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

Click here to the assessment page

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
Current version is 3.1

You can download 25 questions regarding security measures from here

[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.
How 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”.

Click here to start your self-assessment
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.
Part I: 25 Questions

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

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

1. The management is not aware of its necessity.
2. The management is aware of its necessity (company-wide, but only some part 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 regular 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 in the security environment.

(1) Does your company have any policies or rules related to information security and establish policies/rules based on your company’s business and organization? (If you do not have, state the reason.) (If you have, you need to check with everyone within the company, check the state of implementation, and review them on an annual 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.
25 questions about security measures

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) (6 questions)

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:
# How to Answer 25 questions

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

## Not implemented

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

## Implemented
If you click this button, you will see tips for the security measures and recommended approaches.
### Part II: About Your Company Profile (16 Questions)

<table>
<thead>
<tr>
<th>Question</th>
<th>Response Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>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)</td>
<td>Approximately, [ ] (% use one-byte numerical characters only, for example, 1000)</td>
</tr>
<tr>
<td>Total number of employees:</td>
<td></td>
</tr>
<tr>
<td>Percentage of permanent employees:</td>
<td></td>
</tr>
<tr>
<td>Q2: What are your company’s sales figures? (sales of headquarter and branch offices) (Even for departmental assessments, if you are governmental organization)</td>
<td>Sales figures: [ ] (example, 100,000 USD)</td>
</tr>
<tr>
<td>Capital fund:</td>
<td>Capital fund: [ ] (example, 10,000,000 USD)</td>
</tr>
<tr>
<td>Total number of domestic offices (including headquarters and branch offices):</td>
<td>Total number of domestic offices: [ ] (example, 10)</td>
</tr>
<tr>
<td>The number of overseas offices (including headquarters and branch offices):</td>
<td>The number of overseas offices: [ ] (example, 1)</td>
</tr>
</tbody>
</table>
| Your country:                                                           | Your country: Select [ ]
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)
1. Respond to the 40 Questions

Respond to all the questions provided on this website. 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.


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 part of them is in control.
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 department.
5. In addition to those described in item 4 above, your company has improved it to become a good example for companies by dynamically reflecting the changes of security environment.

(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.)

Unanswered questions are highlighted in yellow color; you need to select the most appropriate one from the list.
### Confirm your Input

Be sure to confirm your input before submitting the responses.

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

<table>
<thead>
<tr>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Does your company have any policies or rules for information security and implement them?</td>
</tr>
<tr>
<td>(2) Does your company have an organizational framework which includes the management to promote information security and compliance with law and rules?</td>
</tr>
<tr>
<td>(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?</td>
</tr>
<tr>
<td>(4) Does your company exercise appropriate security measures to protect the 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?</td>
</tr>
</tbody>
</table>

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

| Organization/Company Name: | SAMPLE Company |
| The scope of your self-assessment: | whole organization |

---

- 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.
- Check the input. If everything is OK, click “To Self Assessment Result.”
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

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 in PDF format.

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 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:

<table>
<thead>
<tr>
<th>Security Countermeasure</th>
<th>Your Organization's Score</th>
<th>Desirable Security Level</th>
<th>Average in Group III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Score</td>
<td>70 points / 125 points</td>
<td>85 points / 125 points</td>
<td>61 points / 125 points</td>
</tr>
<tr>
<td>Average Score</td>
<td>2.8 points / 5 points</td>
<td>3.4 points / 5 points</td>
<td>2.5 points / 5 points</td>
</tr>
</tbody>
</table>

Ideal security level in Group III:

Ideal Level

Your score is indicated in red line.

As the line comes closer to the center, your security level indicates low.
What is the Ideal Level?

Average of Top 1/3

Goal to achieve

Average for all the organizations in the group

Ideal Level
Assessment Result: Scatter Chart
Based on the risk index, organizations are classified into three groups: Group I, Group II and Group III.

### Classification Based on Information Security Levels Required

<table>
<thead>
<tr>
<th>Social Influence Index</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organizational Value</strong></td>
</tr>
<tr>
<td>- Sales figures</td>
</tr>
<tr>
<td>- Brand image</td>
</tr>
<tr>
<td><strong>Social Responsibility</strong></td>
</tr>
<tr>
<td>- Public utility in businesses (national, social, economical)</td>
</tr>
<tr>
<td>- Influence to consumers (lives, physical, financial, honorable, etc.)</td>
</tr>
<tr>
<td><strong>Information Assets</strong></td>
</tr>
<tr>
<td>- Quantity of Important Information Possessed (national/operational secrets, privacies, etc.)</td>
</tr>
</tbody>
</table>

1. **Group I**
   - High level
   - IT security measures are required.

2. **Group II**
   - Medium level
   - IT security measures are required.

3. **Group III**
   - Not thorough
   - IT security measures are required.

### Vulnerability Index on Business Structures

<table>
<thead>
<tr>
<th>Dependency to Information System in Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Features in category of business</td>
</tr>
<tr>
<td>- Dependency to information System in mission-critical tasks</td>
</tr>
<tr>
<td><strong>Operational Dependency to Outsource</strong></td>
</tr>
<tr>
<td>- Dependency to agencies, etc.</td>
</tr>
<tr>
<td>- Dependency to the Internet</td>
</tr>
<tr>
<td>- Ratio in permanent employees: nonpermanent employees</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Extent of Concerned Parties/Personnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Number of bases, with/without of the bases in overseas</td>
</tr>
<tr>
<td>- Job separation rate</td>
</tr>
</tbody>
</table>

Vulnerability index on business structures + Social Influence Index
The T-score is derived by using the equation below.

\[
(\text{Your organization’s total score} - \text{the average total score of the group}) / \text{standard deviation} \times 10 + 50
\]

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

As shown in this figure on the left, 68.26% of organizations are within the range of 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.
You can see recommended approaches for security measures that are at lower level than required. Using this information, improve those security measures.

Q1-(G) 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-(G) 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

<table>
<thead>
<tr>
<th>Q 1</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Does your company have any policies or rules for information security and implement them?</td>
<td>3</td>
</tr>
<tr>
<td>(2) Does your company have an organizational framework which includes the management to promote information security and compliance with law and rules?</td>
<td>2</td>
</tr>
<tr>
<td>(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?</td>
<td>2</td>
</tr>
<tr>
<td>(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?</td>
<td>2</td>
</tr>
<tr>
<td>(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?</td>
<td>3</td>
</tr>
<tr>
<td>(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?</td>
<td>2</td>
</tr>
<tr>
<td>(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?</td>
<td>3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Q 5</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Does your company take appropriate measures for the case of information system failures?</td>
<td>2</td>
</tr>
<tr>
<td>(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?</td>
<td>2</td>
</tr>
<tr>
<td>(3) Does your company have a company-wide framework for BCM iBusiness Continuity Management if for the case of system down?</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>2.6</td>
</tr>
</tbody>
</table>
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”.

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 password. | |
3. Other informations
   - Statistic data
   - What you can do with 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:

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/

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.
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