



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

The criteria of development site security for CC evaluations

**IT Security Center
Information-technology Promotion Agency
(IPA)**

Japan

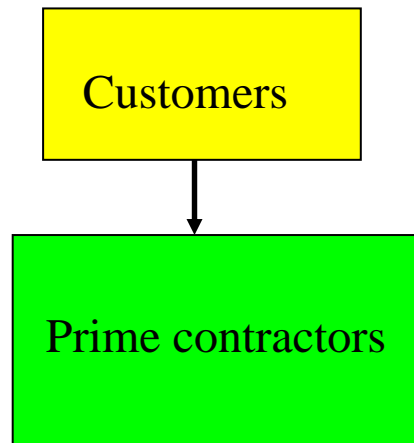
Sep 27, 2011

Structure in the Japanese IT service industry

Software development structure in Japan

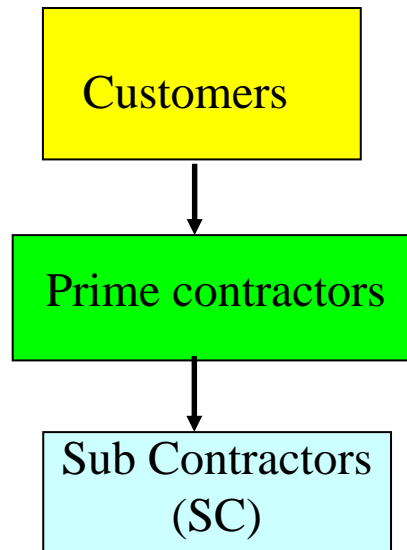


1960s – 70s
(Dawn of mainframe)



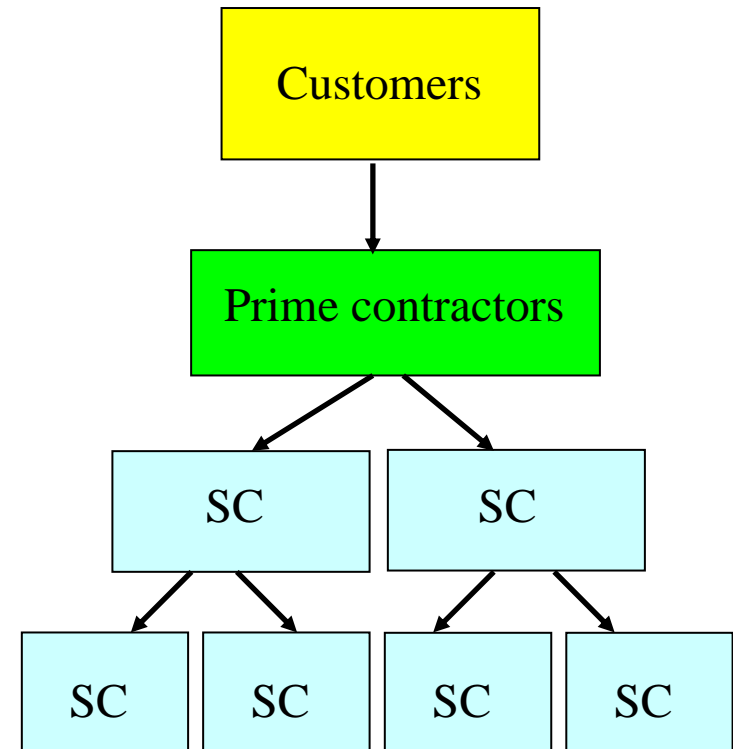
One company developed a whole information system/software

1980s
(Mainframe centric)



Part of development tasks were outsourced to the SCs

1990s and later
(Open and network centric)

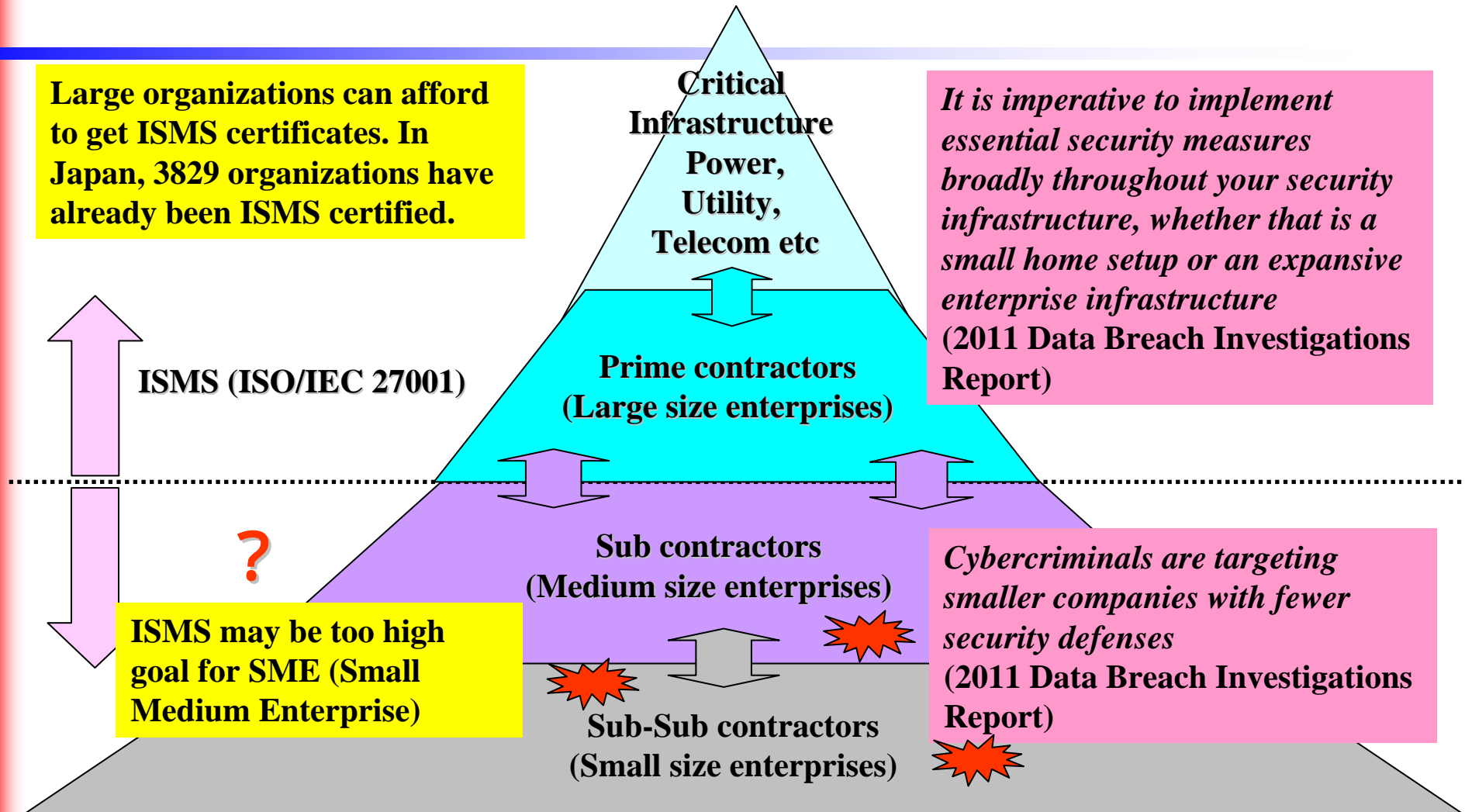


As the number of IT vendors increased, Prime contractors started to outsource labor intensive tasks to reduce development cost, which introduced multi-layered subcontracting structure in Japan

Issues in the subcontracting structure

- Development costs can be reduced through the multi-layered subcontracting structure because prime contractors can select sub contractors at lowest cost.
- However this structure causes various issues:
 - ✓ Low quality because of lack of communication among contractors
 - ✓ Unclear boundary of responsibility among contractors
 - ✓ Difficulty of project management
- Prime contractors are trying to reduce the number of layers. They are starting to prohibit their contractors from entering into subcontracts again.
- It may takes time to change the structure because of strong cost pressure from customers.

Issues in the subcontracting structure



SME can not pay enough attention to their information security. We need more simpler and easier tool to help them to improve their security.

ISM (Information Security Management)-Benchmark

ISM-Benchmark – Solution for SME

IPA developed a web-based self-assessment tool (ISM-Benchmark) to help SME to improve their IS security. More than 11,000 organizations are using the ISM-Benchmark

Click here to start your assessment

Merit of ISM-Benchmark

- Free service offered by the Japanese government
- Easy to use. Requires no special knowledge.
- Provides visual references of your security and subsequent progress
- Compares your security levels with others by size, industry and risk index
- Based on ISO/IEC 27001 (ISMS)

IPA ISM-Benchmark Portal Site
http://www.ipa.go.jp/security/english/benchmark_system.html

1. Respond to the 40 Questions



Respond to all the questions provided on this web site. There are 25 questions in the first part and 15 questions in the second.

Part 1 : About Information Security Countermeasures (5 Sections/25 Questions)

Q1 : The questions Q1-(1) to Q1-(7) are asking about the organizational approaches to information security. Answer the questions by selecting one of the options 1 to 5 provided below which you think is the most appropriate for your company.

Options for Q1-(1) to Q1-(7)

- 1. The management is not aware of its necessity.
- 2. The management is aware of its necessity, but only some parts of it are 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.

Benchmark shows you 25 questions. Each question asks you about your current status of your information security.

(1) Does your company have any policies or rules for information security and establish policies/rules based on your company's business and operational status (e.g., of a sample or template. To ensure the enforcement of those policies and rules, you should inform everyone within the company, check the state of implementation, and review them on an annual basis.)

Click here to see Tips and recommended approaches.

Select

- Select
- 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.

Select one level from 1 to 5 for all questions

25 questions and 146 tips for the measures

https://isec.ipa.go.jp - Tips for the Measures - Microsoft Internet Explorer

Tips for the Measures Q1-(6):

1. Prior to employing a person (including temporary staff), does your company check the person's background, etc. to see if the person is suitable for the job, and have him (or her) sign nondisclosure agreements?
2. Are security roles and responsibilities clearly stated in your company's terms and conditions of employment?
3. Are the rules that should be followed by employees clearly stated in your company's rules and regulations?
4. Upon termination of a person's employment, does your company make sure that the person has returned the company's information assets in his (or her) possession and then remove his (or her) access right in an appropriate manner?
5. Does your company pledge a person going to leave the company to satisfy requirements for confidentiality or non-disclosure agreements, which are still valid after the termination of his (or her) employment?
6. Does your company have a formal disciplinary proceeding for employees who have committed a security breach?
7. Does your company have a framework for managing employees from their recruitment to their retirement?

These tips (suggestions) can be used to determine your levels:

Implement all tips = level 5
 Implement 80% tips = level 4

These tips are suggestions that tell you common practices Japanese organizations are usually doing

If you click this button, you will see tips for the security measures and recommended approaches.

satisfy information security requirements, you need to assign a person responsible for it, make clear the rules that should be followed, and let everybody know them.)

- Select
- Select
 - 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.

Recommended Approaches

(7)

information security threats and countermeasures.)

ary staff) security education and training regarding information security? (It is important to clarify security requirements, prohibited matters, and

Assessment Result : Radar Chart



After answering all questions, your security levels are shown as chart

Your company is classified as Group III where not thorough IT security measures are required (details described in a separate sheet).
 Among Group III, your company is in the position of 31 - 40% from the top.
 (Among all the 3 groups, your company is in the position of 51 - 60% from the top.)

The radar chart below shows your company's score on each security countermeasure, the desirable security level and the average in the group you belong to.

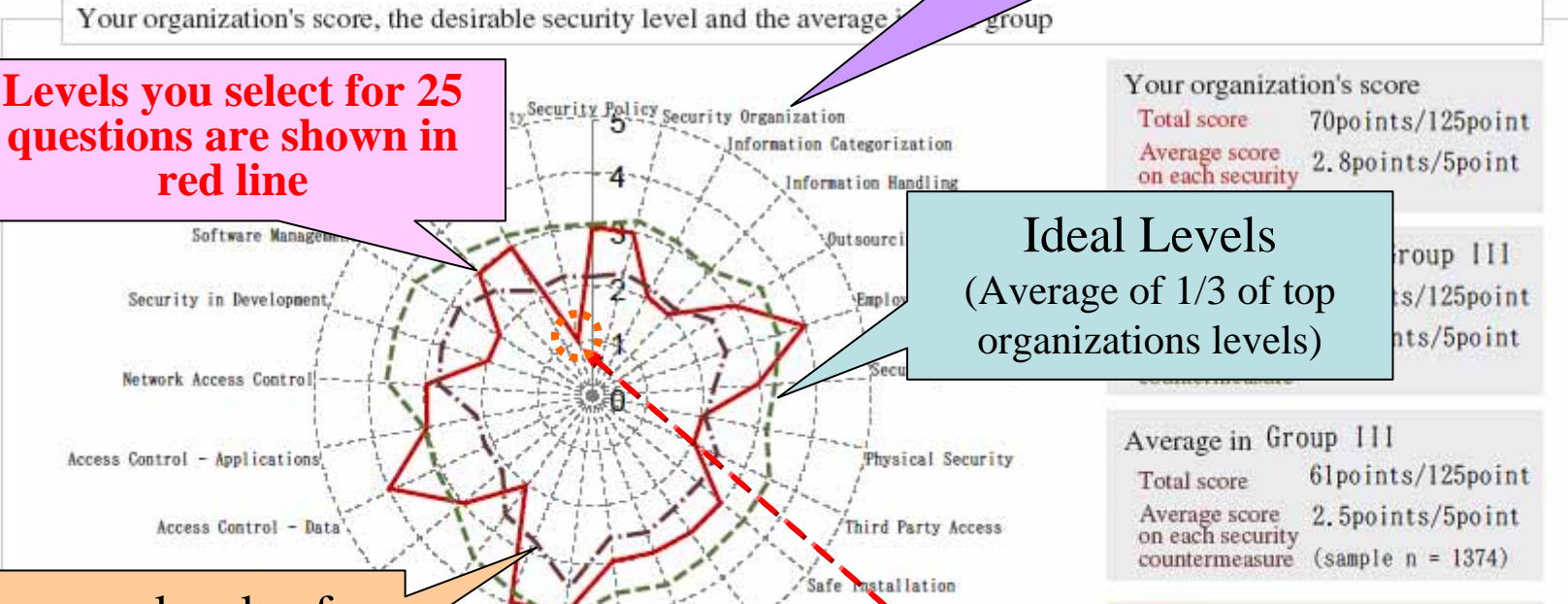
The desirable security level indicates the level to be targeted which is average of 1/3 of top organizations levels. If your score doesn't reach the average score shown below, your organization shall target the average score in the next stage.

Your organization's score, the desirable security level and the average in the group

Levels you select for 25 questions are shown in red line

25 axes for 25 questions

Ideal Levels (Average of 1/3 of top organizations levels)



Average levels of ISM-benchmark users

Radar chart show your weakness (your levels below average)

ISM-Benchmark vs. ISO/IEC 27001



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

7 <= Question

50 <= Tips

133 security controls in ISO/IEC 27001:2005, Annex A (ISO/IEC 27002:2005) are summarized to 25 questions in ISM-Benchmark

ISM-Benchmark question and tips



Control for malicious code

More concrete

Question

Q3-(3) Does your company take countermeasures against malware (such as computer viruses, Worms, Trojan horses, Bots, Spyware etc.) (Countermeasures against malware include installing antivirus software, updating pattern files on a regular basis, applying security patches, etc)

More specific

Tips for the Measures Q3-(3):

- 1) Does your company use appropriate antivirus software?
- 2) Does your company properly update pattern files?
- 3) Does your company scan servers and client PCs for viruses on a regular basis?
- 4) Do users of information system have a clear understanding of what they should do to protect the system against viruses and how to cope with security problems?
- 5) Does your company perform a virus scan on mobile PCs used off-site and clean the viruses detected before connecting them to the company's network?
- 6) Does your company apply security patches to prevent the company's system from being attacked by malicious programs?

According to the survey (Information Security – Report 2008, NRI Secure Technologies), many companies didn't know what and how much they should to improve their security.

Security controls to 25 questions



How are 133 security controls in ISO/IEC 27001 Annex A summarized to 25 questions in the benchmark?

- Examine how Japanese ISMS certified organizations implement controls
- Only choose security controls that we can define common best practices
- Exclude security controls that we can not define common best practices
e.g. “A.10.9.1 Electronic commerce” is excluded because all organization do not conduct electronic commerce
- 146 Best practices (Tips for measure) are defined in our ISM-Benchmark.

Questions and Tips are:

- Developed by ISMS experts and academics
- Conforming to ISO/IEC 27001 Annex A
- Keeping it simple as much as possible
- Avoiding technical jargons

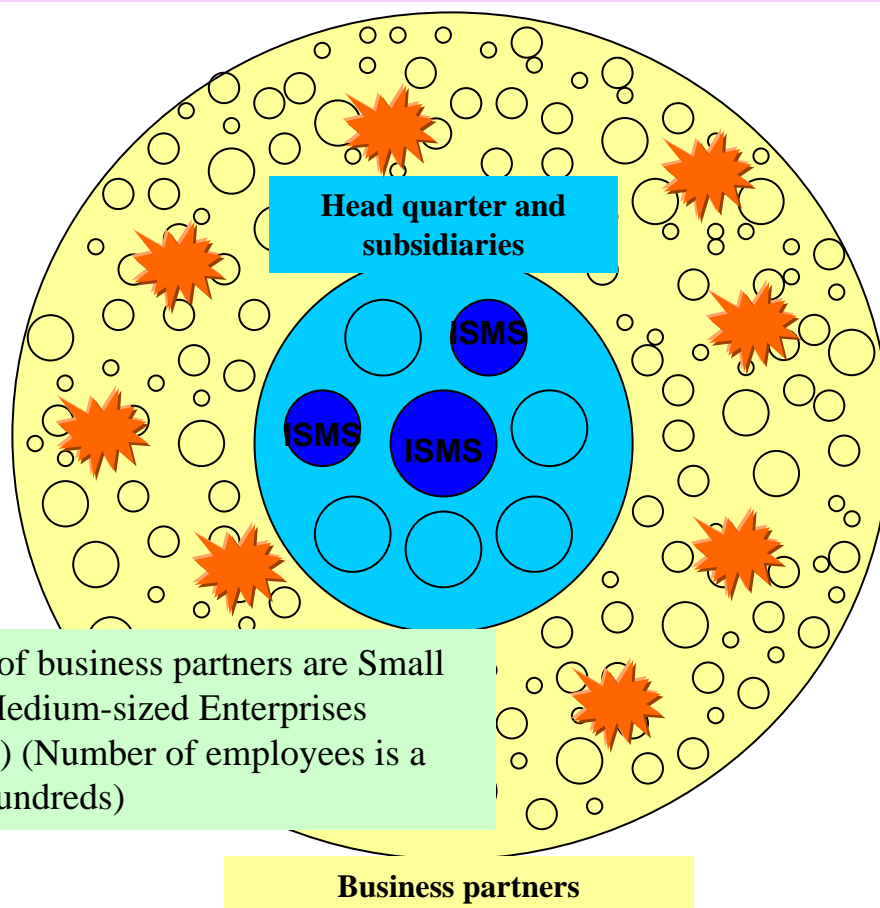
Tips are due diligence for organizations which hold customers' personal information

Case Studies in Japan

How is the ISM benchmark used?

Company Z profile

Company Z (Japanese major manufacturer) has established and applied their own ISMS-based information security standard only to their head quarter and its subsidiaries (A few of them are ISMS certified). However hundreds of domestic and foreign business partners were out of scope.



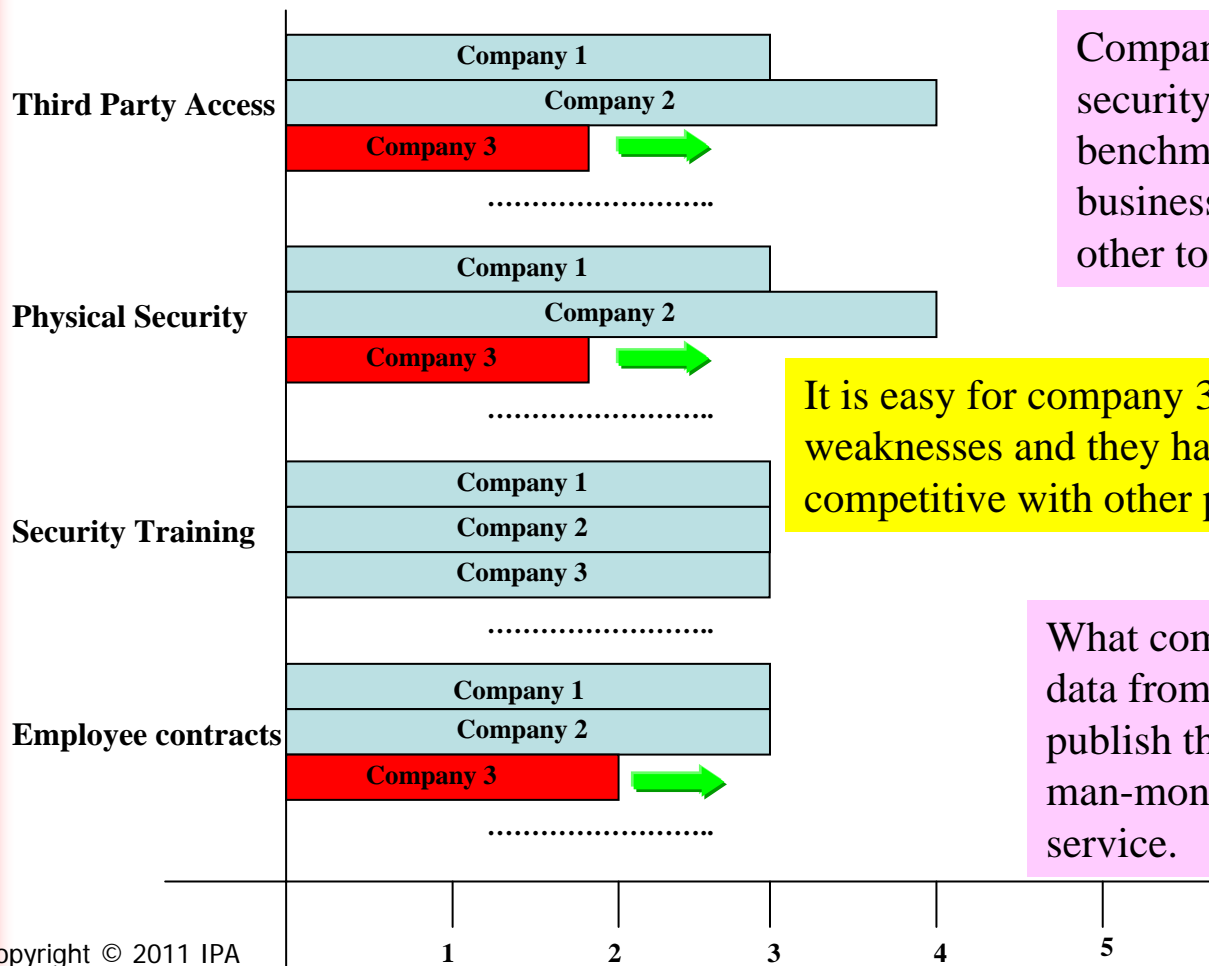
Most business partners are SME. SME usually can not pay enough attention to their information security. However according to “2011 Data Breach Investigations Report“, cybercriminals are targeting smaller companies with fewer security defenses. Company Z actually suffered data breaches caused by the SME partners.

Most of business partners are Small and Medium-sized Enterprises (SME) (Number of employees is a few hundreds)

However company Z realized that applying their ISMS-based security standard to their SME partners was impossible considering current level of their security.

Compare to compete – First Step

Company Z uses ISM-Benchmark to compare business partners' security levels and publish the result



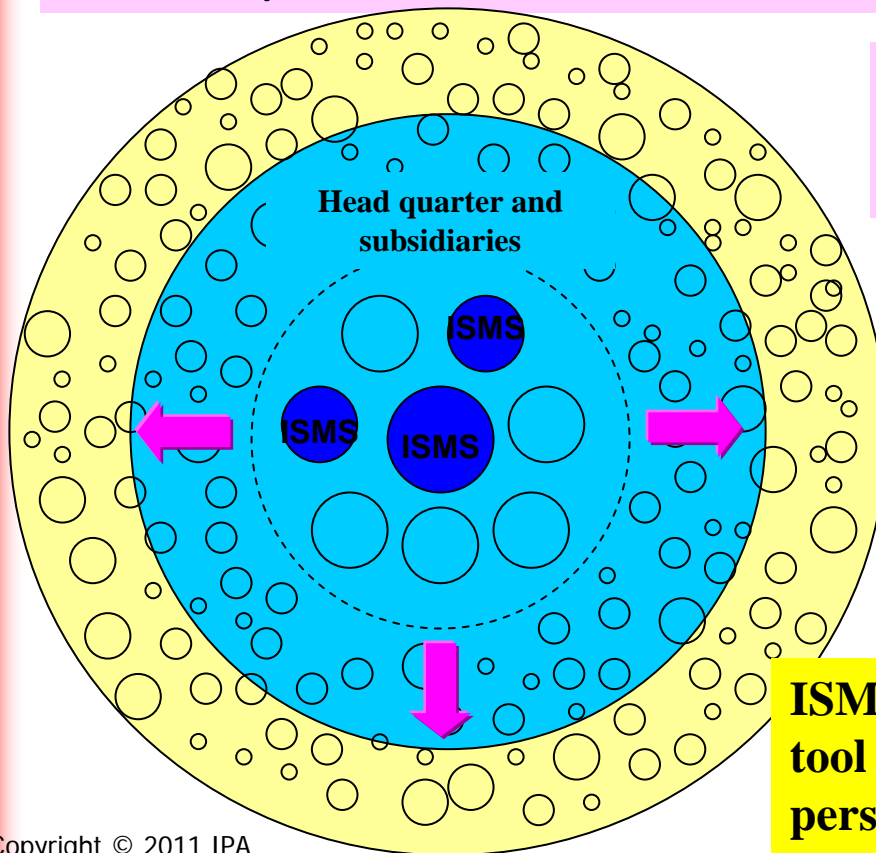
Company Z gather their partners security levels annually using ISM-benchmark. What they see is that business partners are competing each other to level up their security.

It is easy for company 3 to understand their weaknesses and they have to improve them to be competitive with other partners

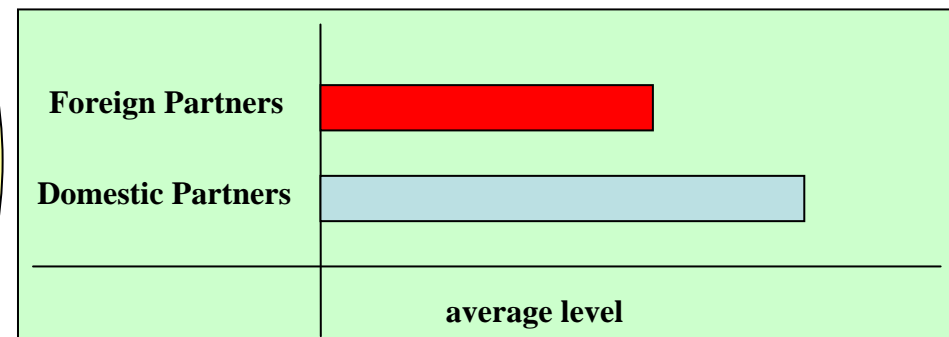
What company Z does is just gathering the data from partners and analyze and publish the result. It usually takes only 1 man-month using free ISM-benchmark service.

Raise the goal – Second Step

Company Z gradually widened the area to apply their own ISMS-based security standards after using ISM-benchmark for 4 years. It is enough time for partners to prepare and follow the same standard as the head quarter does. Company Z said this phased approach worked fine and it was a safer way to avoid too much burden to their partners and at the same time improve the levels of their security in a cost-effective manner.



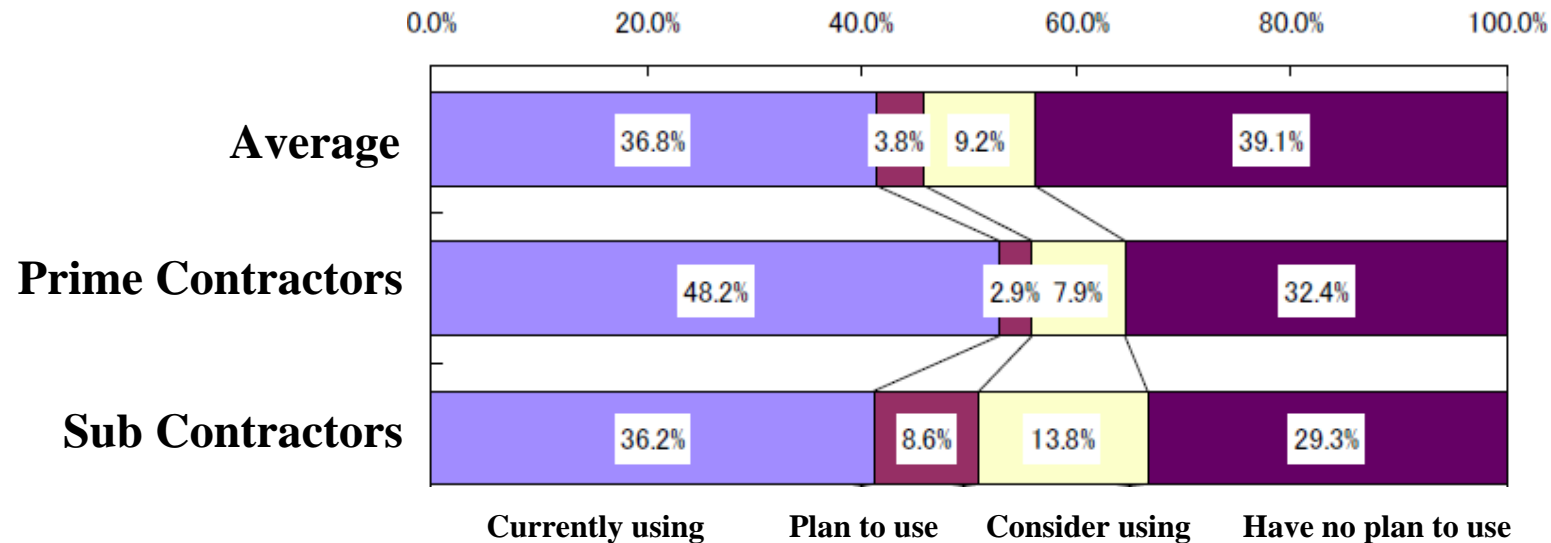
According to company Z, they analyzed data gathered from partners and saw tangible difference between domestic partners and foreign partners' security levels.



ISM-benchmark can be also used as an analysis tool to find own weaknesses from various perspectives to make the right security investment.

Offshore outsourcing and ISM-Benchmark

Offshore outsourcing trend in Japan

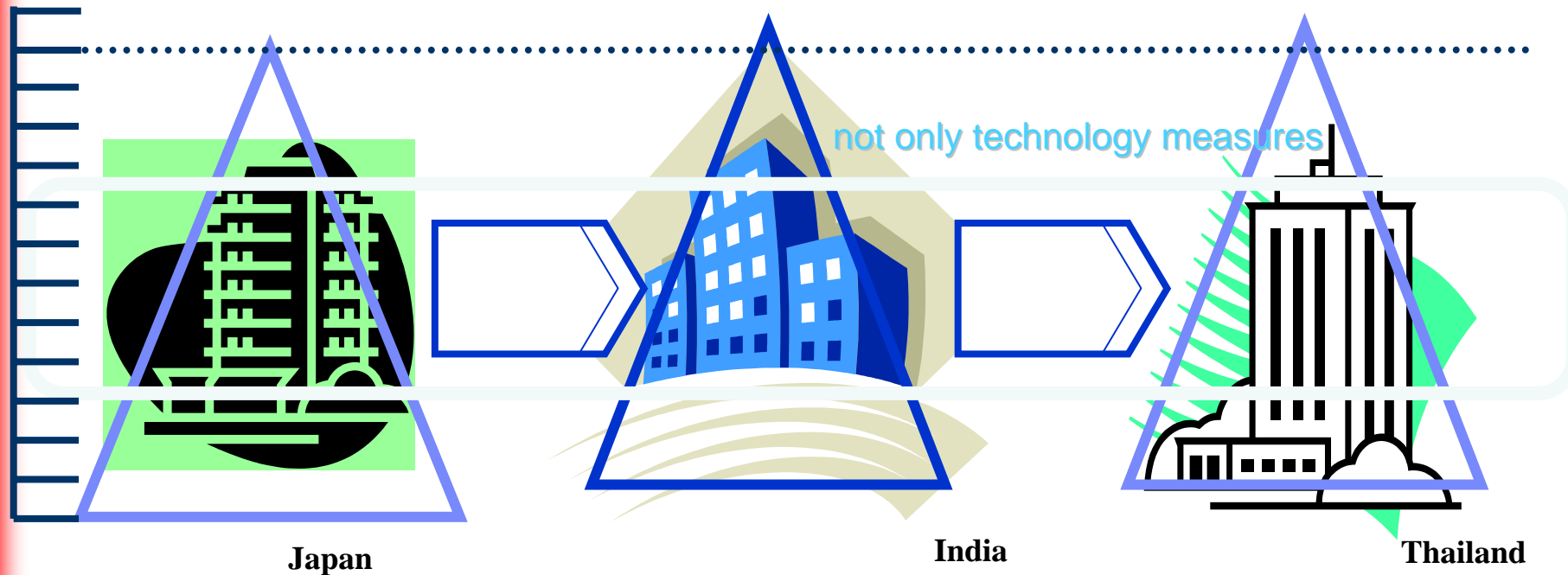


Source : Research on the progress of offshoring and its effect
http://www.soumu.go.jp/johotsusintokei/linkdata/other017_200707_hokoku.pdf

According to the survey, number of prime and sub contractors that are currently using or will use offshoring are increasing. Most of Japanese IT vendors are suffering shortage of engineers and looking for skilled workforce at lower cost in the foreign countries.

Concern for offshore outsourcing

We may have to share key information to work together, however many companies concern about how their partners protect such information



To erase all security concerns, we need to develop a common security scale collectively and share it to learn to trust each other.

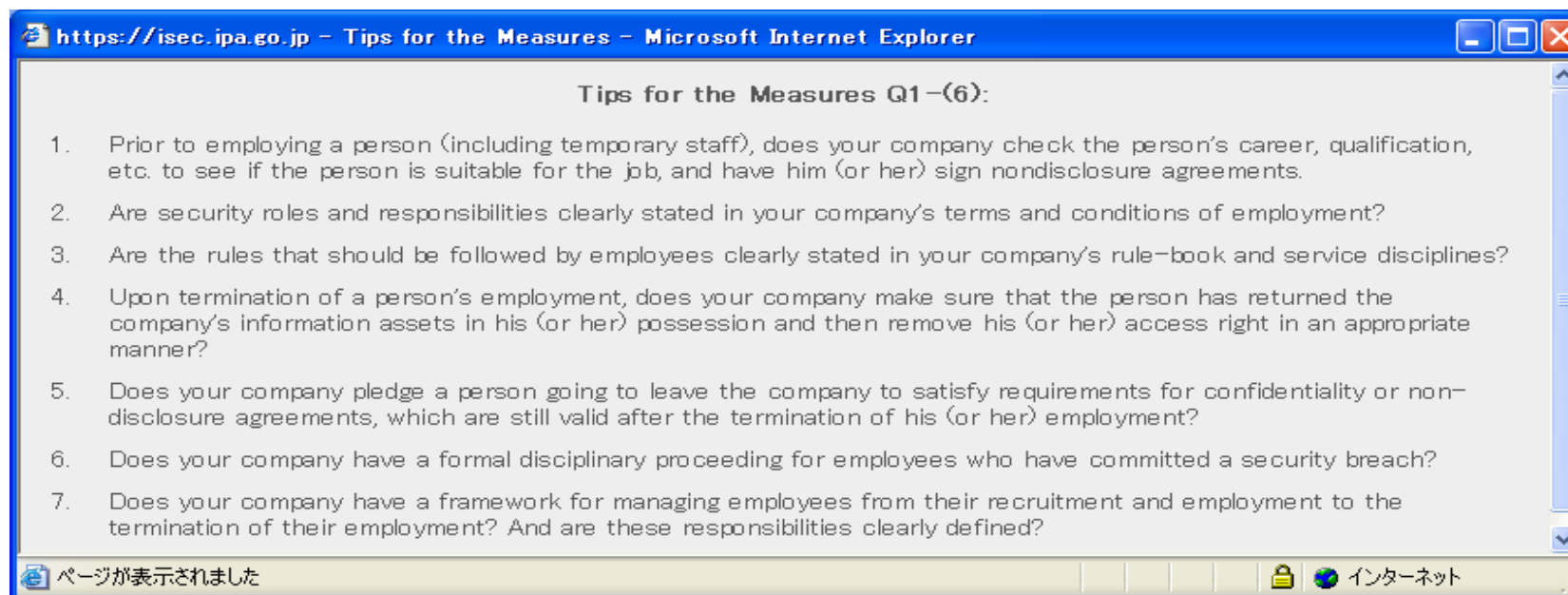
Promoting ISM-Benchmark in the Asia



- IPA has just started to dialog with Asian nations to promote ISM-Benchmark. All nations shows interest in our benchmark however they also raise issues, need for third party validation.
- In Japan, organizations take time to conduct correct assessment. For example, some companies ask 3 or 4 person to score levels and take a mean value to get precise data.
- However Asian countries concern that their organizations may not input correct data worrying about damage to their reputation.
- IPA are trying to find a solution to this issue.
- The CC evaluation could be good reference for the third party validation.

The third party validation

Benchmark questions and tips



CC part3

Requirements for organizations assessed

How to evaluate organizations meet the requirements

CEM

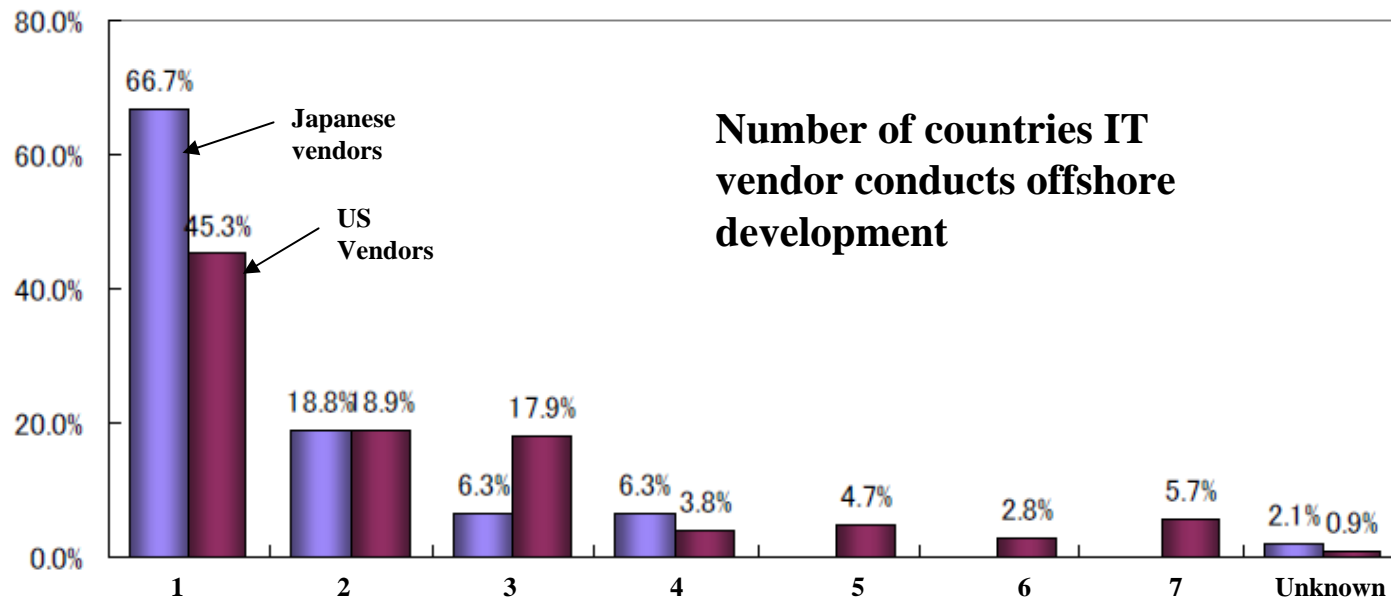
Specific requirements and methods for its evaluation should be defined to conduct repeatable and objective third parity validations

ALC evaluation and site visit



- Development sites are evaluated during ALC evaluation. Sites are also physically checked (Site visit).
- Issue in development site evaluations is lack of clear criteria.
- We can not expect the same level of protection to all companies. Appropriate level of protection should be determined through the risk analysis and attack potential.
- However identifying and measuring risk and determining proper level of protection may be subjective decision.
- Another approach is defining common practices (i.e. what everyone else is actually doing) and evaluating the sites based on these common practices. Evaluators need to look at more closer if the companies do not implement the common practices.

ALC evaluation and site visit



Source : Research on the progress of offshoring and its effect

http://www.soumu.go.jp/johotsusintokei/linkdata/other017_200707_hokoku.pdf

- Site evaluations have to be more cost effective as development sites are more diffused geographically
- Each country may have different unique security concerns based on the culture, law or regulations (i.e. practices can be different among different countries)

ALC evaluation and site visit



- IPA hope to define the common practices for information security in Asia through ISM-benchmark promotion activity.
- These common practices (i.e. baseline requirements for site security) could be used to conduct more objective and cost effective CC evaluations.

Thank you



Naruki Kai (n-kai@ipa.go.jp)

**Information-technology
Promotion Agency, Japan**

<http://www.ipa.go.jp/index-e.html>

**2-28-8 Honkomagome
Bunkyo, Tokyo 113-6591, Japan**

Tel: +81-3-5878-7538

Fax: +81-3-5978-7548

