A Study on Information Security Management System Model for Small and Medium Enterprises

Wan-Soo Lee, Sang-Soo Jang
Enterprise Information Security Management Team
Korea Internet & Security Agency (KISA)
78, Garak-Dong, Songpa-Gu, Seoul
KOREA
complete2@kisa.or.kr, ssjang@kisa.or.kr http://www.kisa.or.kr

Abstract: To address current difficulties of Small and Medium Enterprises (SMEs) that are reluctant to invest in information security due to cost, this paper intends to provide an information security management system that will allow SMEs to adopt efficient security measures. Information protection across the enterprise to organize activities such as ISO 27001 Safety Management System through long-term, sustainable security infrastructure to build, but the current information management system that protects personnel and budgets of small businesses under the circumstances when the use is difficult. Therefore, in this paper, the operating environment of small business information and analysis, and major threats, physical, human and technical threats from a variety of businesses to help strengthen the security level of information security management system was the establishment of research.

Key-Words: Information Security, ISMS, SMEs, Security Level, ISO27001

1 Introduction

Small and Medium Enterprises (SMEs) recognize the need for information security. But, because of the lack of resources and capabilities for building information security management system (ISMS) was vulnerable in part that from the information security policy, security systems, ranging from information security incident response.

Claiming 99% of Korean businesses, 50% of industry production, and 75% of employment SMEs are an important factories in national economy and are investing massively in information every year to enhance business competitiveness. Such efforts resulted in enhancements in productivity, job efficiency, and convenience [1].

But, Korea Small and Medium Business Administration published the "2008 Small Business Informatization Level Evaluation Report," according to the level of information is constantly increasing (76.3% compared to enterprise-level) the need for privacy also high (87.6%) recognized, but the rate for security system (25.5%), information protection policy formulation and implementation (2.1%), shown at the level of privacy is very low state [2]. For the same reason above, the majority of SMEs recognize the need for privacy and data protection measures, but at least the reasons are not lack of knowledge, lack of information, financial problems, due to lack of professional staff were surveyed.

To management of enterprise's security existing information security check service (ISCS) [3], ISO27001, ISMS [4] and other relevant information security policies, but SMEs does not include an obligation to target the lack of ability to perform security management, information protection and Rectangular zone is located. Also, ISO27001 and ISMS policies of the current are the vast scope and the effect on SMEs have difficulty doing.

The security activities of most SMEs are one-time activities or such as homepage and the server that has been focusing on technical area. So, establishing enterprise-wide information security management system is insufficient. Because, this brings uneven security level in a different fields, from the various security threats to threats of enterprise's security level is a factor.

Accordingly, SMEs, to enhance the information protection capabilities necessary to evaluate the status of its own security by establishing a process that can perform security management plan is needed.

Therefore, in order to enhance the information security level of SMEs in Korea, this paper will offer the information security management model and implementation method that allows SMEs to execute information security measures cost-effectively according to their business environment. .

2 Problems in Information security of SMEs

This section describes current issues in the information security difficulties of SMEs in Korea.

There is a lack of the perception of information security for SMEs and necessary policy. SMEs grant

priority specific items of information security management system which are basic elements: SMEs get higher score for identification and assessment of information assets (document, facility etc.), access control of PC and document (printed material), and countermeasure for security incidents and error (maintenance of work continuity), management when compared with large enterprises.

The preliminary researches are focused on technical approach to cope with external cyber attacks, and there exists a lack of researches regarding managerial and environmental elements associated with the information security. In case of SMEs, which operate under limited resources and capabilities, the characteristic of the information security has to be perceived in a different way and countermeasures should be differentiated from those for large enterprises.

The general problems in information security of SMEs described below:

- Employers and employees in large companies compared to the lack of security awareness
- For the protection of information assets, lack of managerial control
- The vulnerability inherent in the enterprise and the absence of risk analysis
- Lack of policies for the protection level and level set for information assets
- The absence of recovery policy in emergency
- Response inferior refer to insider crime and the exterior intrusion

A temporary construction of an information security management system needs a constant investment whenever new vulnerabilities are discovered. Therefore to achieve objectives of information security investment efficiently and effectively, it is critical to build ISMS which retains consistency in terms of managerial level.

In accordance with SMEs and characteristics of SMEs' informatization, a development of ISMS which is differentiated from security system for large enterprises possessing enough resources is essential.

3 Information security management system (ISMS) for SMEs

3.1 Information security

It is information security that ensures on going confidentiality, integrity and availability of an information [5].

- ***Confidentiality***: the protection of information, in any form, while in storage, processing or transport, from being available to any organization or person that is not authorized by its owner to have it [6].
- ***Integrity***: Ensuring that information is accurate and complete in storage and transport; that it is correctly processed and that it has not been modified in any unauthorized way [6].
- ***Availability***: Ensuring that information is available to those who are authorized to have it, when and where they should have it [6].

3.2 Information security management system

Information security management system (ISMS) means continuously managing and operating system by documented and systematic establishment of the procedures and process to achieve confidentiality, integrity and availability of the organization's information assets that do preserve.

When building and operating the ISMS overall (administrative / technical / physical) establishment of protective measures. Also, they can develop cost-effective information protection measures that security awareness and strengthen capacity of staff and emergency security incident response skills and so on.

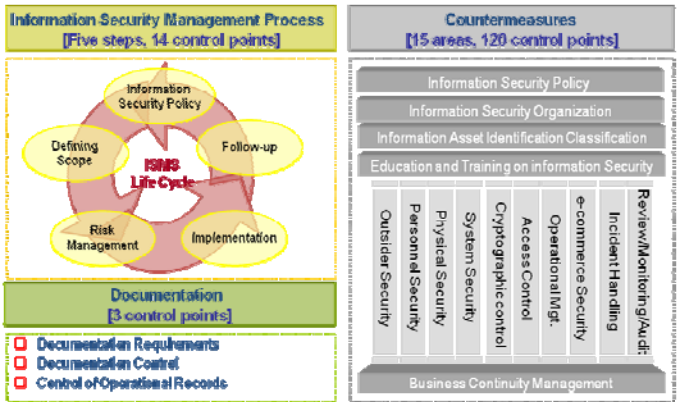

Fig. 1 Overview of ISMS

Figure 1 shows the ISMS certification criteria. For ISMS life cycle, there are 5 major steps; setting up security policy, defining scope, risk management, implementation, and follow-up. It needs 14 control points.

For documentation, there are 3 control points; documentation requirements, documentation control, control of operational records. Also, for countermeasures, there are 15 areas; information security policy, information security organization, information asset identification, education and training on information security, business continuity management. They have 120 control points [4].

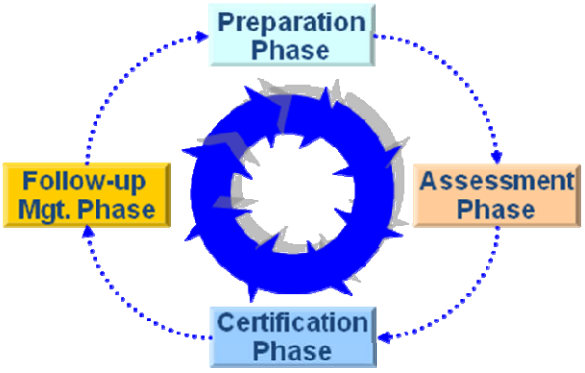

Fig. 2 Features of ISMS Audit Procedure

And figure 2 shows ISMS certification assessment procedures. There are 4 phases for assessment procedure; preparation phase, assessment phase, certification phase, and follow-up management phase. ISMS have a few features in each phase of assessment procedures.

Pre-assessment phase check the situation of preparation and notice of requirements needed before assessment. And penetration test conduct a penetration test of the network and system. The case of complementary measures & confirmation that a leader of audit team give applicant enforcement notice for complementary measures based on documentation and technical assessment results on the last day of audit (period: 30 days). Finally, certification committee review and discuss the audit results at the certification committee meeting.

Construction and operational benefits of ISMS can be implemented by cost-effective information protection measures based on risk management that privacy of internal staff recognition and our ability to protect information, clarifying responsibilities, such as emergency security incident response skills and so on. But, these criteria are inadequate for SMEs that asset-size is small and have an insufficient staff.

3.3 Information security management system Model for SMEs

Generally in case of SMEs suffering from a lack of resources, the maintenance cost of information occupies larger portion than acquisition cost of information. Also, they tend to rely on external environments for acquisition of information and it is difficult for them to do information security with sufficient experts. Therefore, ISMS for SMEs should feature simple processes and system, and should be designed with convenience for operation, management, and maintenance.

The criterion for SMEs' ISMS follows:

1. Control/integrate the documentation and protection measures considering the fact that protected information assets is less and a lack of manpower.
2. Basic procedure to protect information that is commonly applied, and detailed measures to meet small business makes a reality.
3. In the three regions of information security (Integrity, Availability, Confidentiality), takes priority precedence over confidentiality and availability, shall consist of a minimum level of integrity.

Through these processes, ISMS for SMEs in order to establish the following four steps will go through the process.

- Setting up security policy
- Risk management
- Implementation
- Follow-up

Setting up security policy stage determine the scope of the company's policies and scope. In addition, each department responsible for the company's business and to specify responsibilities regarding privacy. In risk management stage, investigate the assets within the organization whether any risk factors, the scale to assess whether the degree it can be reduced to reasonable level of information protection measures and plan to be selected. In the implementation phase, changing procedures and staff training is done according to the information security countermeaseres that created as a result of risk management steps. Finally, in the follow-up phase, operate the ISMS whether it is being kept constant and regular monitoring to check. Make sure it is a violation and if the violation is discovered, depending on the cause and take improvement measures.

Also, the overall control items were reduced from 120 to 67 items. However, the characteristics of small organizations to save the item is added. Because SMEs are comes primarily from other companies that contract work role in outsourcing relationship, in outsider security control, contract security management and dispatch personnel to secure management control purposes, each

controlling two personalized items for a total of four additional items were added

Table 1 shows comparison of control item's number between ISO27001 and ISMS for SMEs.

Table 1. Comparison between ISO27001 and ISMS for SMEs

Section	Area of Control	ISO 27001	Korea-ISMS	
			Before	After
Information Security Management Process		-	5	4
Documentation		-	3	3
Countermeasures	Security Policy	2	5	2
	Organizing Information Security	11	4	2
	Outsider Security	-	4	8
	Information Asset Classification	9	4	3
	Education and Training on Information Security		4	3
	Human Resource Security		5	3
	Physical Security	13	12	5
	System Development Security	32	13	7
	Cryptographic Control		3	2
	Access Control	25	14	8
	Operational Management	16	22	10
	e-commerce Security		5	4
	Security Incident Handling	5	7	3
	Compliance/ Review, Monitoring & Audit	10	11	5
	Business Continuity Management	5	7	2

As mentioned above table, deleted any unnecessary or excessive control items and but an important control objectives, such as document management for small organizations to implement tough measures required to control the information provided about the supplement in a way that the modifications were made.

4 Conclusion

To address current difficulties of SMEs that are reluctant to invest in information security due to cost and security awareness, this paper provided ISMS model for SMEs that help protect their information assets.

The proposed ISMS model for SMEs is significant in that it allows SMEs to take necessary security measures and to realize what actions must be taken for additional information security.

It is also significant in that this is a new approach presenting an information security framework for SMEs that reflect the environment, investment costs and voluntary participation of SMEs. Still, further studies are required in order to define a more extensive and practical method for a variety of SMEs' industries.

References:

[1] Ho-Seong Kim, Mi-Hyun Ahn, Gang-Shin Lee, Jae-il Lee, The information Security Guideline for SMEs in KOREA, *The 2006 International Conference on Security & Management (SAM '06)*, 2006, pp. 48-54.

[2] *2008 Small Business Informatization Level Evaluation Report*, Korea Small and Medium Business Administration, 2008

[3] Information Security Check Service (ISCS), http://www.kisa.or.kr/kisa/iscs/jsp/iscs.jsp

[4] Information Security Management System (ISMS), http://www.kisa.or.kr/kisa/isms/jsp/isms.jsp

[5] Ms. Upasna Saluja, RISK MANAGEMENT: Small and medium enterprises, *MoMM2006 & iiWAS2006 Workshops Proceedings*, 2006, pp. 497-504.

[6] ISO/IEC 27002:2005, Code of practice for an information security management system, 2005