Available online at www.sciencedirect.com
ScienceDirect
The Journal of Systems and Software 80 (2007) 1631–1638
The Journal of Systems and Software
www.elsevier.com/locate/jss

Common defects in information security management system of Korean companies

Sungho Kwon [a,*], Sangsoo Jang [a], Jaeill Lee [a], Sangkyun Kim [b]

[a] IT Infrastructure Protection Division, Korea Information Security Agent (KISA), 78 Garakdong, Seoul, Republic of Korea
[b] Department of Industrial Engineering, Kangwon National University, Chunchon, Republic of Korea

Available online 27 January 2007

Abstract

To reduce the possible trials and errors while promoting the establishment and certification of the information security management system (ISMS) by enterprises is the purpose of this paper. To satisfy this purpose, this study presents the defects by item found during the certification process of the ISMS of a number of enterprises by government certification agency in Korea. As a result, by analyzing the derived defects, this paper has outlined the issues to be attended to among enterprises at each stage of the establishment of the ISMS. Furthermore, this study presents a reference model for conducting a self assessment, so that companies may be able to self verify the completeness of their establishment of the ISMS. The case study is also provided to prove the practical value of this study.

Keywords: Information security management system; Reference model; Self assessment

1. Introduction

Due to the rapid development of the Internet, information leakage and financial loss among enterprises have been increasing as a result of information dysfunctions. With the looming necessity for protecting important information from information dysfunction, and for managing information security systematically, international interest in information security management has increased, and systematic efforts in terms of information security management are expanding. In Korea, to keep up with this trend, a study on the certification system of the ISMS has been being conducted since 2000, and detailed assessment standards and a guide based on the Act on Promotion of Information and Communication Network Utilization and information Protection was prepared under Article 47 in 2001 (MIC, 2004a,b,c). The certification system of the ISMS was addressed as of May, 2005. To date, in order to facilitate the certification system, a number of initiatives have been developed, including those pertaining to technical advice, guideline distribution, prior advice for certification assessment, and cultivation and education of certification auditors.

The certification system of the ISMS represents one which established and documents procedures and process, and is continuously managed and operated to realize the purpose of information security, confidentiality, integrity, and availability of information assets. The system is on under which a third-party certification authority entitled Korea Information Security Agent objectively and independently assesses the organically integrated system of numerous measures for information security as implemented by the information security management process, including the establishment of policy and organization, risk management, measure implementation and consequence management and so on for an information security regime suitable for each body, thereafter certifying the eligibility for the standard (KAB, 2005a,b).

* Corresponding author.
E-mail addresses: ekdsk@nate.com (S. Kwon), ssjang@kisa.or.kr (S. Jang), jilee@kisa.or.kr (J. Lee), saviour@yonsei.ac.kr (S. Kim).

0164-1212/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2007.01.015

This study summarizes the legal basis for the certification system of the ISMS and its certification scheme, in order to develop an understanding of the basic concepts of the certification system being enforced in Korea. In addition, the analysis on defects found in obtaining certification has been conducted on the basis of the bodies to have obtained the certification of the information security management system. Through this, the study presents a reference model for conducting a self check, aimed at helping enterprises self verify the completeness levels of their establishment of the information security management system. Finally, the effectiveness of this study has been identified through the case study of enterprises wherein the reference model for the self check proposed in this study was applied.

2. Certification method

2.1. Certification index

In Korea, the study on the certification index of the ISMS has been being conducted since 2000, and is based on Article 47 of the Act on Promotion of Information and Communication Network Utilization and Information Protection with the standards for certification assessment announced by the Ministry of Information and Telecom-

Table 1
Index for certification assessment

Category	Index	Assessment standards
Management procedures	Establishment of an information protection policy	Establishment of an information protection policy, Establishment of organization and responsibility
	Establishment of the scope of the information protection management system	Establishment of the scope of the information protection management system, Identification of information assets
	Risk management	Establishment of a risk management strategy and plan, risk analysis, risk assessment, selection of information protection countermeasures, establishment of an information protection plan
	Realizations	Effective realization of information protection countermeasures, education and training of information protection
	After the fact management	Re-examination of the information protection management system, monitoring and improvement of the information protection management system, internal audit
Documentation		Document requisite Control of documents Control of recording documents
Control of information protection management	Information protection policy	Approval and announcement of the policy, policy system, policy maintenance management
	Information protection organization	System of organization, responsibility and role
	Outsider security	Security management of contract and service level agreement, outsider security implementation management
	Classification of information assets	Inspection and allocation of responsibility of information assets, classification and handling of information assets
	Education and training of information protection	Establishment of an education and training program, implementation and assessment
	Personnel security	Allocation and regulation of responsibility, qualification examination and management of staff in charge of major jobs, confidentiality
	Physical security	Physical security countermeasures, data center security, equipment protection, office protection
	System development securities	Analysis and design of security management, realization and implementation of security management, change management
	Cryptography control	Cryptography policy, cryptography use, key management
	Access control	Access control policy, user access management, access control region
	Operation management	Operating procedure and responsibility, system operation, network operation, media and document management, malicious software control, mobile computing and remote works
	Electronic transaction security	Exchange agreement, electronic transaction security management, e-mail, open server security management, user public notice item
	Security accident management	Response plan and system, response and restoration, after the fact management
	Examination, monitoring and auditing	Compliance examination of legal requirement items, compliance examination of information protection policies, monitoring, security audit
	Job continuity management	Establishment of job continuity management system, establishment and realization of a job continuity plan, testing and maintenance management of the job continuity plan