International Journal of Security and Its Applications
Vol. 10, No. 6 (2016) pp.123-134
http://dx.doi.org/10.14257/ijsia.2016.10.6.13

A Study on Control Item of ISMS in the Financial Industry

Yong-Sik Kim[1], Gyoocheol Lee[2], Yongtae Shin[3], Younglak Choi[4], Jin-Ho Park[5] and Jong-Bae Kim[6*]

[1,2,5] *Department of IT Policy and Management, Graduate School of Soongsil University, Seoul, 156-743, Korea*
[3,4,6*] *Graduate School of Software, Soongsil University, Seoul, 156-743, Korea*
[1]*yskim7514@gmail.com*, [2]*sopoong297@hanmail.net*, [3]*shin@ssu.ac.kr*, [4]*ylchoi58@ssu.ac.kr*, [5]*j.park@ssu.ac.kr*, [6*] *kjb123@ssu.ac.kr*

Abstract

It is a double bind for financial companies to observe electronic financial transaction law and regulation for maintainment a certain level of information security, as well as to introduce information security management system for improvement the company's information security level. In reality financial companies are suffering from spending a lot of time and money to apply highly professional and technical knowledge information security control items that may be redundancy or dissimilar. This study presents a specific authentication model on the financial industry through unifying a duplicate set of controls in terms of the electronic finance transaction law & regulation on e-banking and complements the missing items ISMS controls on the financial industry.

Keywords*: ISMS, certification, specific, Control item*

1. Introduction

Current electronic financial transactions came to have better availability and usability due to their transaction means (internet banking, mobile phone app and others) but relatively, security threats were increased as the latest attack types are simultaneously multiple, repetitive and highly intelligent, there occurs incidents as private information leaking in large scale (NH Nonghyup in Jan 18, 2014) and infringement accidents via hacking (NH Nonghyup, Shinhan Bank, OOO broadcasting corporation and other in Mar 20, 2013). Though financial corporations' data processing systems are designated as info-communication infrastructures for safe financial transactions, criteria that control information security management level via relevant laws and regulations by financial administrations (such as Electronic Financial Transaction Act, Electronic Financial Supervision Regulation, setting criteria on mother laws for protection works in IT parts of financial corporations and IT inspection manuals, collectively referred as 'regulations related to Electronic Financial Transaction Act' hereafter) exist, those rather frequent data processing accidents are occurring recently. Therefore, financial administrations focus on information security management system strengthening policies [1]. Based on Regulations on promotion of information and communication network use and protection of information, Ministry of Science, ICT and Future Planning is demanding forced authentication on financial industry (criteria: the information and communication service providers with its revenue more than 10 billion KRW or with its users a million or more per day) to adopt am information protection management system (ISMS: Information Security Management System, referred as 'ISMS' hereafter). Therefore, through an

6* Corresponding author. Tel. : +82-10-9027-3148.
Email address: kjb123@ssu.ac.kr(Jong-Bae Kim).

ISSN: 1738-9976 IJSIA

agreement with Ministry of Science, ICT and Future Planning (ISMS seminar hosted by Ministry of Science, ICT and Future Planning on Oct 30, 2013), Financial Committee has recommended and requested to adopt ISMS authentication requests to 24 major financial corporations [3]. However, financial corporations must conform to the control criteria (composition) of information security management system clearly mentioned in the regulations related to Electronic Financial Transaction Act, and this became burdening situation as it causes increased amount of work due to double regulations maintaining information security management system for control items of ISMS authentication system along with the cost for acquiring ISMS authentication. If the corporation plans to go overseas then there is another prep must be done as there is an international standard management system (ISO/IEC 27001) that must be followed and acquired which is not compatible to ISMS authentication which is domestic.

As existing ISMS consists of universal control items targeted for the firms applicable based on Regulations on promotion of information and communication network use and protection of information, it is necessary to add and supplement the composition items suitable for the data processing system specialized for the characteristics of its electronic financial transactions. Via comparisons and verifications on the control items of regulations related to Electronic Financial Transaction Act and ISMS authentication system, this study is to suggest an information security management system authentication model specialized for financial industry with the purpose to resolve the above mentioned double regulation on control items.

2. Relevant Researches

With 104 control items and 253 detailed items from ISMS, this study compared and verified them against the control standards (compositions) clearly mentioned in regulations related to Electronic Financial Transaction Act through quantitative analysis and deduced the items to be repeated and mutually supplemented in control items (criteria).

The domestic ISMS authentication system is a system that approves whether an organization systematically prepares its plans, keeps its documents and continuously manage and operate them in order to protect its major assets as such verification is done by a designated authentication administration (KISA), and request on authentication acquisition can be made within 2 months of minimum after the management system is installed. The authentication is valid for 3 years (annual inspection shall follow) and there are credits for the organization as they receive extra points when applying for public IT projects and a discount on buying insurances related to information protection. The authentication system consists of authentication verification execution, consideration and approval by authentication committee, and final designation by Ministry of Science, ICT and Future Planning as an authenticated organization which is now under management of the ministry.

ISMS authentication consists of 104 control items and 253 detailed inspection items in total of 18 areas and those are for planning and sustaining of preventive, systematic and continuous managerial, technical and physical information protection measures to deal with highly intelligent and meticulous infringement accidents [2].

The control criteria (compositions) clearly mentioned in regulations related to Electronic Financial Transaction Act consists of the items to measure the level of IT security management system targeted for financial corporations. As those control criteria are based on Electronic Financial Supervision Regulation, there are certain differences to general control items which can be used to all industries such as ISMS or ISO27001. Though Electronic Financial Supervision Regulation enables to evaluate by posting analysis and evaluation criteria of information protection management system for financial fields based on 45 control items and 428 detailed items, it is possible to neglect

inappropriate items for analyzing and evaluating such as info-communication infrastructure, IT division projects and others and is regulated to specify the reasons for such exclusion in the results of weakness evaluation. On top of that, financial corporations may selectively add evaluation components with considerations on the characteristics of evaluation target and threats and contents of security issues and others [4].

Control criteria consist of managerial area, technical area, and physical composition.

Table 1. ISMS Configuration Item Classification

Area		Control item	Detailed item
Information protection management process	**1. Information protection policy planning and setting its range**	2	4
	2. Executive responsibilities and organization structure	2	4
	3. Risk management	3	11
	4. Information protection policy realization	2	3
	5. Post management	3	6
Information protection countermeasure	**1. Information protection policy**	6	13
	2. Information protection organization	4	7
	3. Outsider security	3	4
	4. Information asset classification	3	7
	5. Information protection training	4	10
	6. HR security	5	11
	7. Physical security	9	21
	8. System development security	10	22
	9. Passcode control	2	8
	10. Access control	14	46
	11. Management security	22	56
	12. Infringement accident management	7	14
	13. IT calamity restoration	3	6
	Total	104	253

Figure 1. ISO 27001 Standard Structure

Figure 2. PDCA(Plan-Do-Check-Act)

Table 2. A List of Evaluation Control Items to Weakness Analysis for Financial Industry

Control criterion	Detailed item
1. IT HR	4
2. IT organization	3
3. IT budget	2
4. Buildings and facilities	19
5. Data processing room	17
6. Terminal	13
7. Data processing material management	22
8. Information processing system	10
9. Information protection system	7
10. Public web-server	22
11. Network	1
12. IP address	5
13. Information technology plan	4
14. Information technology project	4
15. Information technology contract	9
16. Information technology inspection	5
17. Capacity/performance management	1
18. Job segregation	8
19. Control by head of data processing room	8
20. Transaction control	2
21. Program control	10
22. Batch job control	5
23. Passcode program key management control	4
24. Internal user password management	8
25. Information technology outsourcing	14
26. Status evaluation on IT division	3
27. Electronic transaction guidelines	10
28. User regulation posting	5
29. Security review	3
30. User password management	11
31. Weakness analysis evaluation	2
32. Infringement accident prevention	7
33. Malware infection prevention	5
34. Emergency	17
35. Calamity restoration center	4
36. Calamity restoration training	1
37. Infringement accident corresponding exercise	2
38. Electronic financial transaction accident report for IT division	8
39. UNIX server	14
40. Windows server	46
41. DB	10
42. Security equipment	16
43. Network equipment	14
44. Web service	28
45. Smart phone banking	15
Total	428

As a result from comparison analysis on the control items, it was analyzed as that there are common and/or repeated ones in 79 items that are from regulations related to Electronic Financial Transaction Act, out of 104 of ISMS authentication standard control items. It was investigated that some of ISMS control items were lack of control criteria that can be substituted by regulations related to Electronic Financial Transaction Act and it is indicated that there is a tendency that the Act is biased onto some specific areas (26% of more specific in the Act). Those 13 control items that exist in ISMS but not in the Act were performed as information protection policy planning, asset identification and evaluation, carrying of mobile equipment, utilization of smart devices and others in the forms of official documents by Finance Committee and the Financial Supervisory Service and rules and guidelines. And those 21 control items that exist in regulations related to Electronic Financial Transaction Act but not in ISMS did not contain detailed protection measures reflecting the characteristics of financial work such as compulsory network separation, IT outsourcing, security approval, control by head of data processing room, EULA and others.

Table 3. Electronic Financial Transaction Regulation Control Criteria Comparison to ISMS Control Items

Control item	**Number of comparison results of control items**				
	>	**<**	**=**	**X**	**Total**
Information protection management process	3	0	7	2	15
1. Information protection policy	1	0	0	5	6
2. Information protection organization	0	0	4	0	4
3. Outsider security	0	1	2	0	3
4. Information asset classification	2	0	1	0	3
5. Information protection training	0	1	3	0	4
6. HR security	1	2	2	0	5
7. Physical security	1	2	3	3	9
8. System development security	0	3	7	0	10
9. Passcode control	0	1	1	0	2
10. Access control	2	1	10	1	14
11. Management security	1	12	7	2	22
12. Infringement accident management	1	4	2	0	7
13. IT calamity restoration	0	0	3	0	3
Total	12	27	52	13	104

Table 4. Analysis Results on Control Items

Sign	**Meaning**	**Number of control items**	**Proportion**
>	**ISMS is specific**	12	11.5%
<	**Electronic Financial Transaction Act is specific**	27	26.0%
=	**Both are about same level**	52	50.0%
X	**The one exists in ISMS but not in Electronic Financial Transaction Act**	13	12.5%
Total		104	100%
The one exists in Electronic Financial Transaction Act but not in ISMS		21	-

By applying weights among control items, estrangement ratio (bias) and standard deviation to acquire statistical values, the acquired estrangement ratio was 0.95 which is close to 1 hence it is estimated that ISMS and regulations related to Electronic Financial Transaction Act are almost the same, and as the average segment by standard deviation was large (minimum of 0.48 and maximum of 1.41), it was analyzed that there is no items that can be replaced by the control items from ISMS in the control criteria of regulations related to Electronic Financial Transaction Act, or there is a tendency that specific nature is biased on specific fields.

Table 5. Results after Applying Weighting onto Control Items

Sign	Meaning	Weighting	Quantity	Weighting sum	Bias	Standard deviation
>	**ISMS is specific**	0.5	12	6	0.95	0.46
<	**Electronic Financial Transaction Act is specific**	1.5	27	40.5		
=	**Both are about same level**	1	52	52		
X	**The one exists in ISMS but not in Electronic Financial Transaction Act**	0	13	0		
Total			104	98.5		

* Estrangement ratio (bias): 1 as basis, being smaller than 1 makes ISMS more specific than the Act and begin bigger than 1 makes the Act more specific than ISMS

** Standard deviation: as it gets closer to 0, the coverage and specific nature of both ISMS and the Act become more similar to each other and as it gets further from being 0 then the control criteria in regulations related to Electronic Financial Transaction Act either do not exist in ISMS or it has higher tendency that they are biased to specific fields.

As we matched and compared the ISMS control items applied to private sectors and 'Evaluation on information security management status of public facilities conducted by NIS (25 categories and 127 items)' which is conducted using information protection management system applied to public sectors as its basis, approximately 80% of them were matched [5]. From private sectors, there were no measures taken for secret management part which is under operation by public sectors, while items as information security planning on policies and budgets and information security work performance and information communication device management in operation management area that are used to figure out interest rate of head of facilities indicated some differences to private sectors (reflecting the characteristics of public sectors) [3].

3. F-ISMS Model Specialized for Financial Industry

Based on the analysis on repetitiveness, similarity, weights and estrangement ratio of regulations related to Electronic Financial Transaction Act and ISMS and the contents of financial IT security compliance, it is to suggest control item model for financial information security management system authentication by composing the control items of information protection management system specialized for financial industry.

3.1. Composition of F-ISMS Control Item

As shown in Table 6, the composition plan for F-ISMS authentication system shall be composed with 3 areas of financial security management area, financial security measures and financial transaction, with in total of 130 control items and 282 detailed items.

First, we disregarded the sections from information protection management processed among ISMS control items that are irrelevant to financial industry then we composed the control items that change the sections indicating commonness of composition criteria of regulations related to Electronic Financial Transaction Act into standard terms. We composed the financial security management area into 5 categories, 13 control items and 27 detailed control items and suggested a plan to compose financial security counter-measure area into 9 categories, 81 control items and 177 detailed control items.

Second, we newly added financial transaction protection area for data processing system in order to secure safe electronic financial transaction from regulations related to Electronic Financial Transaction Act that are not contained within ISMS control items and composed it into 6 categories, 26 control items and 63 detailed control items. The supplemented control items have newly added control items such as use, management and disposal of private information and others in order to be prepared for electronic transaction security and outsourcing security, loss of financial firms and social issues. The detailed control items were reflected with factors as risk management, terminal security, passcode control, job segregation and others.

Third, out of the 130 items from F-ISMS control item composition, 86.9% of them (111 items) were reflected to final control items as a result of corresponding comparison of the control items from regulations related to Electronic Financial Transaction Act, while corresponding comparison of the control items from ISMS, 72.3% (94 items) were reflected.

Table 6. F-ISMS Control Item Composition Plan

Category		Control item	Detailed item	Regulation control item	ISMS control item
Financial security management	**1. Setting up financial security policy and its range**	2	7	2	2
	2. Executive responsibility and CISO organization composition	2	5	2	2
	3. Risk management	3	7	2	3
	4. Financial security counter-measure realization	3	4	3	2
	5. Post management	3	4	2	3
Financial security countermeasure	**1. Information security policy**	6	8	6	6
	2. Information protection organization	4	6	4	4
	3. HR security	8	4	7	7
	4. Physical-environmental security	9	15	8	9
	5. Operation management	25	32	22	21
	6. Data processing equipment internal control and access control	15	30	15	13
	7. System development, introduction and maintenance	14	36	14	10

	8. Emergency plan and work continuity management	4	36	2	3
	9. Security accident correspondence	6	10	5	5
Financial transaction protection	**1. Electronic financial transaction security**	5	32	5	1
	2. User protection	5	10	5	3
	3. Outsourcing security	7		7	0
	4. Financial private information collection	4	5	0	0
	5. Use and provision of financial private information	2	15	0	0
	6. Management and disposal of financial private information	3	1	0	0
Total		130	282	111 (86.9%)	94 (72.3%)

3.2. Consideration when Applying F-ISMS Control Items

First, due to Electronic Financial Supervision Regulation, the control items of IT supervision and inspection systems that are unique authorities of the Financial Supervisory Service were not reflected to F-IMSM control items. This was done as the purpose of F-ISMS authentication system that authenticates the level of security management of financial corporations and exempting IT inspection that investigates violation of regulations and/or shrinking its ranges did not meet the purpose of such IT supervision. Irrelevant to F-ISMS authentication acquisition, the control by IT supervision composition must be performed. Second, under the considerations on effectiveness issues on authentication acquisition due to infringement accidents occurred to financial institutions that acquired ISMS and/or ISO27001, it is fair to say that a financial corporation must be under control of F-ISMS evaluation items as it is applied to all systems that are related to electronic financial transactions rather than acquiring F-ISMS authentication on partial financial services and/or systems.

4. Conclusion

Under considerations on the burdened circumstance due to the effects of the control items of information protection management system of financial corporation based on regulations related to Electronic Financial Transaction Act and the responsibility on ISMS authentication acquisition, this study was to resolve the double regulation by suggesting an integrated information protection management system model.

Though it was difficult to identify the exclusive boundaries among the control items from targets in composing the control items for the model, the repetitiveness was modified under considerations on the characteristics of financial corporations that must follow regulations related to Electronic Financial Transaction Act, and through supplementing the system of electronic financial transaction and the categories of private information management. However, it was not adequate in reflecting the control items related to IT risks that are scattered over the places in the industry as a new category.

It is expected that the control item model for specialized F-ISMS shall me enough to resolve the double regulation due to the regulations on financial corporations and to secure the independent nature and the consistence in their policies in information protection management systems of financial industry. Furthermore, it is expected that the model can act as an evaluation criterion or a standard for measuring and authenticating the level of management on information protection management systems. Also, the

model surely can contribute in securing work efficiency as it can disregard those reflected items when IT inspection conducted by the Financial Supervisory Service.

References

[1] KOREA FINALCIAL SERVICES COMMISION, "Enhanced Comprehensive Measures of Financial Computer Security", **(2013)**.
[2] KISA (Korea Internet&Security Agency), "Candidate Training Materials the Certification Examinant of ISMS", **(2011)**.
[3] KOREA COMMUNICATIONS COMMISSION, "Enacted and Amended Notice of Corporate Information Security", **(2013)**.
[4] KOREA FINANCIAL SERVICES COMMISION, "Electronic Financial Transactions ACT & The Detailed Regulation on Supervision of Electronic Financial", KOREAN FINANCIAL SUPERVISORY SERVICE "Best Practices Protect Business of Financial Company for Information Technology", "Financial Sector Vulnerability Assessment Criteria", "Inspection Manual for Information Technology", **(2013)**.
[5] NATIONAL CYBER SECURITY CENTER, "Public Institutions 'Information Security Management Evaluation' Commentary", **(2012)**.
[6] KOREA FINANCIAL SECURITY INSTITUTE, "Financial IT Security Compliance Reference Guide Ver1.0", **(2012)**.
[7] L. Junwon, "Understanding and Issues of ISMS", KOREA FINANCIAL TELECOMMUNICATIONS & CLEARINGS INSTITUTE, **(2012)**.
[8] KOREA FINANCIAL SECURITY INSTITUTE, "Financial IT Security Compliance Research Reports", **(2011)**.

Authors

Yong-Sik Kim, received his Bachelor`s Degree in Economics from Sungkyunkwan University in Korea (1977) and Master's Degree in Business Administration from Yonsei University in Korea (1994). He worked as a President of Ssangyong Cement and Ssangyong Information and Communication Company. And he is studying his Ph.D. degree of IT Policy Business Administration in Soongsil University, Seoul.

Gyoo-Cheol Lee, is studying his Ph.D. Degree of IT Policy Business Administration in Graduated Soongsil University, Seoul. He worked as a developer and operator of a business sale signed by joining Koscom. And He has worked as the analysis and evaluation team leader of information protection center. His current research interests include financial IT, IT security policy, the field of analysis of infringement accident or hacking and information protection management system (ISMS).

Yong-Tae Shin, is a Ph.D. professor in the School of Computer Science and Engineering, Soongsil University, Seoul, Korea. His research interests focus on Multicast, IoT, Information Security, Content Security, Mobile Internet, Next Generation Internet.

Yong-Lak Choi, received his Bachelor's, Master's and Doctor's Degree in Computer Science in Soongsil University, Seoul. Now he is a professor in the Graduate School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, and Database.

Jin-Ho Park, received his Bachelor's Degree in Software Engineering in Soonsil University, Seoul (1998). and Master's Degree (2001), Doctor's Degree in Computer Science in Soongsil University, Seoul (2011). Now he is a professor in the School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, SW Safety/QA/Testing, SW Convergence/Power, IoT, National Defense ISR, IT Service, IT Technical Commercialization and Start-up, *etc*.

Jong-Bae Kim, received his Bachelor's Degree in Business Administration in University of Seoul, Seoul (1995) and Master's Degree (2002), Doctor's Degree in Computer Science in Soongsil University, Seoul (2006). Now he is a professor in the Graduate School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.