

ISM-Benchmark ver.3.1 – Basic data for diagnosis: Desirable security level and average

The Information Security 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. Based on your answer to questions, your score¹ is calculated. Result of the self-assessment is presented in score or charts (Radar chart, distribution chart etc.) Using those charts, you can compare your result with that of others who have performed this self-assessment.

Self-assessment results contain the following items:

[Assessment Results]

1. Distribution 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 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.

Considering rapidly changing information security environment, ISM-Benchmark ver. 3.1 was designed to use the data of the past two years as basic data for diagnosis. Average scores and Desired Levels² for those basic data (2165 records, from Mar. 20, 2006 to Dec. 17, 2007) are as follows:

1. Average scores and Desired Levels (Group-Based)

Based on information security risk index³, organizations are classified into three groups: Group I (high level IT security measures are required), Group II (Medium level IT security measures are required) and Group III (Not thorough level IT security measures are required.) You can get your group's average score and desired level. You can also compare your organization's information security approaches with those of other organizations. Table 1 shows average scores and desired levels for each group.

¹ Based on your answer to 25 questions (5 sections) related to security measures, your score is calculated. The highest score is 125 points with each question giving 5 points at best.

² Desired level is at the same or higher level of top one-third of organizations in the same group

³ Information Security Risk Index indicates risks to which organization is being exposed. Information Security Risk Index is calculated based on several factors, including the number of employees, sales figures, the number of critical information held and degree of dependence on information technology.

Table 1 Average scores and desired levels for each group (2165 records, from Mar. 20, 2006 to Dec. 17, 2007)

Sections	Questions	Serial Numbers	Average			Desired Level		
			G I	G II	G III	G I	G II	G III
1	(1) Security Policy	1	3.21	2.98	2.72	4.11	3.97	3.78
	(2) Security Organization	2	3.24	2.95	2.65	4.13	3.92	3.69
	(3) Information Categorization	3	2.93	2.79	2.61	3.94	3.69	3.49
	(4) Information Handling	4	3.08	2.89	2.67	3.97	3.76	3.59
	(5) Outsourcing Contracts	5	3.27	3.00	2.78	4.05	3.81	3.74
	(6) Employee Contracts	6	3.40	3.15	2.86	4.18	4.01	3.82
	(7) Security Training	7	3.12	2.85	2.59	4.06	3.94	3.62
2	(1) Physical Security	8	3.27	3.02	2.73	4.15	3.98	3.75
	(2) Third Party Access	9	2.95	2.69	2.48	3.86	3.68	3.41
	(3) Safe Installation	10	3.19	3.07	2.81	4.03	3.89	3.74
	(4) Documents and storage media	11	3.15	3.05	2.87	3.99	3.84	3.61
3	(1) Operational environment	12	3.22	3.10	2.83	4.01	3.86	3.75
	(2) IT system operation	13	3.14	2.98	2.72	4.04	3.88	3.71
	(3) Malware	14	3.91	3.83	3.70	4.35	4.25	4.16
	(4) Vulnerability	15	3.38	3.25	3.09	4.07	3.98	3.81
	(5) ICT Network	16	3.21	3.06	2.75	3.94	3.80	3.68
	(6) Prevent Theft or Loss	17	3.01	2.68	2.51	4.02	3.82	3.59
4	(1) Access Control - Data	18	3.39	3.24	3.01	4.12	4.01	3.84
	(2) Access Control Applications	19	3.36	3.24	2.98	4.06	3.94	3.83
	(3) Network Access Control	20	3.51	3.38	3.07	4.13	4.04	3.96
	(4) Security in Development	21	2.81	2.62	2.36	3.72	3.56	3.43
	(5) Software Management	22	2.72	2.58	2.40	3.67	3.50	3.37
5	(1) IT system failure	23	3.14	2.97	2.76	3.93	3.74	3.59
	(2) Security Incidents	24	3.00	2.65	2.38	4.04	3.80	3.50
	(3) Business Continuity	25	2.65	2.35	2.29	3.62	3.19	3.15

Note : GI=Group I, GII=Group II, GIII=Group III

2. Average scores and Desired Levels (Organization-Size-Based)

Results of self-assessment are shown in the Rader Chart. You can compare your score with that of others in the same group which was classified based on the size of the organization. Organizations with more than 300 employees are considered a large company, whereas those with 300 or less employees a small or medium-sized company. After the size-based classification is performed, each group is classified further into small groups based on the information security risk index. Table 2 and Table 3 show average scores and desired levels for each group.

Table 2 Small or medium-sized organizations (with 300 employees or less)
Average scores and desired levels for each group (1306 records, from Mar. 20, 2006 to Dec. 17, 2007)

Sections	Questions	Serial Numbers	Average			Desired Level		
			G I	G II	G III	G I	G II	G III
1	(1) Security Policy	1	2.97	2.75	2.61	3.94	3.89	3.68
	(2) Security Organization	2	2.95	2.65	2.52	3.95	3.74	3.56
	(3) Information Categorization	3	2.78	2.64	2.56	3.86	3.62	3.47
	(4) Information Handling	4	2.90	2.74	2.57	3.84	3.73	3.54
	(5) Outsourcing Contracts	5	3.08	2.83	2.64	3.97	3.73	3.61
	(6) Employee Contracts	6	3.25	3.01	2.72	4.12	3.90	3.73
	(7) Security Training	7	2.87	2.68	2.51	3.92	3.81	3.51
2	(1) Physical Security	8	3.01	2.82	2.60	3.98	3.82	3.59
	(2) Third Party Access	9	2.76	2.58	2.39	3.81	3.59	3.37
	(3) Safe Installation	10	3.03	2.95	2.73	3.93	3.83	3.63
	(4) Documents and storage media	11	3.04	3.01	2.84	3.97	3.83	3.60
3	(1) Operational environment	12	3.05	3.00	2.73	3.96	3.84	3.60
	(2) IT system operation	13	2.98	2.84	2.62	3.90	3.82	3.63
	(3) Malware	14	3.78	3.73	3.61	4.18	4.18	4.06
	(4) Vulnerability	15	3.25	3.18	3.02	3.97	3.91	3.74
	(5) ICT Network	16	3.01	2.88	2.59	3.77	3.62	3.48
	(6) Prevent Theft or Loss	17	2.83	2.56	2.43	3.93	3.78	3.50
4	(1) Access Control - Data	18	3.27	3.14	2.89	4.07	3.93	3.79
	(2) Access Control - Applications	19	3.22	3.11	2.86	4.02	3.87	3.79
	(3) Network Access Control	20	3.29	3.21	2.92	4.07	4.01	3.84
	(4) Security in Development	21	2.64	2.54	2.30	3.56	3.59	3.38
	(5) Software Management	22	2.58	2.54	2.34	3.63	3.51	3.31
5	(1) IT system failure	23	3.03	2.91	2.64	3.83	3.75	3.48
	(2) Security Incidents	24	2.79	2.48	2.22	3.92	3.73	3.32
	(3) Business Continuity	25	2.51	2.30	2.27	3.57	3.27	3.23

Note: GI=Group I, GII=Group II, GIII=Group III

Table 3 Large organization (with more than 300 employees)
Average scores and desired levels for each group (859 records, from Mar. 20, 2006 to Dec. 17, 2007)

Sections	Questions	Serial Numbers	Average			Desired Level		
			G I	G II	G III	G I	G II	G III
1	(1) Security Policy	1	3.47	3.29	2.99	4.27	4.03	3.98
	(2) Security Organization	2	3.57	3.35	3.01	4.27	4.05	3.87
	(3) Information Categorization	3	3.09	2.98	2.75	4.01	3.76	3.53
	(4) Information Handling	4	3.27	3.10	2.92	4.08	3.81	3.69
	(5) Outsourcing Contracts	5	3.49	3.23	3.14	4.12	3.96	3.89
	(6) Employee Contracts	6	3.57	3.34	3.23	4.23	4.07	3.92
	(7) Security Training	7	3.40	3.08	2.81	4.14	4.00	3.81

2	(1) Physical Security	8	3.55	3.30	3.06	4.25	4.08	3.90
	(2) Third Party Access	9	3.16	2.84	2.69	3.92	3.68	3.65
	(3) Safe Installation	10	3.38	3.23	3.03	4.10	3.98	3.84
	(4) Documents and storage media	11	3.28	3.11	2.94	4.03	3.89	3.73
3	(1) Operational environment	12	3.41	3.25	3.09	4.11	3.90	3.98
	(2) IT system operation	13	3.33	3.15	2.97	4.15	3.96	3.82
	(3) Malware	14	4.06	3.98	3.92	4.45	4.34	4.34
	(4) Vulnerability	15	3.53	3.35	3.24	4.12	4.07	3.92
	(5) ICT Network	16	3.43	3.31	3.18	4.03	3.99	4.08
	(6) Prevent Theft or Loss	17	3.21	2.85	2.71	4.11	3.85	3.71
4	(1) Access Control - Data	18	3.51	3.38	3.33	4.15	4.07	3.94
	(2) Access Control - Applications	19	3.50	3.41	3.30	4.10	4.00	3.98
	(3) Network Access Control	20	3.76	3.61	3.46	4.20	4.09	4.10
	(4) Security in Development	21	3.01	2.73	2.54	3.89	3.61	3.40
	(5) Software Management	22	2.87	2.64	2.56	3.76	3.57	3.57
5	(1) IT system failure	23	3.26	3.04	3.08	4.01	3.74	3.87
	(2) Security Incidents	24	3.23	2.87	2.82	4.15	3.86	3.79
	(3) Business Continuity	25	2.81	2.43	2.36	3.72	3.16	3.11

Note : GI=Group I, GII=Group II, GIII=Group III

3. Average scores and Desired Levels (Industry-Based)

For ISM-Benchmark, Japan Standard Industry Classification is applied to perform industry classification. Japan Standard Industry Classification defines 24 types of industries. However, considering that some industries may have little records to compare, we selected the following ten industries for comparison (figure in parenthesis indicates the number of records). Table 4 shows average scores and desired levels for each industry.

- (1) Agriculture, Forestry and Fisheries (5)
- (2) Building Industry (260)
- (3) Manufacturing (638)
- (4) Electric Power Supply, Gas Service, Heat Supply, Waterworks, Traffic (42)
- (5) Information Service (470)
- (6) Tel-Communication, Broadcasting, ISP/ASP, Publishing/Newspaper (52)
- (7) Wholesale/Retail Sales (197)
- (8) Financial/Insurance (71)
- (9) Real Estate, Restaurant/Travel/Hotel, Medical/Public Welfare, Education, Prep school (67)
- (10) Other Services (including Government, Public Agency, Public-Interest Corporations) (363)

Table 4 Average scores and desired levels for each industry (part 1)

Sections	Questions	Serial Numbers	Agriculture, Forestry and Fisheries		Building Industry		Manufacturing	
			Average	Desired Level	Average	Desired Level	Average	Desired Level
1	(1) Security Policy	1	2.40	2.40	2.83	3.72	2.87	3.97
	(2) Security Organization	2	2.60	2.60	2.71	3.66	2.88	3.94
	(3) Information Categorization	3	1.40	1.40	2.78	3.59	2.66	3.58
	(4) Information Handling	4	2.40	2.40	2.74	3.57	2.71	3.57
	(5) Outsourcing Contracts	5	2.40	2.40	2.77	3.59	2.88	3.77
	(6) Employee Contracts	6	2.40	2.40	2.85	3.65	2.97	3.90
	(7) Security Training	7	1.60	1.60	2.69	3.59	2.68	3.82
2	(1) Physical Security	8	3.20	3.20	2.75	3.64	2.88	3.84
	(2) Third Party Access	9	2.60	2.60	2.45	3.29	2.57	3.54
	(3) Safe Installation	10	2.60	2.60	2.94	3.76	2.89	3.77
	(4) Documents and storage media	11	2.20	2.20	2.94	3.69	2.85	3.68
3	(1) Operational environment	12	2.40	2.40	2.95	3.83	2.96	3.82
	(2) IT system operation	13	2.80	2.80	2.86	3.77	2.84	3.79
	(3) Malware	14	3.60	3.60	3.67	4.11	3.80	4.28
	(4) Vulnerability	15	2.00	2.00	3.18	3.92	3.21	3.93
	(5) ICT Network	16	3.00	3.00	2.70	3.58	3.06	3.90
	(6) Prevent Theft or Loss	17	3.00	3.00	2.48	3.43	2.63	3.75
4	(1) Access Control - Data	18	2.60	2.60	3.05	3.84	3.13	3.95
	(2) Access Control - Applications	19	2.40	2.40	3.11	3.93	3.11	3.88
	(3) Network Access Control	20	2.80	2.80	3.10	3.91	3.31	4.08
	(4) Security in Development	21	2.00	2.00	2.40	3.45	2.48	3.42
	(5) Software Management	22	1.80	1.80	2.55	3.49	2.46	3.40
5	(1) IT system failure	23	2.00	2.00	2.85	3.67	2.95	3.74
	(2) Security Incidents	24	2.20	2.20	2.41	3.48	2.59	3.76
	(3) Business Continuity	25	1.80	1.80	2.41	3.30	2.33	3.16

Note: Because Agriculture, Forestry and Fisheries has only five records, it was difficult to calculate the desired level, which indicates the level of top one-third of organization in the same industry, and therefore, average score was shown in the desired level column.

Table 5 Average scores and desired levels for each industry (part 2)

Sections	Questions	Serial Numbers	Electric Power Supply, Gas Service, Heat Supply, Waterworks, Traffic		Information Service		Tel-Communication, Broadcasting, ISP/ASP, Publishing/Newspaper	
			Average	Desired Level	Average	Desired Level	Average	Desired Level
1	(1) Security Policy	1	2.98	4.08	3.42	4.17	2.90	4.00
	(2) Security Organization	2	3.15	4.15	3.35	4.12	2.87	4.06
	(3) Information Categorization	3	2.83	4.00	3.17	3.99	2.85	3.88
	(4) Information Handling	4	2.85	3.92	3.36	4.13	2.98	4.00
	(5) Outsourcing Contracts	5	2.95	3.69	3.51	4.08	3.15	4.06
	(6) Employee Contracts	6	2.83	4.00	3.67	4.18	3.19	4.06
	(7) Security Training	7	2.61	3.85	3.45	4.12	3.00	3.94
2	(1) Physical Security	8	2.81	4.00	3.52	4.23	3.21	4.29
	(2) Third Party Access	9	2.39	3.62	3.27	3.97	2.96	4.12
	(3) Safe Installation	10	3.05	4.15	3.37	4.10	3.15	3.94
	(4) Documents and storage media	11	3.00	4.00	3.44	4.06	3.12	3.88
3	(1) Operational environment	12	3.22	4.08	3.33	4.00	3.17	4.24
	(2) IT system operation	13	2.88	4.00	3.27	4.03	3.06	4.00
	(3) Malware	14	3.81	4.31	3.96	4.33	3.94	4.29
	(4) Vulnerability	15	3.17	3.77	3.50	4.06	3.48	4.18
	(5) ICT Network	16	2.90	3.77	3.25	3.87	3.02	3.88
	(6) Prevent Theft or Loss	17	2.63	3.77	3.22	4.05	2.81	4.00
4	(1) Access Control - Data	18	3.02	3.92	3.57	4.09	3.33	4.24
	(2) Access Control - Applications	19	2.83	3.69	3.50	4.06	3.21	4.12
	(3) Network Access Control	20	3.15	4.00	3.63	4.12	3.31	4.12
	(4) Security in Development	21	2.63	3.69	2.97	3.74	2.58	3.71
	(5) Software Management	22	2.61	3.77	2.80	3.67	2.56	3.82
5	(1) IT system failure	23	3.15	4.23	3.16	3.92	2.85	3.77
	(2) Security Incidents	24	2.54	3.77	3.16	4.06	2.85	3.88
	(3) Business Continuity	25	2.39	3.39	2.74	3.69	2.56	3.65

Table 6 Average scores and desired levels for each industry (part 3)

Sections	Questions	Serial Numbers	Wholesale/Retail Sales		Financial/Insurance		Real Estate, Restaurant/Travel/Hotel, Medical/Public Welfare, Education, Prep school	
			Average	Desired Level	Average	Desired Level	Average	Desired Level
1	(1) Security Policy	1	2.90	3.86	3.16	3.91	2.31	3.05
	(2) Security Organization	2	2.93	3.85	3.39	3.96	2.27	3.00
	(3) Information Categorization	3	2.59	3.48	2.89	3.78	2.18	3.09
	(4) Information Handling	4	2.67	3.63	3.11	3.83	2.42	3.36
	(5) Outsourcing Contracts	5	2.91	3.75	3.18	3.74	2.64	3.46
	(6) Employee Contracts	6	3.12	3.91	3.63	4.13	2.70	3.46
	(7) Security Training	7	2.81	3.88	2.83	3.57	2.09	2.91
2	(1) Physical Security	8	2.88	3.82	3.16	4.00	2.63	3.46
	(2) Third Party Access	9	2.54	3.39	2.79	3.61	2.21	2.96
	(3) Safe Installation	10	3.15	3.91	3.18	4.00	2.55	3.41
	(4) Documents and storage media	11	2.91	3.65	3.34	4.04	2.57	3.41
3	(1) Operational environment	12	3.13	3.85	3.24	4.04	2.46	3.59
	(2) IT system operation	13	2.92	3.80	3.04	3.91	2.45	3.59
	(3) Malware	14	3.92	4.32	3.79	4.09	3.37	4.00
	(4) Vulnerability	15	3.25	4.03	3.13	3.70	2.66	3.59
	(5) ICT Network	16	3.19	3.97	3.13	3.96	2.61	3.55
	(6) Prevent Theft or Loss	17	2.73	3.82	3.01	4.04	2.08	3.27
4	(1) Access Control - Data	18	3.19	3.99	3.49	4.13	2.61	3.59
	(2) Access Control - Applications	19	3.26	3.91	3.47	4.13	2.79	3.68
	(3) Network Access Control	20	3.45	4.12	3.51	4.04	2.70	3.46
	(4) Security in Development	21	2.68	3.62	2.79	3.78	2.05	3.09
	(5) Software Management	22	2.71	3.54	2.62	3.78	1.93	2.96
5	(1) IT system failure	23	2.99	3.75	3.03	3.87	2.51	3.50
	(2) Security Incidents	24	2.62	3.75	2.93	3.96	1.91	3.09
	(3) Business Continuity	25	2.41	3.22	2.62	3.65	1.94	2.91

Table 7 Average scores and desired levels for each industry (part 4)

Sections	Questions	Serial Numbers	Other Services (including public institutions)	
			Average	Desired Level
1	(1) Security Policy	1	2.86	3.92
	(2) Security Organization	2	2.84	3.90
	(3) Information Categorization	3	2.71	3.78
	(4) Information Handling	4	2.84	3.82
	(5) Outsourcing Contracts	5	2.95	3.91
	(6) Employee Contracts	6	3.03	4.06
	(7) Security Training	7	2.77	3.90
2	(1) Physical Security	8	2.91	3.93
	(2) Third Party Access	9	2.64	3.65
	(3) Safe Installation	10	2.89	3.84
	(4) Documents and storage media	11	2.98	3.89
3	(1) Operational environment	12	2.98	3.89
	(2) IT system operation	13	2.90	3.91
	(3) Malware	14	3.79	4.23
	(4) Vulnerability	15	3.14	3.90
	(5) ICT Network	16	2.82	3.79
	(6) Prevent Theft or Loss	17	2.61	3.75
4	(1) Access Control - Data	18	3.14	3.97
	(2) Access Control - Applications	19	3.07	3.92
	(3) Network Access Control	20	3.20	4.02
	(4) Security in Development	21	2.57	3.57
	(5) Software Management	22	2.53	3.53
5	(1) IT system failure	23	2.89	3.70
	(2) Security Incidents	24	2.61	3.80
	(3) Business Continuity	25	2.36	3.29

Relevant Materials

- 1) Information Security Measures
<http://www.ipa.go.jp/security/benchmark/>
- 2) Information Security Governance (Ministry of Economy, Trade and Industry)
http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html
- 3) Ministry of Internal Affairs and Communications, Bureau of Statistics 2006 Business Institution/Statistical Research
<http://www.stat.go.jp/data/jigyoku/2006/>
- 4) Japan Standard Industry Classification (Revised in March 2002)
<http://www.stat.go.jp/index/seido/sangyo/>