Journal of Engineering and Applied Sciences 13 (Special Issue 2): 3042-3047, 2018
ISSN: 1816-949X
© Medwell Journals, 2018

Design of Information System Audit Model for Information Security in Smart Work Environment

Hee-Wan Kim
Department of Computer-Mechatronics Engineering, Shamyook University, 01795 Seoul, Korea

Abstract: Information system audit has contributed greatly to the construction and operation of a safe and reliable information system. It is necessary to establish a proper information system audit model for the establishment and operation of smart work environment and to carry out the audit, so that, the informatization project can be successfully performed. Information security must be implemented and managed in a smart work environment that guarantees continuity of research even in a physical space that cannot be controlled by enterprises and organizations. Therefore, an information security audit model that can be used to build a secure smart work environment is needed. However, in the existing information system audit, the information security implementation is not constituted as a separate control area and there is no information security control framework specialized in the smart work environment. In this study, it is proposed the checklists and an information system audit model for technical information security audit suitable by using information security management system in smart work environment. In order to verify whether the proposed information security checklists meet the purpose of smart work information security audit, it is verified the suitability through questionnaires of the IT industry practitioners.

Key words: Information system audit, audit model, smart work, ISMS, checklists, environment

INTRODUCTION

Information systems are more than just simply computers. They have several components that make up the business solution. An auditor can only give assurance about an information system if the components are evaluated and secured by the organization (Lovaas and Wagner, 2012). Information system audit was introduced in Korea in 1987 to enable efficient management of information technology resources by optimally building and operating information systems. Information system audit is being carried out to improve the efficiency of the information system and to ensure safety by comprehensively checking the issues related to the construction and operation of the information system from a third party perspective and improving the problems. Also, based on the Industrial revolution, the social paradigm from the previous agrarian society to the modern society and the modern information society is continuously changing. In the modern case, it is imminent to enter into an aging society and focuses on individual productivity improvement as a solution to this. In order to improve productivity, smart work is introduced by adopting recently developed information technology. In Korea, smart work is rapidly activating based on ICT infrastructure. In addition, BYOD (Bring Your Own Device) (Disterer and Kleiner, 2013; Miller *et al*., 2012) which utilizes your own devices such as smartphones and tablet PCs is spreading. The spread of nationwide wireless network services and the development of cloud computing technologies such as Service Base Cloud (SBC) provides an environment that can activate the smart work. The government and the private sector are pursuing smart work in various ways. In promoting smart work, many companies have improved efficiency of research productivity and cost reduction. However, there are a variety of security threats and companies try to solve security threats to information assets and services. Information system audit has been carried out for 27 years in Korea, contributing to the safety of information system construction and operation. It is necessary to establish a proper information system audit model for the establishment and operation of smart work environment and to carry out the supervision, so that, the informatization project can be successfully performed. However, the existing information system audit does not constitute the implementation of information security as a separate control area. In this study, it is proposed a security audit model using the information protection management system in smart work environment by presenting the countermeasures against risks and checking items by using ISMS (Information Security Management System) (Alavi *et al*., 2014).

SMART WORK INFORMATION SECURITY AND SECURITY AUDIT

Smart work: The development of mobile communication technology and the proliferation of smart devices have made a great change in the work environment. Using smart phones and tablets with built-in high-performance computing devices and storage devices, there is no limit to the work space that was previously limited to office work, remote work places and so on enabling smart work that efficiently handles work anywhere and anytime. Smart work means a future-oriented work environment that allows users to engage in work conveniently and efficiently anytime, anywhere in various places and on the mobile environment by moving away from the conventional concept of an office as a designated work space. As the interest and use of smart work is increasing, it is necessary to clarify the conceptual definition of smart work through characteristics of smart work. Smart work is a collective term for advanced work methods that can be used anytime and anywhere regardless of time and place by utilizing IT. It differs from conventional telework in that it does not just mean flexibility in the workplace but also includes the way of working and the advancement of the work culture (Koh *et al*., 2014). Smart work is not done simply by changing the office environment by introducing a device such as a smart phone. Smart work is not just about teleworking, it is about including remote collaboration. As a form of collaboration that has emerged along with the development of information and communication, researchers can perform smart work anytime and anywhere without any time and space constraints, thereby increasing productivity. It is possible to speed up work process and improve productivity and enables rapid decision making and problem solving through the use of real-time collective intelligence through remote collaboration. In addition, employment opportunities for the vulnerable groups are expected to expand, resulting in a harmony of work and life. Companies are increasingly trying to improve their work efficiency by using smart devices. There is an increasing number of companies and public institutions and organizations introducing smart offices to provide corporate environment access to corporate intranets anytime and anywhere. Since, the main tasks that PC-based processes are extended to mobile devices such as smart phones, security threats that can occur on existing PC-based devices can be reproduced on smartphones and the risk of loss due to light mobility is relatively large. Although, smart work are not limited by space, security threats of smart devices are directly related to security threats of smart work.

Information security management system: Information security management system is necessary prerequisite for business continuity in organizations. To fulfill ISMS goals and objectives, a solid security framework requires ensuring confidentiality, integrity, availability, authenticity and auditability of the critical information assets (Alavi *et al*., 2014). It is a comprehensive system for systematically establishing and managing information protection management procedures and processes in order to protect the important information assets of the organization and establishes and operates to secure the safety and information reliability of the information communication network as a legal definition means a comprehensive management system that includes all administrative, technical and physical safeguards. As part of the overall management system or management system for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security based on business risk approach, all information including documented information, is the subject of security and evaluates information about such risks to achieve the confidentiality, integrity, availability and compliance of information assets and establishes and operates measures to prevent such risks. The government has unified into the Information Security Management System (ISMS) certification system to improve the information protection environment of vulnerable companies. In addition, they has established an Information Security Management rating System for ISMS certified companies, preliminary inspection of information security and appointment of CISO as the chief information security officer (Anonymous, 2011). It is imperative for organizations to use an Information Security Management System (ISMS) to effectively manage their information assets. ISMS consist of sets of policies by an organization to define, develop, construct and maintain security of their hardware and software resources (Susanto *et al*., 2011).

IS security: Information is “knowledge that interprets and summarizes data collected through observation or measurement to help the actual problem.” According to Article 2 of the Informatization Promotion Basic Law, “information or any kind of data or knowledge expressed by a natural person or a corporation in the form of codes, letters, voices, sound and images processed by optical or electronic methods for a specific purpose” is defined as information. In other words, information refers to the processing of the information in a form that is organized and expressed, so that, it is meaningful to the user of the information. In this context, in order to define and identify the information, we need to protect, we need to know

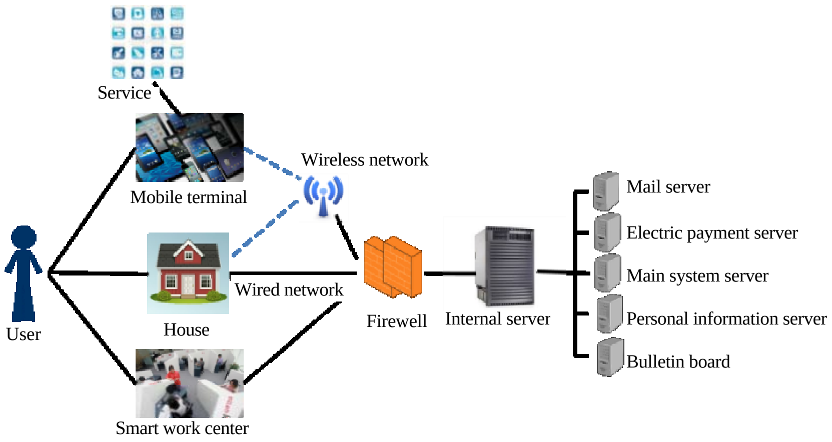

Fig. 1: Security threats in smart work environment

exactly what it means to the person or organization that uses it. High-priority information has the same importance as other assets. It is necessary to accurately assess the value of the information to be protected to calculate the amount of damage to the organization and to establish information protection measures to prevent it. The cost of implementing these information protection measures should be estimated and the most reasonable method should be established at an effective cost. The IS security management in organizations is a difficult task, especially, avoiding the threat from insiders from within the organization. Employee's illegal and deviant acts represent a key threat to organizations. Information systems in an organizational context are best expressed as a combination of technology, people and management. Among those three factors, people play a key role in the process of IS security governance in organizations from both research and practice perspectives as people could be the weakest link in IS security (Cheng *et al*., 2013).

Security threats and vulnerabilities by smart work: Based on smart work information protection requirements, security threats and vulnerabilities were derived from smart work introduction and operation. The smart work classification is classified into the location where the work is performed and the difference between the terminal and the service used. However, it is the same in that it actually uses information in the corporate network or that it uses a wired or wireless network. Therefore, from a structural point of view, smart work can be divided into a common part, a mobile office, a telecommuting and a smart work center. As a result, as shown in the following Fig. 1, a complete common part such as a network company. For each type, the countermeasures can be divided into different common parts and specific parts for smart work types.

Table 1: Security threats and vulnerabilities by smart work structure

Categories	Contents
Common threats and vulnerabilities	
User	Malicious employees who want to leak information
	Withdrawal of employees with company information
Service	Security vulnerability in business services
	Use non-licensed business services for account hijacking
Wireless	Wireless LAN connection with non-secured AP
	Direct exchange of information between employees
Network	Packet sniffing in network section
	Hacking network equipment such as switches, routers
Internal Network	Internal server hacking via mobile terminal
	Security vulnerability in cloud computing
Security threats and vulnerabilities of mobile office	
User	Careless work by employees
Terminal	Lost or stolen business terminal
	Use terminal of family members, relatives, etc.
	Information backup, synchronization of employee terminal
	Sale and transfer of employee terminals
	Security vulnerability of terminal operating system
	Use business applications on unlicensed terminals
Telecommuting security threats and vulnerabilities	
Home	Lost or stolen business terminal
	Use terminal of family members, relatives etc.
	Malicious software such as viruses and worms
	Lost or damaged printouts
Security threats and vulnerabilities of smart work center	
Center	Lost or damaged printouts
	Access to non-licensed centers
	Use non-licensor's public terminal
	Malicious software such as viruses and worms
	Business information stored in public terminal

As shown in Fig. 1, there are various security threats in the smart work environment. If security threats are managed in terms of users or corporations, a more secure smart work environment can be constructed. In order to promote the introduction of smart work to domestic and foreign companies (organizations) and activate smart work environment, security measures for smart work should be prepared, so that, security incidents that can occur in smart work environment can be minimized and prevented in advance. Table 1 appears the security threats and vulnerabilities by smart work structure (Anonymous, 2016).

Necessity for security audit in a smart work environment: It is possible to construct a remote collaborative environment regardless of working position through smart work and it is possible to form a more flexible work environment based on the work efficiency and so on. In November 2010, the Ministry of the Interior in Korea opened the Smart Work Center No. 1 and built the first space in Korea that can be used by employees of public agencies and private companies as well as information ministries and municipalities. In addition by 2015, the company will expand the number of Smart work Centers to 50, support the establishment and operation of smart work centers for public and private companies by enacting standards and methods for smart work center facilities and the legal and institutional basis for spreading smart work to build a domestic smart work environment (Anonymous, 2015).

However, as mentioned above, the smart work environment has a lot of security vulnerabilities and many companies (institutions) who want to introduce smart work are hesitating to introduce it because of security problem. The analysis of the domestic and Foreign smart work security guides mentioned above provides guides such as terminal, network and server, human security, access control and physical security are being discovered. So, there are many items that do not agree with the control items of existing information protection management system. Therefore, in order to establish a secure smart work environment, it is necessary to have an information protection audit system that can check whether risk has been analyzed and evaluated through highly reliable and systematic risk management to establish appropriate information protection measures.

ADVANCED PROPOSAL OF SMART WORK INFORMATION SYSTEM AUDIT MODEL USING INFORMATION SECURITY MANAGEMENT SYSTEM

Audit model: In order to strengthen the security audit, it is necessary to integrate the security check items integrated in the system architecture, the application system and the database into the security domain. In the case of 13 domains of information security management system, only the technical domain that is commonly used in security services such as security consulting is designed. When the separated security model is integrated with existing business type, audit time, audit area, audit view and inspection standard, the following audit framework of Fig. 2 is proposed.

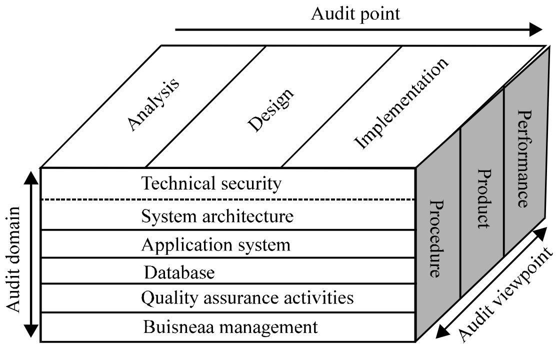

Fig. 2: Proposed audit model

Identification of checking items for information security vulnerabilities in smart work environment: In response to information security vulnerabilities in the smart work environment, various countermeasures may exist for a single vulnerability and threat and measures for information protection by smart work environments such as common, mobile office, home work and smart work center was summarized. Provides information protection supervision items that utilize the information protection management system according to the items of information security check by smart work type and countermeasures. The technical security checklist consists of three control areas and consists of seven detailed controls (19 control items). Technically apply cryptographic control to important information, perform information system access control and suggests items related to media security, malicious code infection, log and monitoring during operation. Table 2 is the proposed technical security audit checklists of smart work information security.

VALIDATION OF SMART WORK SECURITY AUDIT

Survey: The contents of the questionnaire were composed of the items related to the appropriateness of the security audit appropriateness and the control item using the information security management system in the smart work environment. The survey subjects consisted of 30 persons including security consulting, security information protection management system certification auditor, information system auditor, developer, system administrator as the Table 3.

Survey on the suitability of security audit checklists using information security management system: The questionnaire for the smart work information protection audit was used for each item as a 5-point scale that is highly required, required, moderate, less necessary and no need.

Table 2: Technical security audit checklists of smart work information security

Field/Detailed	Checklist
Password control	
Password policy	(Password policy establishment) Establish and implement policies for encryption targets, cryptographic complexity, key management and equipment cryptographic use
Access control	
Access control policy	(Establish of access control policy) Access control policy should be established such as access control areas and scope, access control rules and methods
User authentication and identification	(User authentication) It should be controlled by a secure user authentication process such as user authentication, limits of login, warning illegal login attempts (User identification) Identifiers should be assigned and restricted using specifiable identifiers (User password management) It is important to note that the user is responsible for password management such as password complexity, initial password change and change cycle
Access control area	(Network access) Establish procedures for network access control lists and network identifiers, internal and external networks should be separated (Server access) Access restriction method and safe access method should be defined and applied (Application access) Limit application access rights and minimize unnecessary exposure of sensitive information (Database access) Application and user tasks should be clearly defined, and access control policies should be established (Mobile device access) Mobile device authentication, access control measures and security measures should be established (Internet access) Internet access should be controlled through an intrusion prevention system and monitored for internet access
Operation security	
Media security	(Information system storage media management) Discard and reuse procedure of storage media such as hard disks, storage and documents should be established and protection mechanisms such as DRM for documents should be established (portable storage management) procedures and regulations related to the handling, storage, disposal and reuse of portable storage media shall be provided
Malignity code management	(Malicious code control) Protection measures such as malicious code prevention, detection, response, introduction of security solution should be established (Patch management) You should periodically apply the latest patches and, if necessary, analyze the impact on the system
Log management and monitoring	(Time synchronization) The information system time must be accurately synchronized with the official standard time (Logging and retention) The log type should be defined and maintained for a period of time and reviewed periodically (Access and usage monitoring) User access to critical information, information systems, applications and network equipment should be periodically verified (Infringement attempt monitoring) A system and procedure should be established to monitor attempts of infringement from the outside

Table 3: Surveyors

Variables	Security related	ISMS auditor	IS auditor	Developer	Total
Respondent	10.0	8.0	15.0	5.0	38
Distribution (%)	26.3	21.1	39.5	13.2	100

Table 4: Suitability of security audit checklists using information security management system

		Response						
Field	Checklist	1	2	3	4	5	Avg.	SD
Password Policy	Password policy establishment	2	5	13	17	1	3.26	0.99
Access Control Policy	Establish of access control policy	0	2	4	27	5	3.92	0.77
User authentication and identification	User authentication	0	0	5	16	17	4.32	0.69
	User identification	0	0	5	13	20	4.39	0.71
	User password management	0	0	3	19	16	4.34	0.62
Access control area	Network access	0	0	8	22	8	4.00	0.65
	Server access	0	0	4	28	6	4.05	0.51
	Application access	0	0	14	20	4	3.74	0.64
	Database access	0	0	16	11	11	3.87	0.83
	Mobile device access	0	0	11	21	6	3.87	0.66
	Internet access	0	0	10	12	16	4.16	0.81
Media security	Information system storage media management	0	0	3	18	17	4.37	0.62
	Portable storage management	0	0	3	24	11	4.21	0.57
Malignity code management	Malicious code control	0	0	8	9	21	4.34	0.80
	Patch management	0	0	3	29	6	4.08	0.48
Log management and monitoring	Time synchronization	0	0	3	26	9	4.16	0.54
	Logging and retention	0	0	3	31	4	4.03	0.43
	Access and usage monitoring	0	0	11	11	16	4.13	0.83
	Infringement attempt monitoring	0	0	3	10	25	4.58	0.63

CONCLUSION

The rapid development of information technology has been actively promoting smart work and the importance of information security has been emphasized. The BYOD (Bring Your Own Device) which uses smart phones and tablet PCs for business is getting a lot of attention. Smart work environments such as mobile office, telecommuting, it is rapidly spreading according to the environment of the enterprise (institution). Security threats and vulnerabilities related to smartware are also rapidly increasing.

Therefore, companies can build a secure smart work environment considering security by complying with administrative, physical and technical information protection measures such as access control of important assets.

In this study, it is proposed a secure smart work in accordance with a reliable standard procedure even in an organization in which an enterprise information protection plan and system is not established. In order to organically link with the existing information security management system, the security audit model and the checklists were established.

Through this information protection management model based on this information protection management system, it is expected to be able to construct an environment that can safely and efficiently protect the enterprise's assets and services from security threats in a rapidly changing IT environment such as smart work environment.

In this study, the approach of information protection audit is presented based on KISA-ISMS. It is expected to improve the existing information protection audit and to cope with the smart work environment. However, there are following limitations and further study is needed.

First, the scope and scope of information protection depends on the type of smart work environment. In this study, some items of smart work related check items are presented but the study of specialized items such as smart work telecommuting, smart work center and mobile office should be followed up successively.

Second, it is necessary to study how to implement information protection audit efficiently in a limited audit schedule and manpower environment, although, detailed results can be derived by using items of inspection of information protection management system.

Finally, this study has limitations that it cannot be verified by applying it to actual smart work environment construction project. Therefore, it is necessary to follow up further research to make it more realistic as a supervisory model by revising and supplementing the application to the actual smart work information protection audit.

REFERENCES

Alavi, R., S. Islam and H. Mouratidis, 2014. A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations. In: Human Aspects of Information Security, Privacy and Trust, Tryfonas, T. and I. Askoxylakis (Eds.). Springer, Cham, ISBN:978-3-319-07619-5, pp: 297-305.

Anonymous, 2011. Guide for smart work introduction and operation for enterprises. The Korea Communications Commission (KCC), South Korea.

Anonymous, 2015. Smart work promotion plan. Ministry of Public Administration and Security, Seoul, South Korea.

Anonymous, 2016. National information society white paper. Korea National Information Society Agency, Seoul, Korea.

Cheng, L., Y. Li, W. Li, E. Holm and Q. Zhai, 2013. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Comput. Secur., 39: 447-459.

Disterer, G. and C. Kleiner, 2013. BYOD bring your own device. Procedia Technol., 9: 43-53.

Koh, E.B., J. Oh and C. Im, 2014. A study on security threats and dynamic access control technology for BYOD, smart-work environment. Proceedings of the International Multi Conference on Engineers and Computer Scientists Vol. 2, March 12-14, 2014, IAENG, Hong Kong, China, ISBN:978-988-19253-3-6, pp:1-6.

Lovaas, P. and S. Wagner, 2012. IT audit challenges for small and medium-sized financial institutions. Proceedings of the Annual Symposium on Information Assurance & Secure Knowledge Management, June 5-6, 2012, Empire State Plaza, ALBANY, New York, USA., pp: 1-20.

Miller, K.W., J. Voas and G.F. Hurlburt, 2012. BYOD: Security and privacy considerations. Prof., 14: 53-55.

Susanto, H., M.N. Almunawar and Y.C. Tuan, 2011. Information security management system standards: A comparative study of the big five. Intl. J. Electr. Comput. Sci., 11: 23-29.