



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

The Information Security Management Benchmark (abbr: ISM-Benchmark)

How to use the ISM-Benchmark

Information-technology Promotion Agency, Japan (IPA)

<http://www.ipa.go.jp/security/>

1. How to use ISM-Benchmark - at the first time

How to start your self-assessment



IPA ISM-Benchmark Portal Site

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

IT Security

JAPANESE

- Security Alerts
- Measures Against Computer Viruses & Unauthorized Computer Accesses
 - Monthly Reports
 - Quarterly Reports
 - Publications
- Security Certifications
 - JISEC
 - JCMVP
- Measures for Information Security Vulnerabilities
 - Quarterly Reports
 - JVN
- Cryptographic Technology Research & Evaluation Activities

Information Security Measures Benchmark - The Self-Assessment Tool for Security Measures -

Information-technology Promotion Agency
IT Security Center

Please answer 40 questions in this web site. The result will show you your company's security status. You can use the results to review and improve your company's security level.

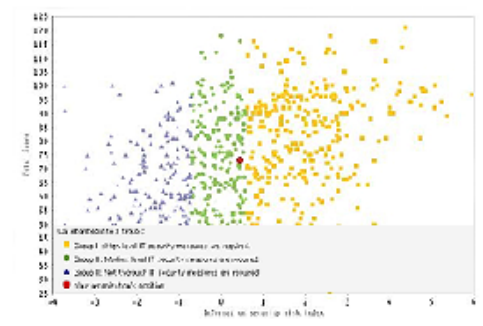
Click here for your Self-Assessment:

[Japanese Benchmark Portal Site is here](#)

[Outline of Information Security Measures Benchmark](#) (196KB PDF File)
Current version is 3.1

[You can download 25 questions regarding security measures from here](#) (412KB PDF File)

[Sample of the Self-Assessment Results]



Based on your answer to 25 questions asking the information security countermeasures, your score is calculated. Based on your answer to 15 questions regarding your company profile, you will be classified into one of the 3 groups, Low, Medium or High. The distribution chart shows the distribution of all the companies and your position.

Click here to the assessment page

How to start your self-assessment



Click here to start your self-assessment

What is Information Security Measures Benchmark?

Information Security Measures Benchmark is a self-assessment tool to visually check where the level of your company's security measures resides by responding to questions relevant to security measures (25 questions) and to company profile (15 questions).

Issue of your log-in account

You can apply to issue your log in account after you answered all the questions in your self-assessment. The registration of the log-in account is optional. If you register your login account, you can enter your own page named "MY Page" where you can use variety of functions such as conduct a new diagnosis using your answers stored in the system, or correct answers and so on.

- If you apply to register your log-in account, the account number will be displayed in the diagnosis result page.

Please keep and remember your account and password as it is necessary to enter it when you log-in to your "MY Page".

The screenshot shows a web interface for a self-assessment tool. At the top, there is a dark header with the text "Self-Assessment Test". Below the header is a prominent red button with a white right-pointing triangle and the text "Click here to begin your Self-Assessment". Underneath the button, there is a grey box containing the text: "If you have your log-in account, please enter your ID and password to log in." Below this text are two input fields: the first is labeled "ID:" and the second is labeled "Password:". At the bottom of the grey box is a "Login" button.

The Flow of your self-assessment



1. Respond to the 40 Questions:

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

Your responses will be calculated to show the results of your assessment. To increase the granularity of this tool, please input precise information, accordingly.

Your responses stored in our system will be strictly and adequately managed.

Responses will only be used in this tool to calculate the result and for statistic purpose.

2. Confirm the Input :

Be sure to confirm your input before submitting the responses.

3. Display the Result of your Self-Assessment:

The result of your self-assessment as well as the recommended approaches will be displayed based on your responses.

The desirable security level and average is calculated based on the data stored in Japanese benchmark system in the first stage. In future, if the sufficient amount of the assessment data of the particular nation will be stored in the English benchmark system, it might be possible to calculate and show the result based on the data of the particular nation.

1. Respond to the 40 Questions

Respond to the 40 Questions

Confirm the Input before Submitting

The Result of your Self-Assessment



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 the rules and controls, but only some parts of the rules and controls. |
| 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. |

Part I : 25 Questions

Answer the question by selecting one of the options 1 to 5.

Click here to see Tips and recommended approaches.

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

- 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.

(2) management to promote information security, it is important for responsibilities assigned to each person in charge, including auditors. To ensure the enforcement of those policies and rules, everybody within the company needs to understand them fully and clearly.)

25 questions about security measures **IPA**[®]

Consists of 5 sections, each of which has 3 to 7 questions, 25 questions in total.

- (a) **Organizational Approaches** to Information Security (7 questions)
- (b) **Physical (Environmental) Security Countermeasures** (4 questions)
- (c) **Operation and Maintenance Controls** over Information Systems and Communication Networks (6 questions)
- (d) Information System **Access Control** and Security Countermeasures during the **Development** and Maintenance Phases (5 questions)
- (e) Information Security **Incident Response and BCM** (Business Continuity Management) (3 questions)

The 25 questions of ISM-Benchmark based on 133 security controls in **ISO/IEC 27001:2005, Annex A (ISO/IEC 27002:2005).**

Characteristics of this questions are:

- Developed by a working group of security specialists
- Uses simple and easy-to-understand expressions
- Number of questions(= evaluation items) is limited to 25 so that it is not difficult for SMEs to conduct self-assessment



You can download 25 questions from:

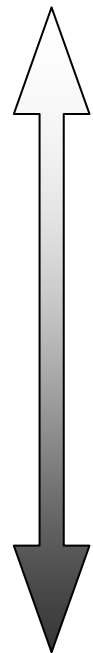
http://www.ipa.go.jp/security/english/documents/InfoSec_Benchmark_V3_25questions.pdf

How to Answer 25 questions



For each answer, the user selects the most appropriate level from the five levels below

Not implemented



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	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.

Implemented

25 questions and 146 tips for the measures



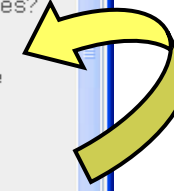
146 tips for the security measures in Total

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 career, qualification, 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 rule-book and service disciplines?
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...
7. Does your company have a framework for managing employees from their recruitment to the termination of their employment? And are these responsibilities clearly defined?

ページが表示されました



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

(6) Does your company make the security obligations clear to your employees (including temporary staff), nondisclosure agreements signed when they enter or leave your company? (To ensure that everybody in your company 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.

(7) ...ary staff) security education and training regarding information security? (It is important security requirements, prohibited matters, information security threats and countermeasures.)

Recommended Approaches

Part 2 : About Your Company Profile (16 Questions)

Q1 : How many employees (including temporary staff and part-time worker) does your company have and what is the percentage of permanent employees?
(Even for departmental assessments, please enter the numbers of your whole organization)

Total number of employees: Approximately, (*Use one-byte numerical characters only, for example, 1000)

Percentage of permanent employees:

Q2 : What are your company's sales figures, sales category, sales region, sales headquarter and branch office?
(Even for departmental assessments, please enter the numbers of your whole organization)
(If you are governmental organization, please enter the numbers of your whole organization)

Sales figures:
example: 1000000000

Capital fund: ,000 USD. (*Use one-byte numerical characters only, put dollars in thousand, for example, if you input 1000, it means 1000,000 USD)

Total number of domestic offices (including headquarters and branch offices): (*Use one-byte numerical characters only, for example, 10)

The number of overseas offices (including headquarters and branch offices): (*Use one-byte numerical characters only, for example, 1)

Your country:

Part II: 15 Questions about your company profile, including number of employees, category of industry and number of personal information held etc.

Enter your Organization name/The scope of your self-assessment



The organization/company name and the scope of your self-assessment you entered would be included in the diagnostic outcome (can be output in the html or pdf format.) They are optional, but if you did not specify anything for these columns, you would see blanks in the corresponding fields in the outcome.
If you apply to issue your log-in account, to enter the organization/company name is a must.

Organization/Company Name:

(*Use one-byte alphabetical characters only)

The scope of your self-assessment:

(*Use one-byte alphabetical characters only)

The scope of your self assessment means the whole organization, please enter your organization name.
If you assess one specific division, please enter the division name.

Issue of your log-in account

Do you want to issue your log-in account?

Yes No

If you apply to issue your log-in account, your log-in ID will be issued.

Please enter your password:

Please enter your password for confirmation purpose:

*Number of characters
More than 8 characters

*Only following characters are allowed

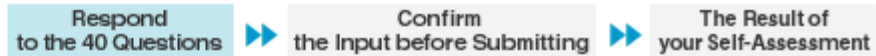
One-byte numerical and alphabetical characters, for example, a~x A~Z 0~9
One-byte code, for example ! # % & () = ~ ^ | + - * / , . : ; < > ? [] _ { } \$

The organization/company name and the scope of your self-assessment you entered would be included in the diagnostic outcome.

Once you have applied for issuance of login account and received it, you can use it from the next time you use the ISM-Benchmark.
(To apply for issuance of login account, you need to enter your organization/company name)

Click here to confirm the input.

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.



There is something wrong with the input data as described below. Check the items displayed in yellow.

***Not all the required items are entered. Enter or select text for the missing items.**

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 to establish information security controls, or is not aware of its necessity.
2.	The management is aware of its necessity to establish information security controls, but only some part of them is implemented.
3.	The rules and controls have been established 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, 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 of other companies by dynamically reflecting the changes of security environment.

Unanswered questions are highlight in yellow color; you need to select the most appropriate one from the list.

(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 make them known to everyone within the company, check the state of implementation, and review them on an as-needed basis.)

Select

Confirm your Input



Be sure to confirm your input before submitting the responses.

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.	
(1)	Does your company have any policies or rules for information security and implement them?	2. Only some part of it is implemented.
(2)	Does your company have an organizational framework which includes the management to promote information security and compliance with law and rules?	3. Implemented but the state has not been reviewed.
(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?	3. Implemented but the state has not been reviewed.
(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, utilization, saving, exchange, provision, deletion and disposal?	

Login ID is included in the diagnostic outcome. You can use the login ID and password from the next time you use the ISM-Benchmark. Be sure not to forget them.

Enter your Organization name/The scope of your self-assessment

Organization/Company Name : SAMPLE Company

The scope of your self-assessment : whole organization

Check the input. If everything is OK, click "To Self Assessment Result."

To Self Assessment Result Back

How to Make Use of the Assessment Result

- Used as a reference material given to external organizations that describes your company's approaches to information security.
- Used as an evaluation indicator for the company you are going to outsource part/parts of your business.

3. The Result of your Self-Assessment

Respond
to the 40 Questions



Confirm
the Input before Submitting



The Result of
your Self-Assessment

This page shows the result of your self-assessment for your security measures.

Based on your answer to 15 questions regarding your company profile, you will be classified into one of the 3 groups, Low, Medium or High. Based on your answer to 25 questions asking the information security countermeasures, your score is calculated. In the result, you can see your security level, the ideal security level and the average, along with recommended security approaches.

Please click the "PDF file" button, if you would like to save the

Results can be saved in PDF format.

PDF file

Information Security Measures Benchmark Ver.3.1

Date : 2008/07/02 16:00
Organization : SAMPLE Company
The scope of your self-assessment: whole organization
Login ID : 666666

Your login ID is displayed.

You can use it from the next time you use the ISM-Benchmark.

SELF ASSESSMENT RESULT

Your company is classified as Group II where medium level IT security measures are required (details described in a separate sheet).

Among Group II, your company is in the position of 51 - 60% from the top.

(Among all the 3 groups, your company is in the position of 51 - 60% from the top.)

Assessment Result (Radar Chart)



Your diagnosis is presented as a radar 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.)

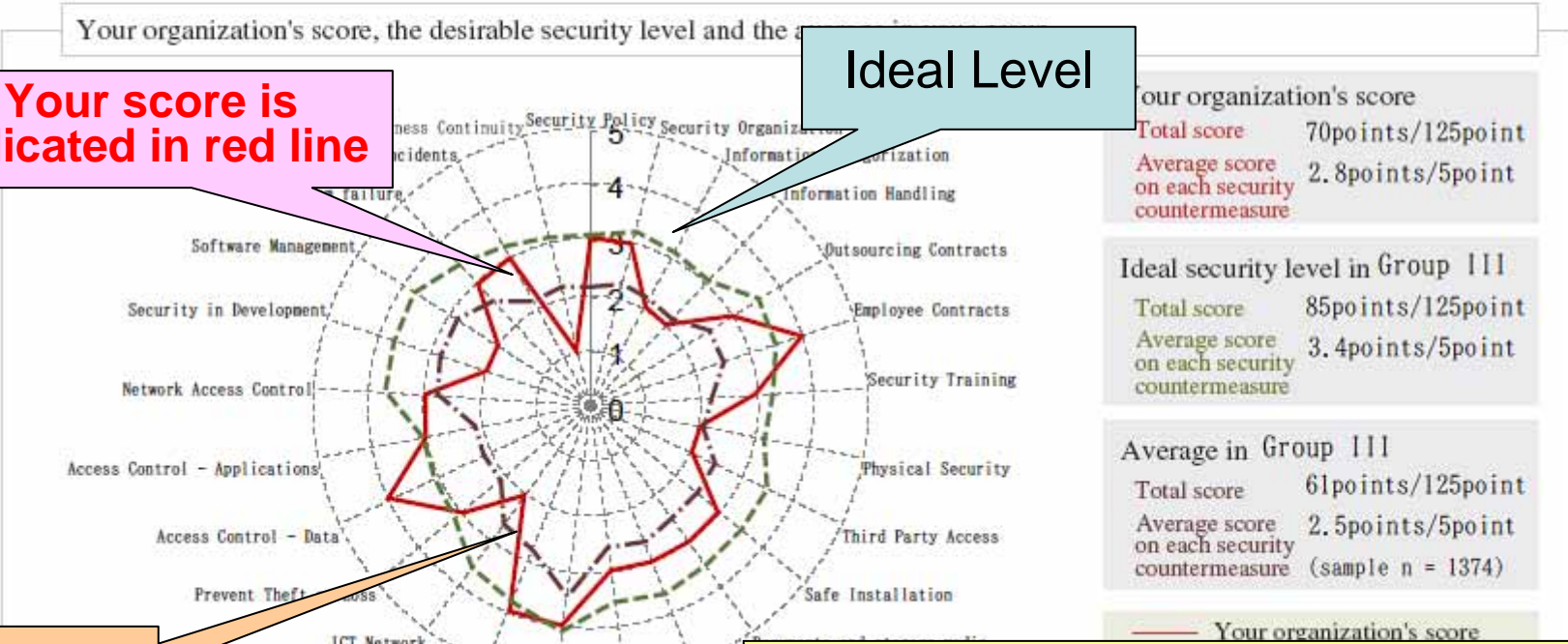
The radar chart below shows your company's score on each security countermeasure, the desirable security level and the average in the group you belong to.

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

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

Your score is indicated in red line

Ideal Level



Your organization's score
 Total score 70points/125point
 Average score on each security countermeasure 2.8points/5point

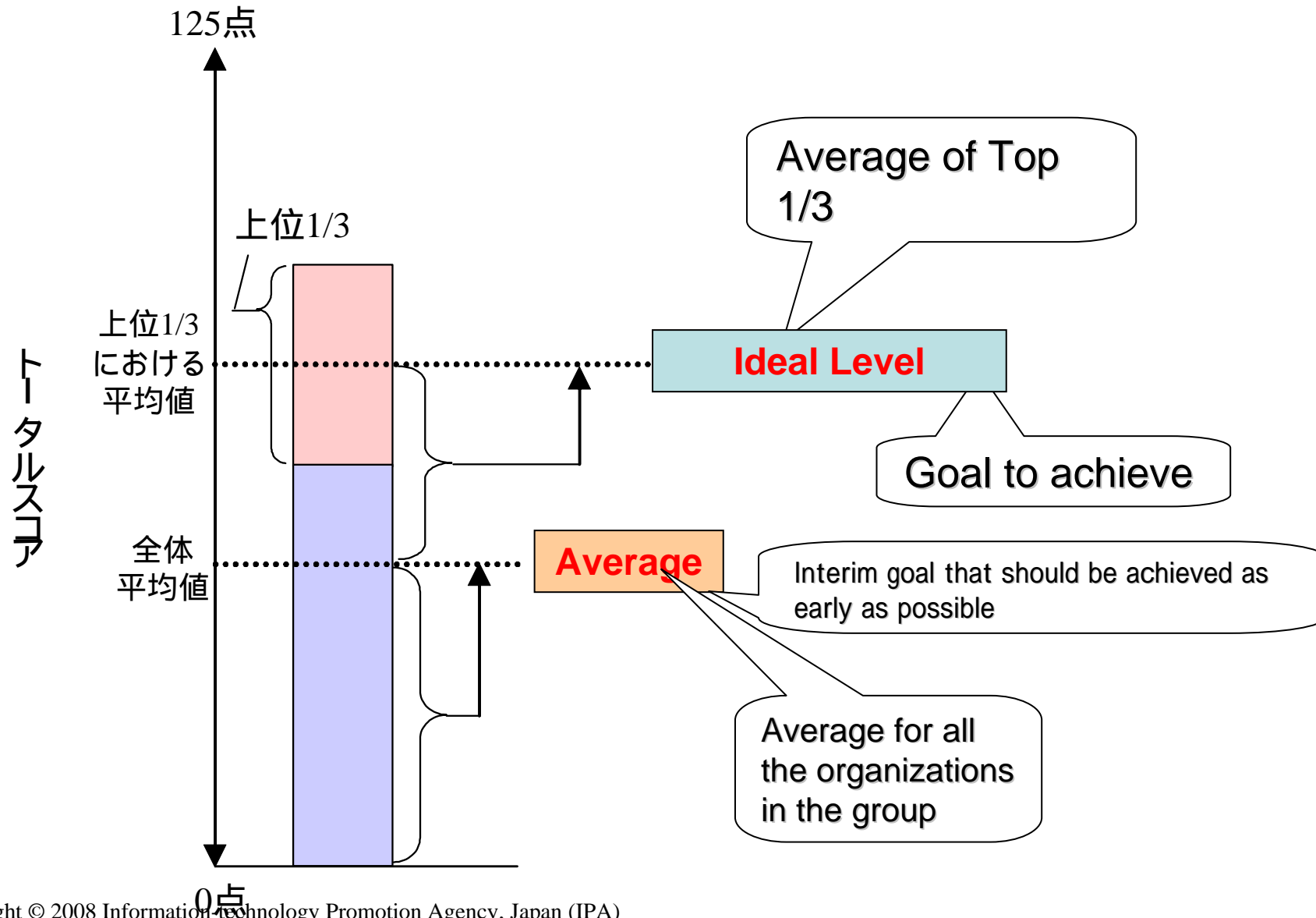
Ideal security level in Group III
 Total score 85points/125point
 Average score on each security countermeasure 3.4points/5point

Average in Group III
 Total score 61points/125point
 Average score on each security countermeasure 2.5points/5point (sample n = 1374)

Average

As the line comes close to the center, your security level indicates low.

What is the Ideal Level?



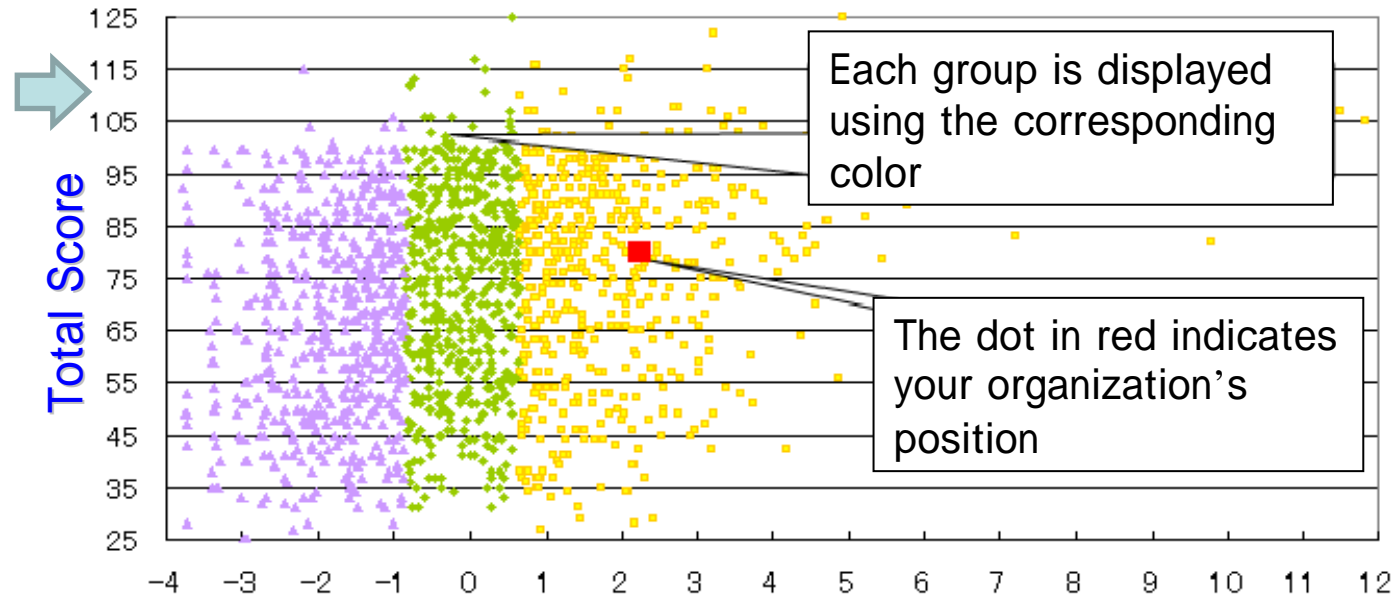
Assessment Result: Scatter Chart



Displays your company's position using a scatter chart.

Y - Axis:
Total Score
(125 points)

25 questions of security measures: each answer is assessed with five grades: 5 x 25 Items = 125 Points

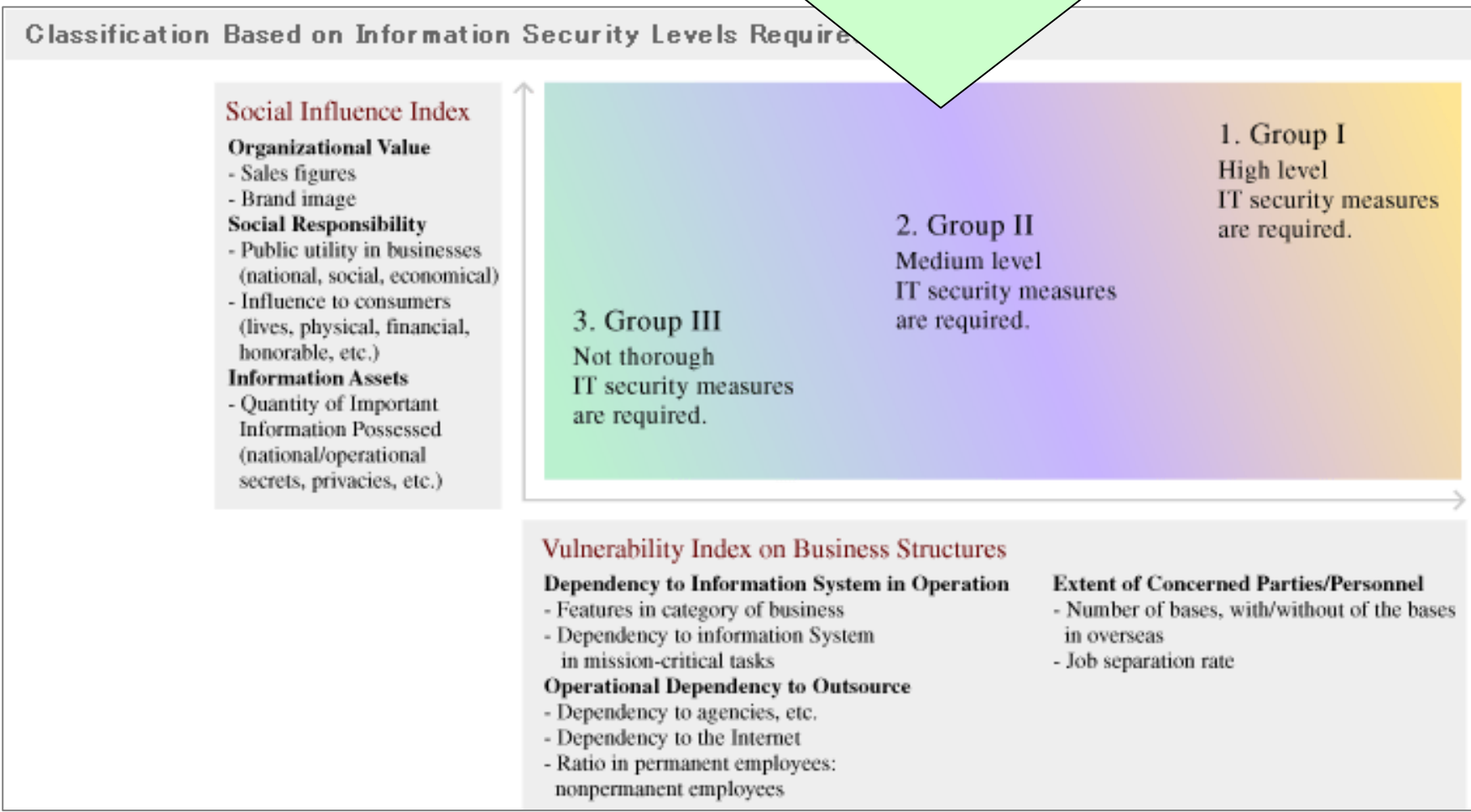


X - Axis: Information Security Risk Index

Index: indicating the risk level calculated based on the answers of Corporate Profile (number of employees, sales figure, etc)

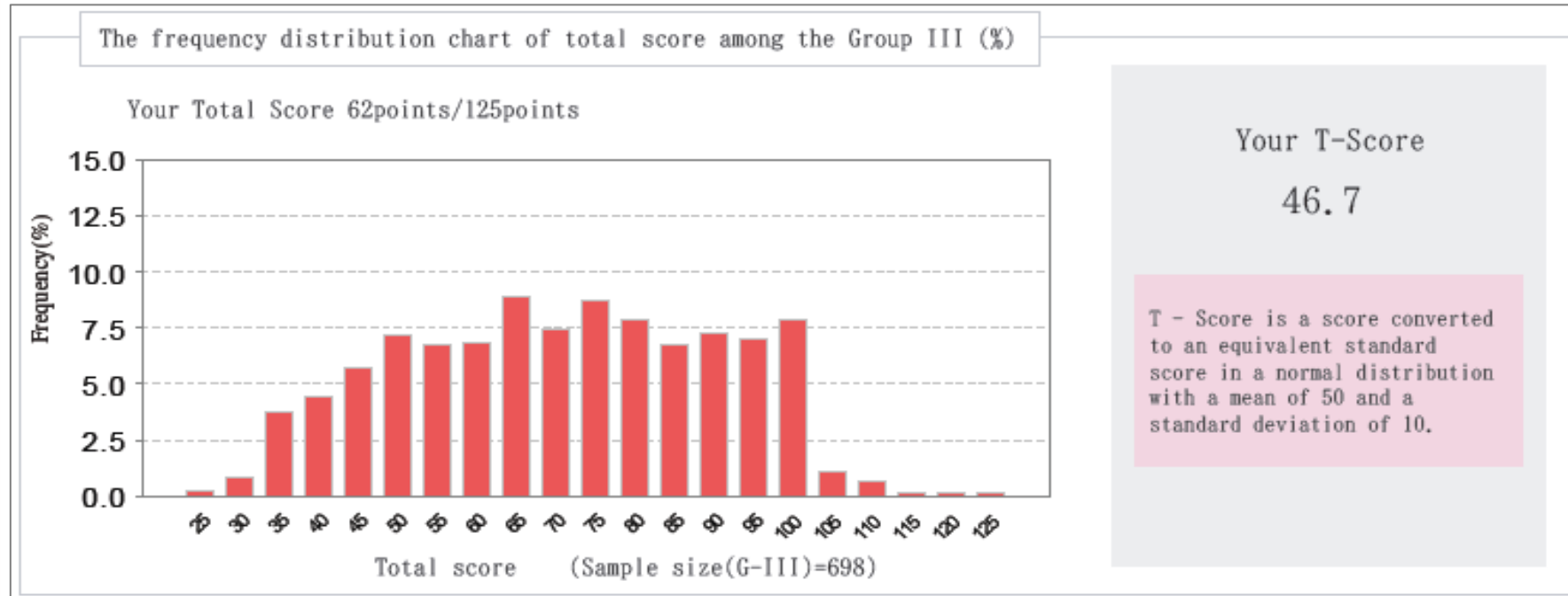
Based on the risk index, organizations are classified into three groups: Group I, Group II and Group III.

Based on the risk index , organizations are classified into three groups: Group I, Group II and Group III .



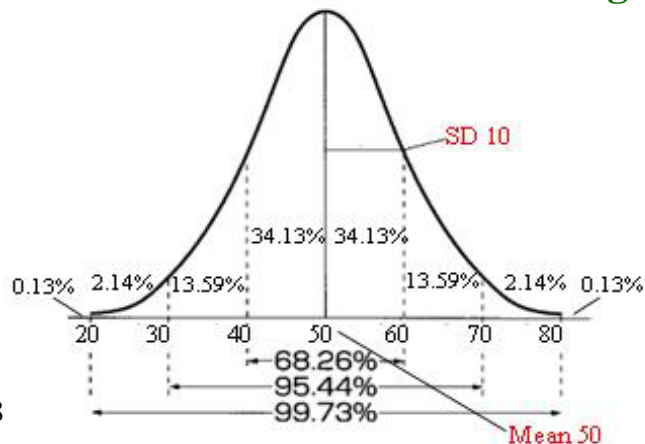
Information Security Risk Index= Vulnerability index on business structures + Social Influence Index

Assessment Result: frequency distribution and T-score of total score



The T- Score is derived by using the equation below.

(Your organization's total score – the average total score of the group) / standard deviation x 10 + 50



T - Score is a score converted to an equivalent standard score in a normal distribution with a mean of 50 and a standard deviation () of 10. As shown in this figure on the left, 68.26% of organizations are within the range of ± 1 (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.

Assessment Result: Recommended Approaches (in HTML only)



The recommended security approaches

The items which you have answered with option 4 (Implemented and the state has been reviewed on regular basis) or option 5 (Implemented enough to be recognized as a good example for other companies)

A further step-up is hoped to the items which you have answered with option 1 (Not implemented) or option 2 (Not implemented but planned). The link to the recommended approaches is shown below. Please refer it for further improvement.

The items which you have answered with option 1 (Not implemented) or option 2 (Not implemented but planned) are shown below. Please refer it for further improvement.

The recommended approaches are shown below. Please refer it for further improvement.

You can see recommended approaches for security measures that are at lower level than required. Using this information, improve those security measures.

Q1-(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?

Explanations :

The contract for business operation or information system management should include information security requirements necessary to prevent information leakage or loss of data, misuse of information and information systems and so on. They should cover the work contents, required level of services that has to be reached, and safety controls that should be implemented in each phase. You also need to request your subcontractor to submit reports and records pertaining to the job, so you can ensure that things are in progress as planned, in pursuance of the terms of the contract.

[More information](#)

Q3-(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?

Explanations :

Appropriate protective measures include using VPN, SSL, or other secure protocols. It is effective to encrypt important data sent by email.

[More information](#)

Assessment Result: Score Chart



Information Security Measures Benchmark - Score Chart			
			Score
Q 1	(1)	Does your company have any policies or rules for information security and implement them?	3
	(2)	Does your company have an organizational framework which includes the management to promote information security and compliance with law and rules?	2
	(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?	2
	(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?	2
	(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?	3
	(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?	2
	(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?	3

Q 5	(1)	Does your company take appropriate measures for the case of information system failures?	2
	(2)	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?	2
	(3)	Does your company have a company-wide framework for BCM iBusiness Continuity Management jfor the case of system down?	1
Total			64
Average			2.6

Assessment Result: Summary



Both comparative and quantitative assessments with various comparative functions

- ⊕ Distribution of total scores and position are shown in a scatter chart
 - Shows two types of information: 3 groups or company-size-based
 - Can compare current position and past two positions
- ⊕ Rader chart shows scores in the following four different forms:
 - Risk based group (classified by IS Risk Index)
 - Company-size based (Large company and SME)
 - Business industry based
 - Your company's current position and past two positions
- ⊕ Shows frequency distribution and T-score of total scores
- ⊕ Shows a list of scores
- ⊕ Displays recommended approaches

Results can be shown both in Html & PDF formats

Assessment results can be used to provide information to contractors etc

2. How to use ISM-Benchmark - using your log-in account

Using your log-in account



What is Information Security Measures Benchmark?

Information Security Measures Benchmark is a self-assessment tool to visually check where the level of your company's security measures resides by responding to questions relevant to security measures (25 questions) and to company profile (15 questions).

Issue of your log-in account

You can apply to issue your log in account after you answered all the questions in your self-assessment. The registration of the log-in account is optional. If you register your login account, you can enter your own page named "MY Page" where you can use variety of functions such as conduct a new diagnosis using your answers stored in the system, or correct answers and so on.

- If you apply to register your log-in account, the account number will be displayed in the diagnosis result page.
Please keep and remember your account and password as it is necessary to enter it when you log-in to your "MY Page".

Self-Assessment Test

[Click here to begin your Self-Assessment](#)

If you have your log-in account, please enter your ID and password to log in.

ID:

Password:

Login

If you have login ID and password, please enter them.

Then you can use "my page function"!

The My Page



MY Page

The previous self-check: 2008/06/09
The latest log-in: 2008/06/12

▶ Corrects answers (conducts diagnosis again)

Displays the latest answers stored, enabling you to correct answers you entered before.

(If you made correction, the previous answers would be overwritten and the current answers registered.)

▶ Displays the result of the latest diagnosis

Displays the latest answers stored and shows the result of the latest diagnosis.

▶ Conducts a new diagnosis using the answers stored

Displays the latest answers stored, enabling you to change where necessary, so that you can save time of answering all the questions.

(The previous answers remain as it is and the current result would be registered as the latest one.)

▶ Changes your password

Changes your password to log in.

▶ Deletes account

Deletes and disables your login ID and

If you log into the system, My Page is displayed; you can correct answers stored in the system and conduct the diagnosis again (or conduct a new diagnosis). Because the answers you gave in the previous diagnosis are displayed, you do not need to reenter all the necessary information.

3. Other informations

- Statistic data**
- What you can do with ISM-Benchmark?**

The Statistic data of ISM-Benchmark

- ⊕ From ver. 3.1, statistic information for basic data that is used for the diagnosis is made available to the public.
- ⊕ To increase trust level of and transparency to diagnosis

Statistic information is available at:

http://www.ipa.go.jp/security/benchmark/benchmark_tokuchover31.html#toukei

The desirable security level and average is calculated based on the data stored in Japanese benchmark system currently.

In future, if the sufficient amount of the assessment data of the particular nation will be stored in the English benchmark system, it might be possible to calculate and show the result based on the data of the particular nation.

What you can do with ISM-Benchmark?



- Use to grasp your company's security level
 - Where to start?
 - **Plan**: What controls should be considered?
 - Consider which security level you should aim?
 - **Do and Check** : Analyze your weakness comparing with other companies.
 - **Act**: Use for further improvement.
- Use to show your business partners your security level in order to be competitive.
- Use to provide consultation
 - can be used as educational materials

Japanese ISM-Benchmark Portal Site

<http://www.ipa.go.jp/security/benchmark/>



こんなときに！



30分程度で自己診断ができます。ぜひご利用下さい。

診断サイトはこちら



ENTER

Click here to move to the Self-Assessment page.

Information contained in ISM-Benchmark portal site

- What is the ISM-Benchmark
- Characteristics of the ISM-Benchmark ver.3.1
 - Statistical Information
- How to use the ISM-Benchmark
- Handbook on how to make use of the ISM-Benchmark
- List of questions about the ISM-Benchmark
- Recommended approaches
- FAQ about the ISM-Benchmark
- Materials on the ISM-Benchmark

ISM-Benchmark portal site contains various information.

It takes only about 30 minutes to finish Self-assessment.
Please feel free to use this diagnosis system.



Input



Provides answers to 40 questions on the Web

i.e. Does your company have any policies or rules for information security and implement them?

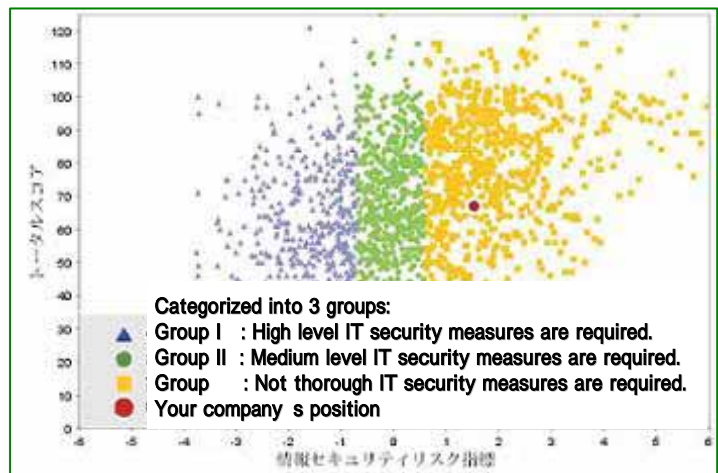
Assessment Items (40 Items in Total)

- Information Security Measures (25 Items)**
- Organizational security
 - Physical and environmental security
 - Communications and operations management
 - Access control, Systems development and maintenance
 - Security incidents and malfunctions

- Corporate Profile (15 Items)**
- Number of employees, sale figures, number of basis
 - Number of people whose information is held, degree of dependence on Information Technology

Self Assessment Result

1. Displays your company's position using a scatter chart.
2. Compares your organization's score with the desirable security level and the average in your business industry, using a radar chart.
3. Shows your score
4. Displays recommended security approaches.



Example of Self Assessment Result (Scatter Chart)

Thank you!



IPA <http://www.ipa.go.jp/>
Email : isec-info@ipa.go.jp
2-28-8 Hon-Komagome
Bunkyo-ku, Tokyo 113-6591, Japan

