VI. Appendix 2. IPA Information Security Management Benchmark (ISM benchmark)

1. Overview

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.

For the ISM Benchmark, user companies (or user organizations) are classified into three groups (see Table A2-1), 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.

Table A2-1 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

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.

As a diagnosis outcome, the following items are displayed (see Figure A2-1):

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

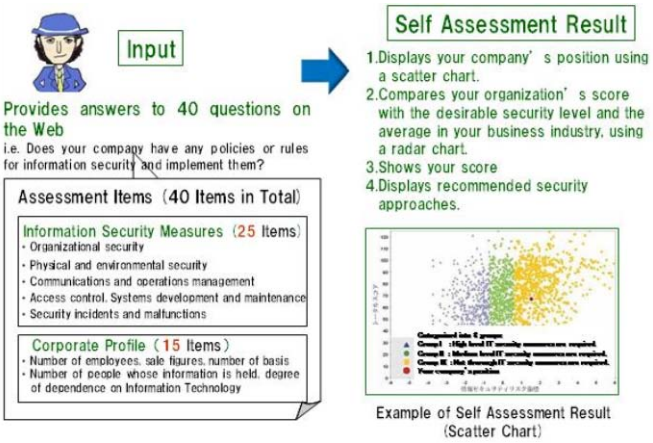

Figure A2-1 Input and Output of ISM Benchmark

2. Questions

Regardless of group, all the organizations to be diagnosed need to answer 25 information-security-related questions (see Table A2-2) 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 A2-2 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

3. Assessment Result

Using assessment result, users can check their organization's score and compare it with that of other organizations. For comparison, a radar chart and a scatter chart are displayed to allow users to check where the level of the 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:

a. Scatter Chart – shows the distribution of all the companies and the organization's position.

- Presents two types of distribution: all (in three groups) or organization-size-based.
- Compare the organization's position with other companies.
- Compare the organization's current position with past two positions.

b. Radar Chart –compare a score with that of others from four different angles.

- Group-based Comparison − compare a score with that of others in the same group which is classified based on the information risk index.
- Organization-size-based Comparison - compare a score with that of others in the same group which is classified based on the size of the organization.
- Industry-based Comparison - compare a score with that of others in the same group, which is classified based on the business industry.
- Time series Comparison - compare organization's current position with past two positions.

c. Frequency Distribution and T-score of Total Score.

d. Self-Assessment Results in PDF format

e. Score List.

f. Recommended Information Security Approaches.

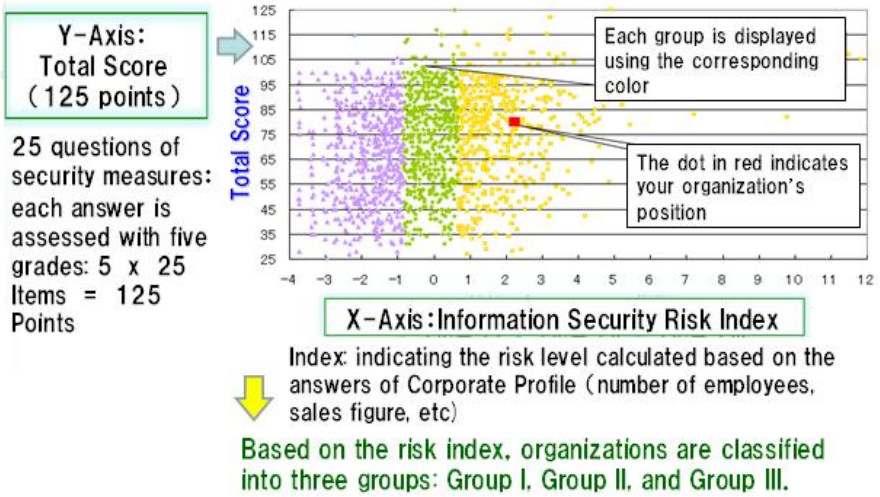

Figure A2-2 Assessment Result (Scatter Chart)

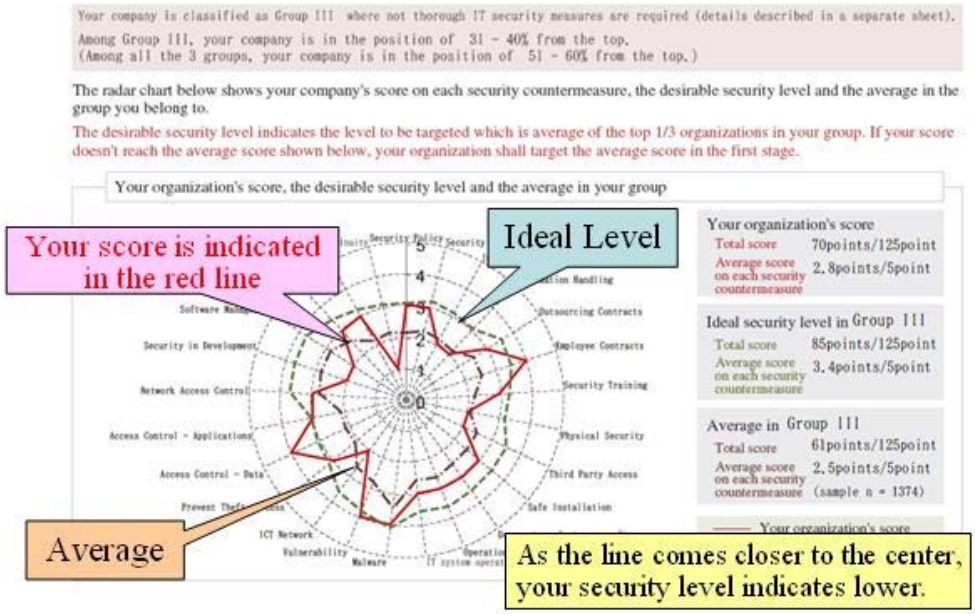

Figure A2-3 Assessment Result (Radar Chart)

4. Usage

Table A2-3 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 A2-3 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.