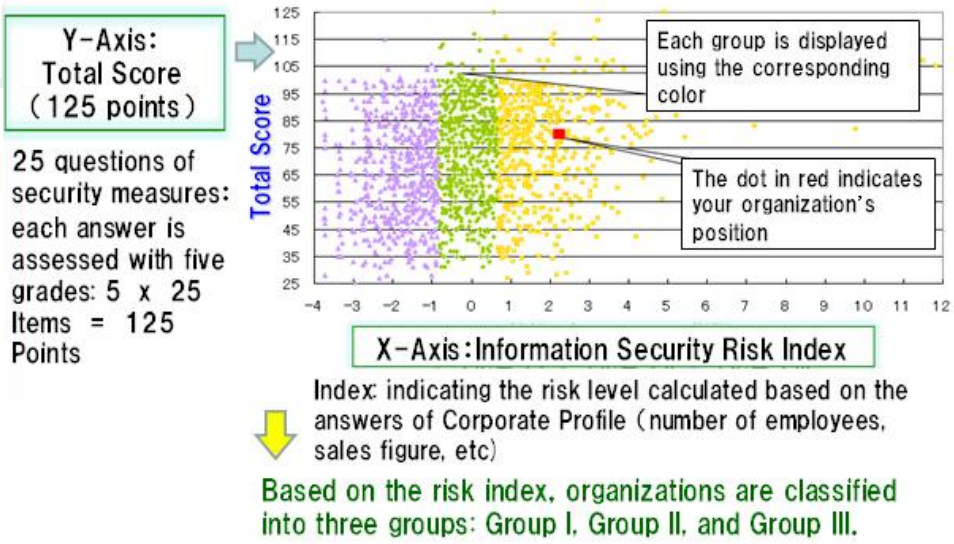


Figure 4 Assessment Result (Scatter Chart)

Rader chart provides information on implementation status of 25 security measures. It shows not only the user company's score for the 25 security measures, but average and ideal scores (See Figure 5).

The ideal score indicates average score of top 1/3 organizations in the group. Score comparisons can be made from four different angles: group-based comparison, organization-size-based comparison, industry-based comparison, time series comparison that allows you to compare your organization's current position with past two positions.

Companies that failed to reach the group's average can set the target at that level, and if they achieved the level, they can try to get to the ideal level. In this way, organizations can improve their security level step by step (See Figure 6). If the organization has not reached the ideal level, recommended approaches are displayed.

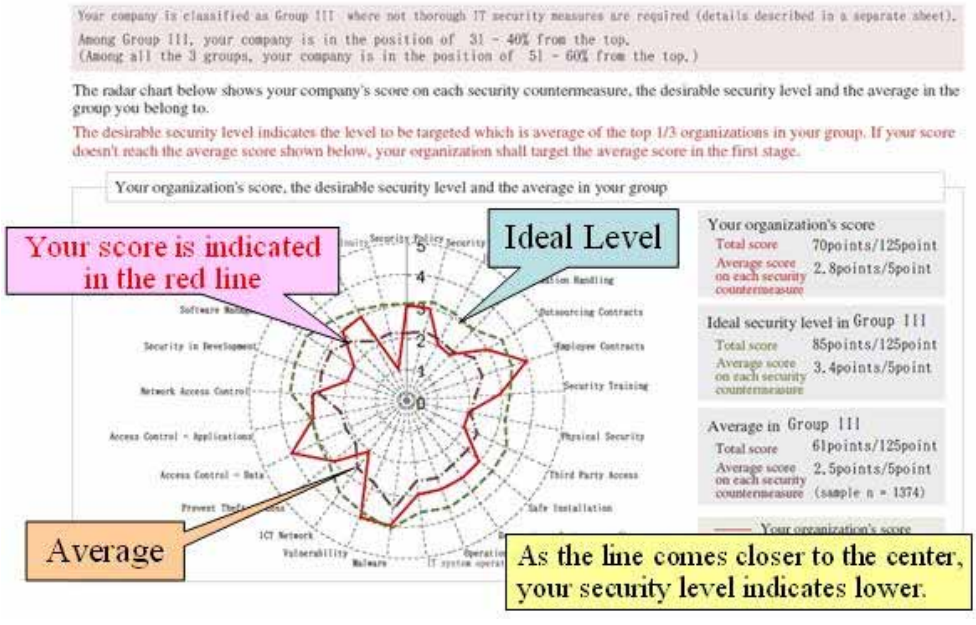


Figure 5 Assessment Result (Radar Chart)

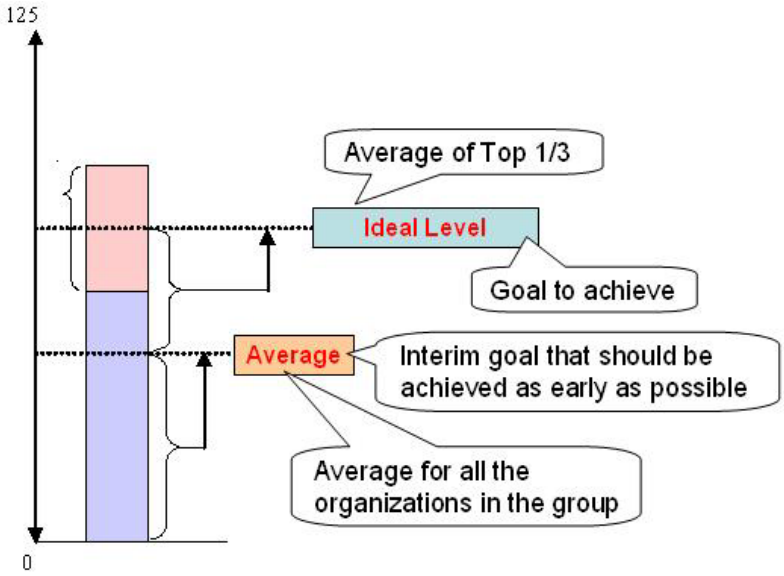
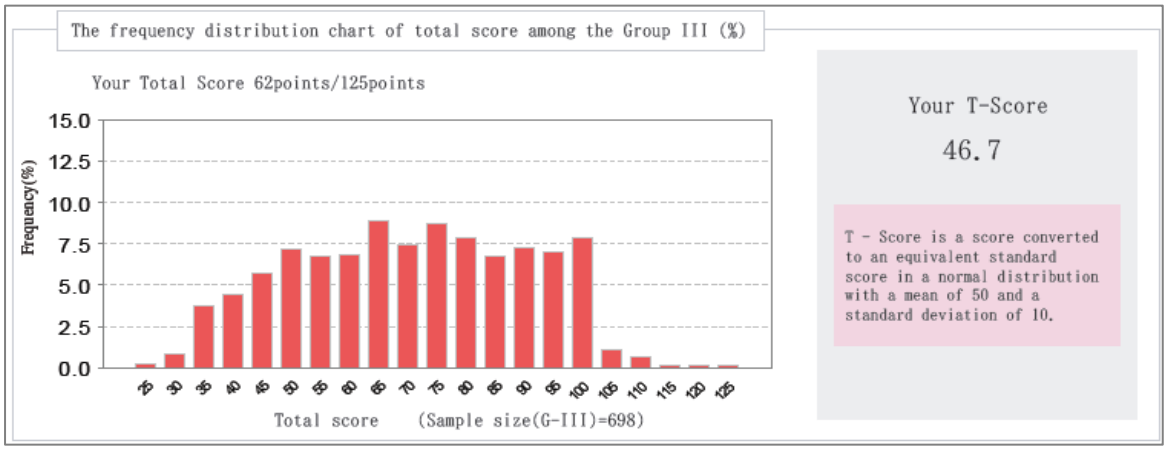
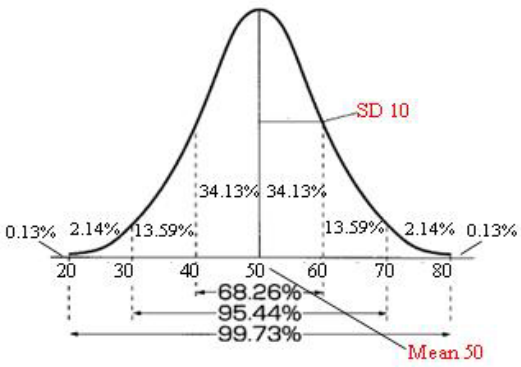


Figure 6 Ideal Level

Diagnosis outcome also includes frequency distribution and T-score of total score (See Figure 7). One of the three groups' data is presented in these charts (grouping is based on Risk Index.)





T - Score is a score converted to an equivalent standard score in a normal distribution with a mean of 50 and a standard deviation (σ) of 10.

As shown in this figure on the left, 68.26% of organizations are within the range of ±1σ (40 to 60). That is to say, if your organization's T-score is 60, it means that your organization has been ranked in around 15.87% from the top.

Figure 7 Frequency Distribution and T-score of Total Score

4. How well is the ISM-Benchmark being used?

Table 1 shows the number of records collected from Aug. 4, 2005 to Mar. 19, 2008. By March 19, 2008, the number of records had exceeded 13,000. Among those records, more than 5,000 records (including 885 for initial records) are used by this system as basic data for diagnosis until Mar. 19, 2008.

Table 4 Number of Diagnosis Performed (As of Mar. 19, 2008)

Period	Diagnostic Data Provided for the System (Total Number)	Diagnostic Data Not Provide for the System (Total Number)	Total (Total Number)
Initial Data (March 2005)	885*	—	885
Ver. 1.0 (Aug. 4, 2005 to Mar. 19, 2006)	490	2008	2498
Ver. 2.0 (Mar. 20, 2006 to Dec. 17, 2007)	4062	4689	8751
Ver. 3.0 (Dec. 18, 2007 to Mar. 19, 2008)	325	604	929
Total	5762	7301	13063

* Initial data (885) was collected from a questionnaire that was conducted at the time this system was developed.

5. New Stage of the ISM-Benchmark

1) The basic data for diagnosis and the statistic data.

The ISM-Benchmark is a comparative and quantitative assessment tool whose assessment results are presented in scores and charts, allowing you to check your organization's position in relation to that of other organizations. In the comparative assessment, the result may change depending on the data with which the user company's data is compared.

Considering rapidly changing information security environment, from ISM-Benchmark ver.3.1, it was designed to use the data of the past two years as basic data for diagnosis. The duplicated data was removed from the data collected from Mar. 20, 2006 to Dec. 17, 2007, reaching 2165 records. And the statistic information for basic data that is used for the diagnosis is made available to the public now to increase trust level and transparency to diagnosis. You can find the statistic data at the following URL:
http://www.ipa.go.jp/security/benchmark/benchmark_tokuchover31.html#toukei

2) The Handbook of the ISM-Benchmark .

The ISM-Benchmark can be used in information security measure development and operation phases to improve information security.

You can also use it to check your level before undergoing the ISMS conformity assessment or information security audit. In the past, this tool was not fully used for multipurpose as there was no use case. To overcome this situation, experts in various fields gathered to create a handbook that contains needs-based use cases as well as know-how for making use of the ISM-Benchmark during the preparation stage for the ISMS Certification or information security audit.

The handbook is called "The Handbook of the ISM-Benchmark (Japanese only)"; this can be downloaded from the following URL:
http://www.ipa.go.jp/security/benchmark/benchmark-katsuyou.html

6. Conclusion: Why ISM-Benchmark is so popular in Japan?

Because;

- It Conforms to international standards ISO/IEC 27001:2005
- Free of charge.
- Provided by the government agency.
- Organizational, technical, physical and human security measures are assessed in good balance
- Can compare your company's position with that of other companies so that it can be a tool to improve awareness at the management level
- "Gateway" to assessment/certification by third party such as ISMS conformity assessment and information security audit
- Provides ideas on how to make use of it (Handbook released:Jan, 2008)
- In addition to 25 security measures, 146 tips displayed in pop-up
- etc…

[URL]

(IPA)Information Security Measures Benchmark (English)
http://www.ipa.go.jp/security/english/benchmark_system.html
(METI) Information Security Governance web page(Japanese)
http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html
(METI) Information Security web page(English)
http://www.meti.go.jp/english/information/data/IT-policy/securityl.htm

Appendix ISM-Benchmark ver.3 List of 25 Questions

Q１．Organizational approaches to information security	
1	Does your company have any policies or rules for information security and implement them?
2	Does your company have an organizational framework which includes the management to promote information security and compliance with law and rules?
3	Are the key information assets (information and information systems) classified based on the level of importance? And are there any rules to manage and present such assets based on the level?
4	Does your company exercise appropriate security measures to protect key information (including personal data and confidential information) in each phase of the information life cycles, including acquisition, creation, utilization, saving, exchange, provision, deletion and disposal?
5	Are information security requirements included in your company's written contract, which is exchanged when you outsource your business operation or information system management?
6	Does your company make the security obligations clear to your employees (including temporary staff), for example, nondisclosure agreements signed when they enter or leave your company?
7	Does your company give your employees (including management and temporary staff) security education and training regularly to teach them your company's approaches and associated rules regarding information security?
Q2．Physical (Environmental) security countermeasures	
1	Does your company implement security countermeasures required for the buildings and sites where you want to improve security?
2	Does your company formulate and enforce any security-related rules for the people moving in and out from your company, including clients, vendors, common carriers, cleaners etc?
3	Are the important information equipment and wires/cables correctly placed and set up in safety so they can be protected against natural and man-made disasters?
4	Does your company handle important documents, mobile PCs, and removable storage media in an appropriate manner?
Q３．Operation and maintenance controls over information systems and communication networks	
1	Does your company protect information systems and data used in the actual operational environment in an appropriate manner?
2	Does your company implement security countermeasures required for information system operation?
3	Does your company take countermeasures against malware (such as computer viruses, Worms, Trojan horses, Bots, Spyware etc)?
4	Does your company take countermeasures to mitigate vulnerabilities of the information systems used in your company?
5	Does your company take appropriate protective measures (such as encryption) for data being transferred across communication networks and data stored on a public server?
6	Does your company implement appropriate security countermeasures to protect storage media such as mobile PCs, USB memories, floppy disks etc in case of their loss, theft and so on?
Q４．Information system access control, Security countermeasures for the development and maintenance phases	
1	Does your company implement necessary measures to restrict access to information (data) and information systems, including appropriate management of user IDs, adequate user identification and authentication etc?
2	Does your company implement appropriate access controls over information (data), information systems, and business applications, including granting users adequate access rights for such resources?
3	Does your company implement appropriate access controls over the network?
4	Does your company define security requirements for business application development and satisfy them in the design and implementation phases?
5	Does your company perform security controls over the selection and purchase of software products and/or the development and maintenance of systems?
Q５．Information security incident response and BCM (Business Continuity Management)	
6	Does your company take appropriate measures for the case of information system failures?
7	Does your company have written procedures for security incident responses that determine how to act in a quick-and-appropriate manner when such an incident occurs?
8	Does your company have a company-wide framework for BCM（Business Continuity Management）for the case of system down?