

Information Security Measures Diagnosis

This is a diagnosis result of the Information Security Benchmark service hosted by Information-technology Promotion Agency, Japan (IPA). The diagnosis results and recommended actions for your company are shown based on your responses to the questions.

Date of Diagnosis : 2021/04/05 00:15:04
 Name of Company :
 Scope of Diagnosis :
 User Number :

Information Security Management Benchmark Ver.5.0

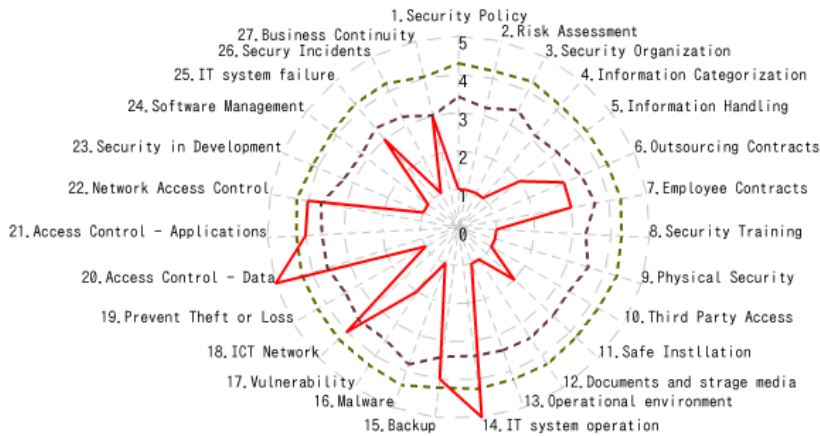
Results

Your company belongs to the layer (Layer for which critical security level is required (Group I)) the required security level of which is justified as such. Among Group I, the score of your corporate is positioned in top 91~100. (Among all the Groups, it is positioned in top 81~90.)

In comparison with the preferred level of measures in this Group, the current level of your corporate is as follows.

"Preferred Level" is the one that you company is suggested to target, which is the average of top one third of each Group. (If your company does not reach the total average, the total average is suggested to be set as a tentative target to be reached at the earliest.)

Your company's status as opposed to Preferred Level in the Group



Your Company Score	
Total Score	58/135Point
Average Score of Question	2.2/5Point

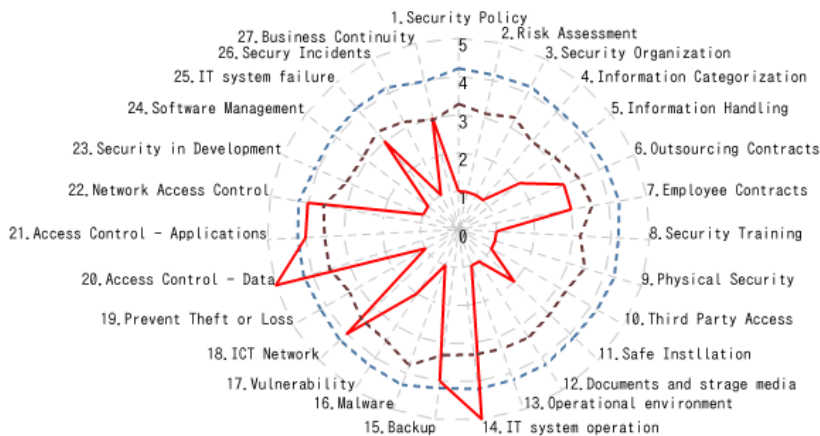
Preferred Score Level in Group I	
Total Score	115/135Point
Average Score of Question	4.3/5Point

Average Score in Group I	
Total Score	92/135Point
Average Score of Question(Group I)	3.5/5Point
= 3377)	

Legend
— Your Company Score
- - - Preferred Score Level
- - - Average

Your company falls into the category of 300 Employees or Less based on your responses to the questions in "Part 2 (1) Number of Employees" Your position is as follows in comparison with the Corporate Group 300 Employees or Less.

Radar Chart for the Corporate of 300 Employees or Less



Your Company Score	
Total Score	58/135Point
Average Score of Question	2.2/5Point

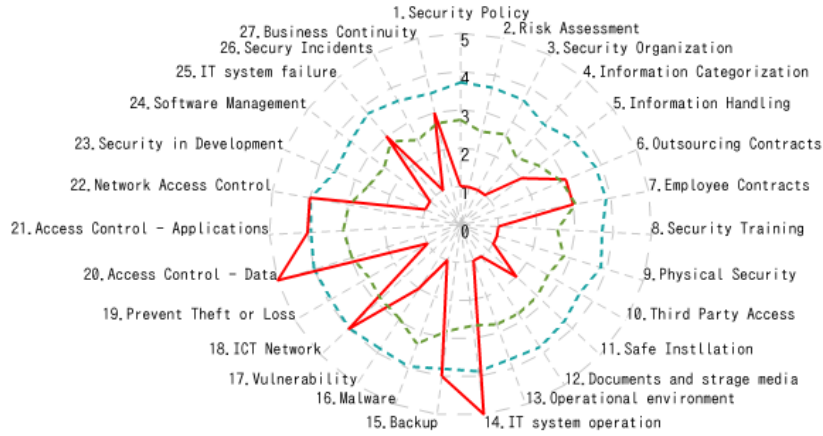
Preferred Score Level in the Company Scale	
Total Score	113/135Point
Average Score of Question	4.2/5Point

Average Score Level in the Company Scale	
Total Score	90/135Point
Average Score of Question	3.4/5Point
(Number of Samples(300 Employees or Less) = 1764)	

Legend
— Your Company Score
- - - Preferred Score Level
- - - Average

On top, your company's position is as follows in comparison with your industry average.

Your company's status as opposed to Your Industry Average



Your Company Score

Total Score 58/135Point
Average Score of Question 2.2/5点

Preferred Score Level in the Same Industry

Total Score 102/135Point
Average Score of Question 3.8/5Point

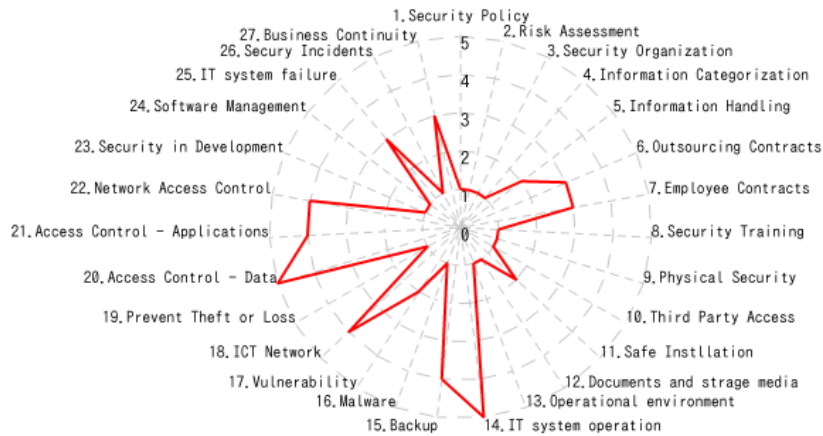
Average Score in the Same Industry

Total Score 75/135Point
Average Score of Question 2.8/5Point

— Your Company Score
- - Preferred Score Level
- - Average in Same Industry

The diagnosis result of this time is as follows as opposed to that of last time.

Comparison of diagnosis results between this time and last



Score of This Time

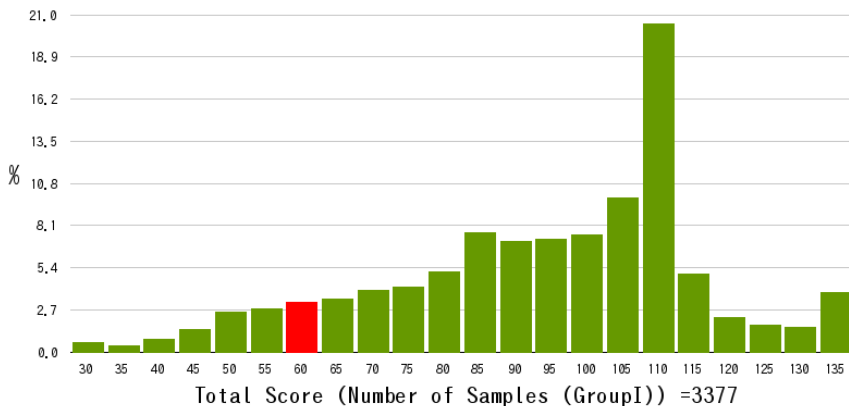
Total Score 58/135Point
Average Score of Question 2.2/5Point

— Score of This Time

Your company deviation value along with total score distribution status in Group I is as follows.

Total Score Distribution Status in Group I

Total Score of Your Corporate 58Point/135Point



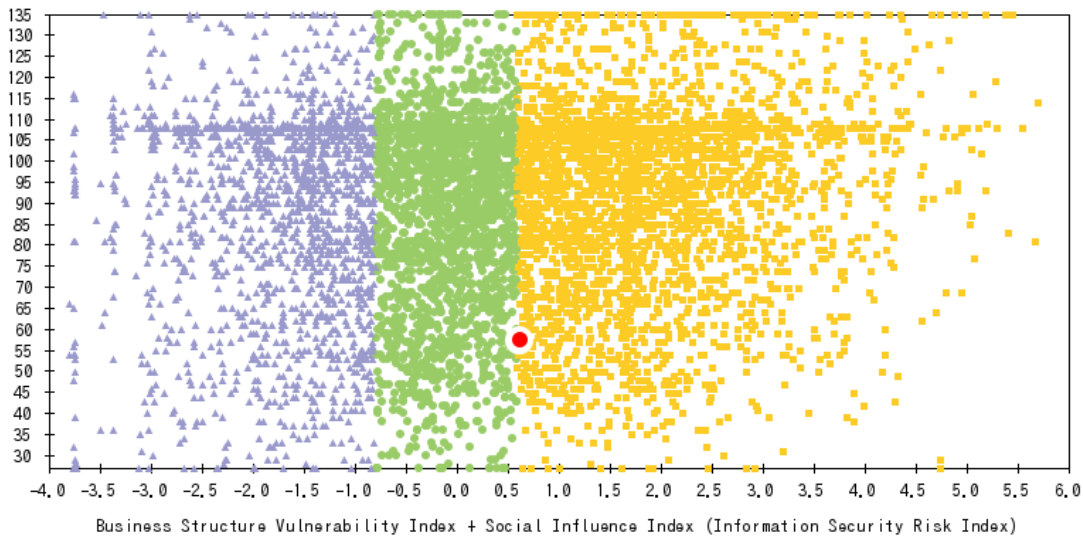
Deviation Value of Your Company 34.9

Deviation Value of Total Score

Result Details in Group Classification

Your company belongs to the layer (Layer for which critical security level is required (Group I)) the required security level of which is justified as such. Your company total score and your corporate position are shown in the graph format as per the "Information Security Risk Index" which is the addition of "Business Structure Vulnerability Index" and "Social Influence Index" calculated based on your responses.

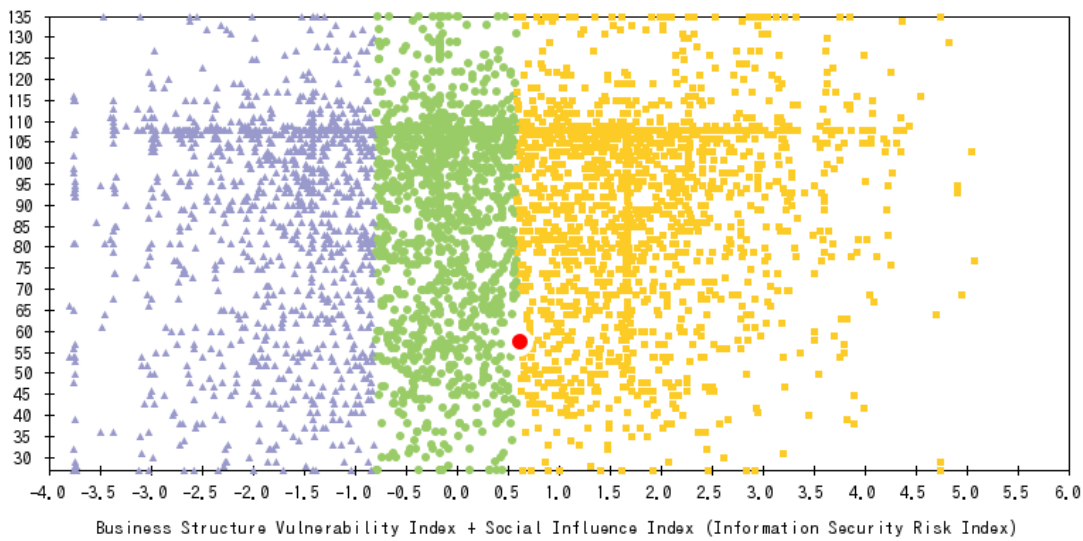
Scatter Diagram of Total Score (Your Company Position in Distribution of All Corporates)



▲ Layer for which information security is not an immediate issue (Group III)
 ● Layer for which medium security level is preferred (Group II)
 ■ Layer for which critical security level is required (Group I)
 ● Your Company Position (This Time)

(If Information Security Risk Index value exceeds 6, the result is not shown in the scatter diagram.)
 (In the case you perform the diagnosis multiple times, your company positions may be overlapped if the Total Scores and Information Security Risk Indices are close respectively.)
 (Number of Samples = 7227)

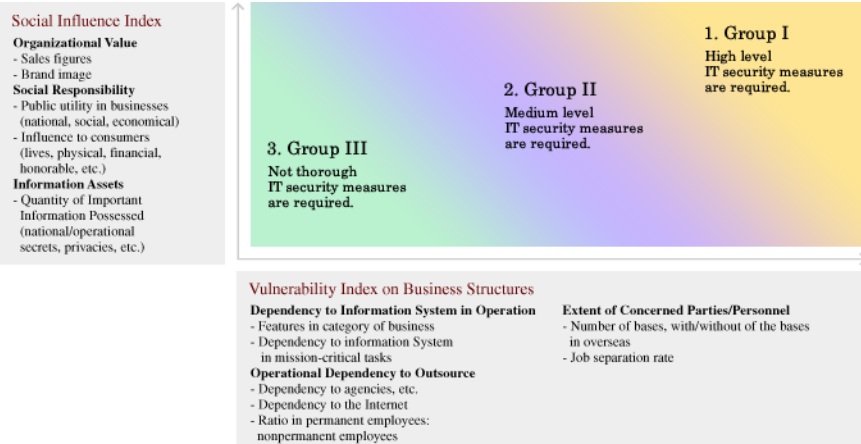
Scatter Diagram of Company of 300 Employees or Less



▲ Layer for which information security is not an immediate issue (Group III)
 ● Layer for which medium security level is preferred (Group II)
 ■ Layer for which critical security level is required (Group I)
 ● Your Company Position (This Time)

(If Information Security Risk Index value exceeds 6, the result is not shown in the scatter diagram.)
 (In the case you perform the diagnosis multiple times, your company positions may be overlapped if the Total Scores and Information Security Risk Indices are close respectively.)
 (Number of Samples(300 Employees or Less) = 4190)

Category by Required Information Security Level



Attachment

Date of Diagnosis : 2021/04/05 00:15:04 +0900

Name of Company :

Check Sheet of Information Security Measures Benchmark

		Score
Q1-(1)	Does your company have any policies or rules for information security and implement them?	1Point
Q1-(2)	Does your company evaluate dangers and vulnerabilities regarding the security of vital information assets within your organization in deciding security rules and countermeasures?	1Point
Q1-(3)	Does your company have an organizational framework which includes the management to promote information security and compliance with law and rules?	1Point
Q1-(4)	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?	1Point
Q1-(5)	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?	2Point
Q1-(6)	Are information security requirements included in your company's written contract, which is exchanged when you outsource your business operation or information system management?	3Point
Q1-(7)	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?	3Point
Q1-(8)	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?	1Point
Q2-(1)	Does your company implement security countermeasures required for the buildings and sites where you want to improve security?	1Point
Q2-(2)	Does your company formulate and enforce any security-related rules for the people moving in and out from your company, including clients, vendors, common carriers, cleaners etc?	1Point
Q2-(3)	Are the important information equipment and wires/cables correctly placed and set up in safety so they can be protected against natural and man-made disasters?	2Point
Q2-(4)	Does your company handle important documents, mobile PCs, and removable storage media in an appropriate manner?	1Point
Q3-(1)	Does your company protect information systems and data used in the actual operational environment in an appropriate manner?	1Point
Q3-(2)	Does your company implement security countermeasures required for information system operation?	5Point
Q3-(3)	Does your company have documented procedures for the backup of vital business data and related systems, and implemented them?	4Point
Q3-(4)	Does your company take countermeasures against malware (such as computer viruses, Worms, Trojan horses, Bots, Spyware etc.)	1Point
Q3-(5)	Does your company take countermeasures to mitigate vulnerabilities of the information systems used in your company?	2Point
Q3-(6)	Does your company take appropriate protective measures (such as encryption) for data being transferred across communication networks and data stored on a public server?	4Point
Q3-(7)	Does your company implement appropriate security countermeasures to protect storage media such as mobile PCs, USB memories, floppy disks etc in case of their loss, theft and so on?	1Point
Q4-(1)	Does your company implement necessary measures to restrict access to information (data) and information systems, including appropriate management of user IDs, adequate user identification and authentication etc?	5Point
Q4-(2)	Does your company implement appropriate access controls over information (data), information systems, and business applications, including granting users adequate access rights for such resources?	4Point
Q4-(3)	Does your company implement appropriate access controls over the network?	4Point
Q4-(4)	Does your company define security requirements for business application development and satisfy them in the design and implementation phases?	1Point
Q4-(5)	Does your company perform security controls over the selection and purchase of software products and/or the development and maintenance of systems?	1Point
Q5-(1)	Does your company take appropriate measures for the case of information system failures?	3Point
Q5-(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?	1Point
Q5-(3)	Does your company have a company-wide framework for BCM(Business Continuity Management)for the case of system down?	3Point
Statistics	Total Score of All 27 Questions (out of 135 Full Score)	58Point
Average	Total Score Divided by Number of Questions	2.2Point