Information Security Resilience for Public Sector

HarkSoo Park
Dept. of Science and Technology Cyber Security Center
Korea Institute of Science and Technology Information
Daejeon, Korea
e-mail: hspark@kisti.re.kr

Gwangil Ju
Dept. of Science and Technology Cyber Security Center
Korea Institute of Science and Technology Information
Daejeon, Korea
e-mail: kiju@kisti.re.kr

Abstract— **Recently, rapid changes in IT environment have shifted the security paradigm from data protection to protection of people. As a result, IT-related government policies have also changed. In terms of IT compliance, government bureau have suggested diverse laws and guidelines. Under these circumstances, this study attempts to determine IT compliance issues from the perspective of IT security personnel in a public agency and derive the related issues from the information security standpoint. Furthermore, it targets to address how to develop the IT security compliance in a progressive manner, focusing on the case of the public authority 'K Agency' after checking current IT security compliance issues.**

Keywords-component; Information Security System; Resilience; Compliance.

I. INTRODUCTION

Security Resilience refers to the ability to continuously deliver the intended outcome despite adverse cyber events. [1]. According to the National Information Protection White Book [2], the government passed the 'National Cyber Security Bill' during the National Assembly due to the continued threats to national security by North Korea and other serious cyber security issues on January 3, 2017. In a public sector, for the establishment of cloud security policy, an Act on the Development of Cloud Computing and Protection of its Users was put into effect in September 2015. In case of the Personal Information Protection Act, in addition, privacy protection has been stricter every year. In fact, many public agencies have made a lot of effort to examine and implement IT security compliance requests whenever they occur.

As a result, the security officers at various levels of the organizations are continuously spending administrative expenses to implement IT security compliance for the public sector in Korea and abroad. In addition, there is the burden of the implementation.

II. IT SECURITY COMPLIANCE IN KOREA

Domestic compliance has been proposed starting from 2009 with the focus on the financial sector. Since IT compliance is an information technology related to internal control, it is closely related to information security and IT systems of each organization are met with the requirements of government policies and guidelines, as well as to establish information systems in the direction that they can achieve.

According to Financial Security Institute (FSI) [3], it has reviewed and analyzed domestic and international laws & standards and industrial standards for IT system security management and published the compliance (2000). Then, the guidelines (2015) have been provided to each financial institution [4].

In the public sector, an FSI guide-level promotion system is not available yet. The administrative body 'Ministry of the Interior and Safety' and professional agency 'Korea Internet & Security Agency' have promoted IT security-related compliance. The major IT compliances are listed in TABLE I.

TABLE.1 IT COMPLIANCE STATUES IN PUBLIC SECTOR

Category	Description
Public Sector IT Compliance (Domestic Law)	- National Information Framework Act - Act on Information Network Promotion and Information Protection, etc. - Information Communication Infrastructure Protection Act - E-government Act - Privacy Act - Act on Promotion of Information Protection Industry - Development of laws Concerning Development of Cloud Computing and Protection of Users
Other Domestic Laws	- Electronic document and electronic trading Act - Electronic Signature Act - Communication Confidentiality Protection Act - Copyright law - Industrial Technology Protection Act - Act on Protection and Utilization of Location Information, etc.
Global	GDPR
Standard/Certification	ISO27001, ISMS, PIMS, ePrivacy

Public sector IT compliance major issues can be divided into information security, privacy, and informatization. The Ministry of Public Administration and Security is promoting related policies to establish information system and information management system for the public sector based on the National Informatization Basic Law and the Personal Information Protection Act. The Information Security Division is responsible for assessing the level of information security at various levels of the National Intelligence Service (NIS), which acts as the National Cyber Security Control Tower, and has designated and managed major information and communication infrastructure.

In particular, the national information security management system is structured for the NIS to handle the national information security planning and coordination, as

 ISBN: 978-1-61208-661-3

stated in Figure 1 (defined by Kim [5]). This management system is handled separately from the informatization and privacy protection which is done by the Ministry of the Interior and Safety. Therefore, the information security manager from a public agency is required to respond to each compliance issue by informatization, information security and privacy protection individually.

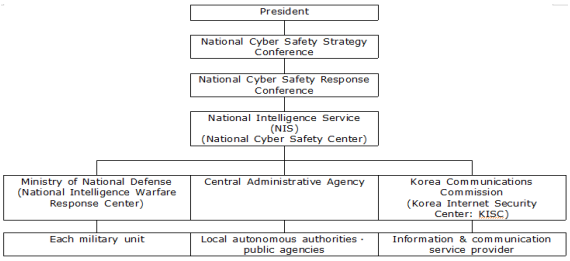

Figure. 1. National Information Security Management

III. CASE STUDY : 'K' AGENCY'S IT SECURITY COMPLIANCE

The 'K' agency affiliated with the Ministry of Science and Technology is a government-funded research institute in the IT infrastructure field of science and technology, and operates more than 100 information systems. To operate on many information systems and informatization projects, the information security system of 'K' agency was divided into information security governance (Figure 2) and the following information security management system (Figure 3) was drawn as follows [6]:

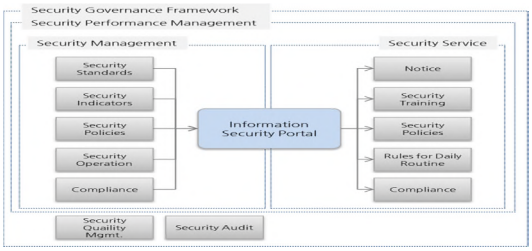

Figure. 2. Information Security Governance

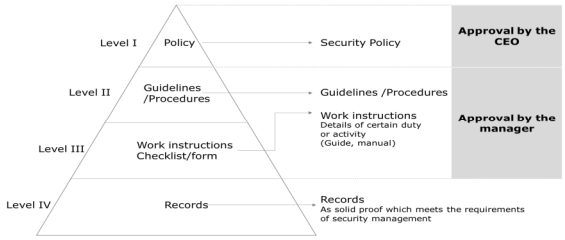

Figure. 3. Information Security Management Frame (Process)

In information security governance, 'K' agency has responded to the related information and compliance issues in real-time through the information security portal. In 2017, the security management was integrated with the intranet and provided in an electronic payment format (11 duties in total). As a result, the duties of security managers from each department and agency became more convenient (TABLE II).

TABLE II. APPLICATION EXAMPLE OF IT BUSINESS INTEGRATION

Category	Related Work Process
Informatization	- Enable / Change / Terminate DNS - LAN / Telephone Installation Request - Review of Equipment Installation - VPN Request - Review of RFP(Informatization Project) - Review of Output(Informatization Project)
Information Security	- Review of Information Security - Review of Security Level - External Access Permission / Blocking
IT Asset	- Import Asset(RFID connection) - Export Asset(RFID connection)

IV. CONCLUSION

In order to secure resilience, close implementation of government policy should be preceded. The government-level IT compliance has been performed in accordance with its related laws. Under some laws, a fine is charged on the un-fulfillment. Under these circumstances, IT departments can fulfill their role provided that there is close implementation with government compliance, and the related duties in the agencies are efficiently integrated. Then, the tasks should be promoted to improve the management level in each category (informatization, information security, personal information).

For this purpose, it is necessary to take active role in ensuring the information security dedicated organization and actively participate in the project in terms of the working organization, the management, the staff, and the auditing, and public relations activities of the government IT compliance are the most important.

This study approached what should be fulfilled first from the IT security compliance's perspective in a public sector. It is anticipated that it would suggest specific guidelines for the public sector and make a contribution to the improvement of the information security management level in a public sector.

REFERENCE

[1] B. Fredrik et al, "Cyber Resilience Fundamentals for a Definition", Advances in Intelligent System & Computing, 2015.

[2] National Intelligence Agency, National Information Protection White Book in 2017, 2017.

[3] Financial Security Institute, Financial Compliance Analysis Report, 2009

[4] Financial Security Institute, Financial Security Governance Guideline, 2015

[5] J. Kim, "National Information Security Agenda and Policies", Digital Policy Studies, Vol. 10, 2012

[6] G. Ju et al, A study of the factors that influence the information security compliance, Lecture Notes in Electrical Engineering, 2017, Vol. 448, p.720-728.

 ISBN: 978-1-61208-661-3