Information Security Management System Diagnosis Service

We design feasible roadmap of security measurement by diagnosing process, system, technical measures, and formulating the measurement from the result of the diagnosis.

Companies operate in an environment that is increasingly digitized. This poses information security issues. Information leaks escalating into a major business-threatening crises are no longer a rare occurrence. Managing information assets properly to establish and maintain information management systems is essential for business continuity.

Information security risks facing companies

The actions a company takes during an information security incident have the potential to damage the company's credibility significantly. The wrong moves could make recovery from the crisis enormously costly. Such costs alone could lead to a business-threatening crisis. This is why managers view information security measures as part of their key strategic efforts to safeguard company assets.

Prevalence of new digital Technology	Prevalence of smart devices and accelerating commercialization of new technologies like IoT, AI and FinTech are bringing security issues to the fore.
Sophistication of cyber attacks	The damage caused by targeted email attacks, ransomware and other cyber attacks is spreading. The attacks cause leakage of personal data and can even close down factories.
Clarification of legal corporate responsibility	Data-related legal and regulatory reforms are making security measures for handling personal data essential.

The Value ABeam Consulting offers

In order to formulate appropriate risk-mitigation measures, it is important to assess possible risks from three critical perspectives: process (operations), personnel/organization (operational framework), and technology. ABeam Consulting's information security management system diagnosis service provides appropriate diagnosis which suitable for clients needs; we identify security risks, and diagnose the preparedness of company's information security management system against risks.

Corporate information security risks

Information security management system diagnosis service

Our approach

Information security measures are implemented in two phases: planning phase and implementation phase. Our information security management system diagnosis service focus on the planning phase. We visualize the company's current status of information securities, plan the measures against security issues, and draw up implementation plan.

Planning Phase			Implementation Phase
Step1: Survey of current status	**Step2: Consideration of measures**	**Step3: Plan development**	**Step4: Implementation**
· Visualize the current information security management system (management process, system, implementation status)	· Consider direction of information security management system and measurements	· Develop plans to enhance information security management systems	· Implement specific information security measures based on the plans developed

Scope of this service

What makes our service special

ABeam Consulting assists clients in realizing essential security measures, by industry-based, flexible, and well-balanced methods. Our solution complies with ISO27001, the standards of information security management system.

Step1：Survey of current status

We conduct a survey of your current status with the results of security diagnosis survey forms, and interview with your management. Then we quantify and visualize the maturity of your security measures. Checking the result, we sort them out to extract the points of issues, sort them out, and identify the real causes of risks and their degrees of importance.
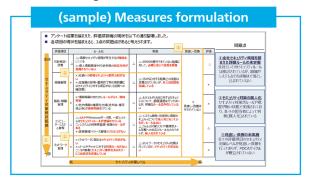
- Responses to security diagnosis survey forms*
- Hearing from management/ People in charge
- Investigating internal documents
- Researching IT environment

→ Sort out and visualize the survey results

→ Extract problems and identify risks, rank by importance

Example of security diagnosis survey results

*We use our security diagnosis tools in compliance with the ISO27001 standard of ISMS.

Step2：Consideration of measures

We support considering security measures, taking account of combinations of security risks on which clients put importance and weaknesses based on the result of security diagnosis. Then we assist making decision, which measures to implement, from the dimension of importance, effectiveness and costs.

Formulation of security measures

From ordered out and visualized status of security measurements, we surface the issues and categorize the direction of policies. Then, we assist extracting several measures from the result.

(sample) Measures formulation

Prepare plans for security measures

From the aspect of importance, effectiveness and costs, we support considering which measures to implement or not.
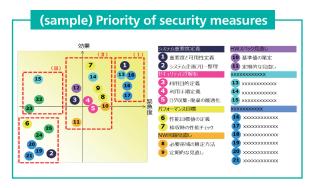
(sample) Security measures plans

Step3：Plan Development

We support prioritize on security measures and formulate feasible plan, considering task volume, schedule, and viability. We write up the result in security measurement plan.

Defining the priority of security measures

Prioritize security measures. Assess the volume and viability of tasks, as well as scheduling concerns.

(sample) Priority of security measures

A roadmap for security measures

Schedule defined priorities to create a roadmap for viable security measures.

(sample) Security measures roadmap

ABeam Consulting Ltd.   www.abeam.com