Compliance Risk Assessment Measures of Financial Information Security using System Dynamics

Ae Chan Kim[1], Su Mi Lee[2] and Dong Hoon Lee[3]

[1, 3]*Graduate School of Information Security, Korea University*
[2]*Financial Security Agency, Korea*
{[1]holytemple, [3]donghlee}@korea.ac.kr, [2]smlee@fsa.or.kr

Abstract

In this paper, we analyze relationships between EFT (Electronic Financial Transaction) Act of Korea and risk assessment standards and propose the map that helps financial institutions determine the priority of security control areas. It is a new method for financial information security risk identification and assessment through correlation analysis between the variety security standards and requirements. We attempt to integrate different information security standards and propose risk assessment measures specializing in financial companies based on the mixed methods of quantitative and qualitative methods to determine the priority through the calculation of weights. From the results of correlation analysis, three main security control areas are found to be more important than other areas and it can be utilized as a risk management measure about security countermeasures. In addition, financial companies should improve three main security control areas in an interval of at least 10 months. We expect that our result can be provided to security manager and IT auditor for establishment of risk mitigation strategies as basic data.

Keywords: *Risk Assessment, Financial Information Security, System Dynamics*

1. Introduction

The reason why information technology has its significant implications in financial sector is that financial business is an information industry, and information production technology is an important source of the competitiveness of financial institutions. However, IT systems have widely been applied to the financial companies, security incidents of financial IT services such as internet banking hacking against the financial companies have occurred continuously, resulting in a loss of the financial IT systems.

In this regard, it was required to apply the enhanced compliance regulations of Sarbanes-Oxley Act: 2002, Basel Ⅱ and PCI DSS: 2010 to financial IT systems. In Korea, to respond effectively to the financial IT security incidents, policy institutions, supervisory agencies and related businesses have suggested countermeasures to minimize the extent of damages. And yet, there are limitations in information security budget and workforce despite the presence of numerous standards, policies and regulations for information security compliance in each organization [4]. Accordingly, security managers and executives will strive to comply with information protection from high-risk portions depending on the situations of each organization. For risk management, systematic and exact risk identification should be preceded, and the effectiveness of risk management is most noticeable when the threats and security requirements corresponding to it are properly reflected in the analysis. Our study deals with risk assessment measures of financial companies based on ISO27001, KISA ISMS Certification system and EFT Act [3].

2. Background and Approach

2.1. IS (Information Security) Standards

The international ISMS (Information Security Management Systems) standards were disseminated through determination of the British standard BS7799 on the ISM, and certification system on the ISMS was first established based on BS7799 Part2 (certification standards) in 2002. After that, through the international organization for standardization (ISO), BS7799 Part1 (ISM best practices) became ISO17799, then ISO 27002, and BS7799 Part2 became ISO 27001 through several revisions. ISO 27001 sets out specific requirements related to ISMS, and ISO 27002 consists of codes of practice for ISM [7]. ISO 27001 is composed of a total of 11 control areas, 39 control objectives and 133 control items. The international standards for ISMS include ISO 27001, and the new ISO27000 series is to be updated by 2012 [6]. Among them, ISO 27005 is about risk management, and it serves as general guidelines to meet the requirements of ISO 27001.

In Korea, ISMS certification scheme was established based on the Article 47 of ICI Act [5] (ICI: Act on Promotion of Information and Communications Network Utilization and Information Protection) for the establishment of ISMS, and KISA has examined and issued certificates to private companies. As a certification system based on the TTA standards, KISA ISMS includes all ISO 27001 international standards, and it has strengthened security requirements of incident prevention, encryption and electronic trading to fit the situation of Korea. Accordingly, KISA ISMS certification guarantees that ISMS is established in accordance with domestic information security environment, while satisfying all standards required by ISO 27001 certification criteria [1, 2]. Meanwhile, Korea Financial Services Commission and the FSS (Financial Supervisory Service) established the information security best practices that meet the situation of financial companies in Korea based on 'The Regulation on Supervision of EFT' and distributed the FISS (Financial Information Security Standards) to each financial company [4].

2.2. Risk Management

Risk refers to the possibility of threats using the vulnerability that have a negative impact on the organization. The main goal of risk management is to reduce the risk to an acceptable level. Risk management is a process to improve problematic elements based on the security check items presented in ISO27002, and it is dealt with in various ways, not limited to information system. Managing risks mean considering not only technical aspects that identify and remove technical vulnerabilities, but also administrative and physical aspects of organization. In addition, the risk management procedures include process to predict the scale of resources to be inputted to reduce the possibility of security incidents and level of risks to be improved after the input in addition to passive administration duties. Risk Management goes through the process of (i) Risk Identification (ii) Risk Analysis (iii) Risk Mitigation(Choose the appreciate safe-guard).

Risk Assessment is the process of identifying risks to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analysis, and considers mitigations provided by security-controls planned or in place.

Synonymous with risk analysis, Risk Assessment can justify security safeguard by providing the management with statements needed to determine which risks are mitigated, imputed and accepted. Risk analysis is to analyze which threats exist in the assets after giving values to assets in which support is required and calculate risk by identifying threats and evaluating the impact through correlation analysis. The main objectives of the risk analysis are to measure risks on the IT assets and provide a basis to judge whether the level of the measured risks is acceptable or not. The next step is to quantify the effects of the potential threats and provide an economic balance between the impact of the risk and the costs of the countermeasure (cost / benefit justification) [9]. Figure 1 illustrates the entire process of risk management [8].

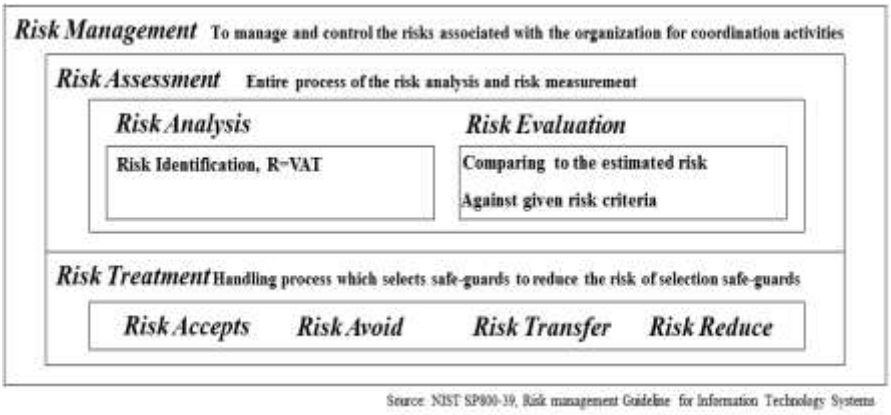

Figure 1. Risk Management Overview

2.3. System Dynamics

System Dynamics is one of simulation methodologies that defines the system composed of variables directly or indirectly related to the problems presented and solves the problems by identifying dynamic characteristics of the system through simulation after analyzing the relationship between variables quantitatively. In other words, it is suitable for exploring ways to resolve problems as one of the optimization techniques to analyze how system behaviors lead as a whole rather than to analyze them in detail. It is expressed in the form of causal map using system dynamics techniques, and '+' represents positive effect, and '-' negative effect. In this study, the risk is identified by analyzing the causal relationship between the compliance factors using 'Vensim' known as a System Dynamics tool.

3. Risk Assessment of Financial IS Compliance

3.1. Compliance Risk Identification

Figure 2 shows mapping results of the correlation on the security control areas of ISO 27001, KISA ISMS and FISS.

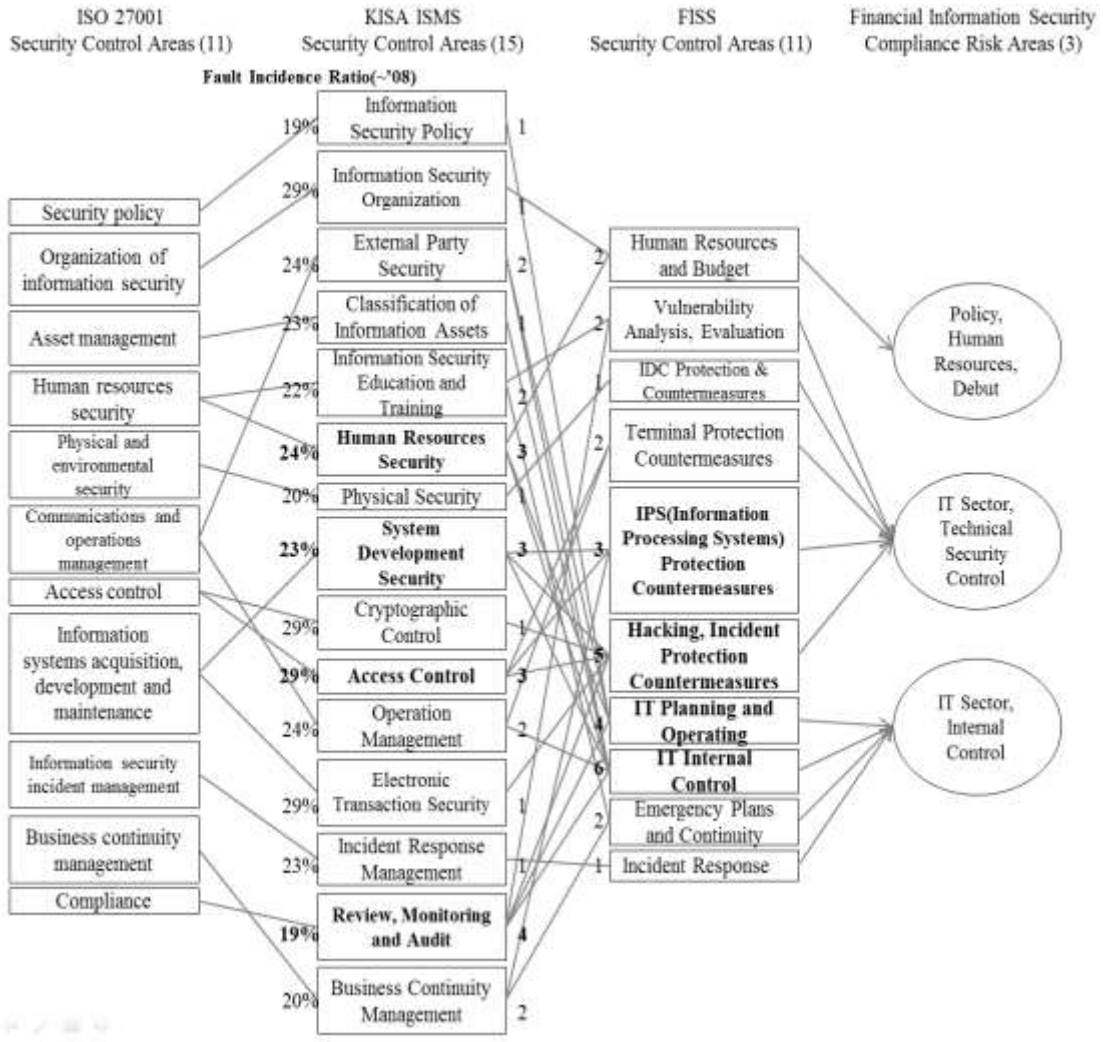

Figure 2. Mapping Results of Security Control Areas between ISO 27001, KISA ISMS and FISS

The results of correlation analysis of Figure 2 show that areas of 'Human Resources Security'(mapped into 3 pieces), 'System Development Security'(3), 'Access Control'(3), 'Review, Monitoring and Audit'(4) of KISA ISMS are more important than the rest, and areas of 'IPS Protection Countermeasures'(3), 'Hacking, Incident Protection Countermeasures'(5), 'IT Planning and Operating'(4) and 'IT Internal Control'(6) are more important than others in FISS.

Table 1 shows the results of analysis in which the defect cases of ISMS occurred before 2008 are reflected as basic data.

Table 1. Results in Estimating the Importance of Security Control Areas

Security Control Areas	Number of Relations (N)	Defect Ratio (%)	Importance	Order
Human Resources and Budget	2	26	52	5
Vulnerability Analysis, Evaluation	2	21	42	7
IDC Protection & Countermeasures	1	20	20	10
Terminal Protection Countermeasures	2	26	52	5
IPS(Information Processing Systems) Protection Countermeasures	3	23	69	4
Hacking, Incident Protection Countermeasures	**5**	**25**	**125**	**2**
IT Planning and Operating	**4**	**21**	**84**	**3**
IT Internal Control	**6**	**23**	**138**	**1**
Emergency Plans and Continuity	2	20	40	8
Incident Response	1	23	23	9
Total and Average	28	22.8	64.5	

3.2. Compliance Risk Assessment

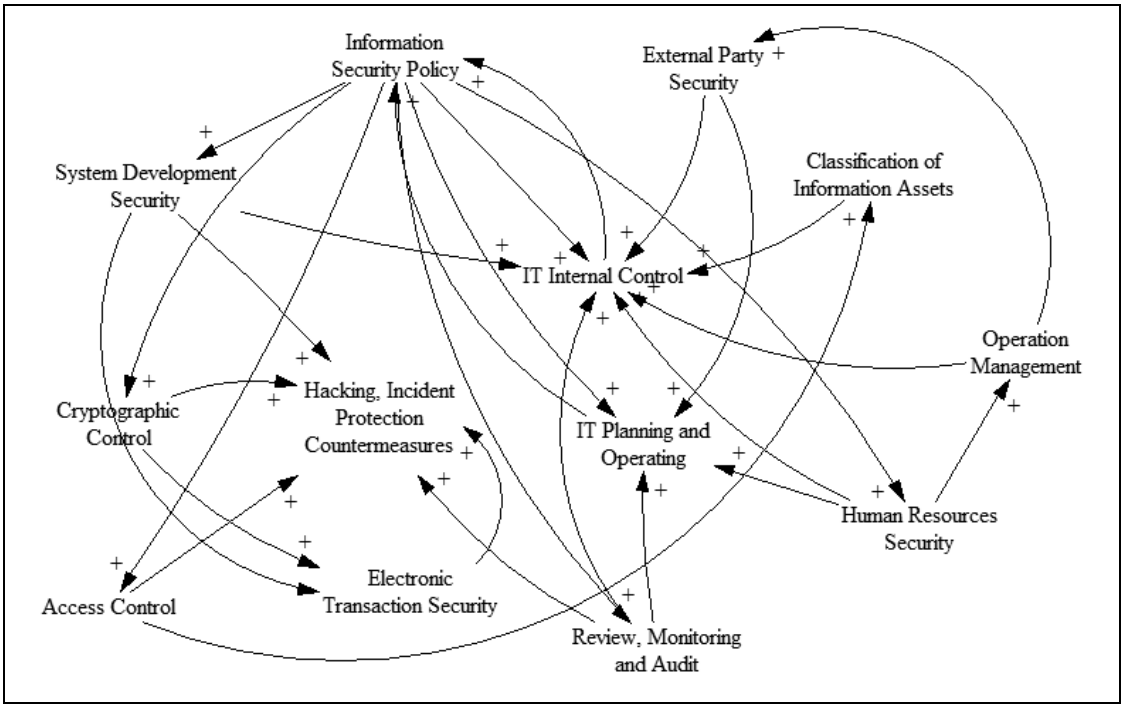

Figure 3. Correlation Analysis on the Security Control Areas (causal map)

The risk mitigation strategies for specific security control areas were established by means of correlation analysis through a causal map using system dynamics techniques, targeting 3 security control areas identified to be ranked first, second and third in importance with the highest relevance from the analysis results. Models in this study mainly show positive (+)

affects since they are designed not to take costs into consideration. In addition, Figure 4 shows the structural analysis results of the security control areas in Figure 2, 3.

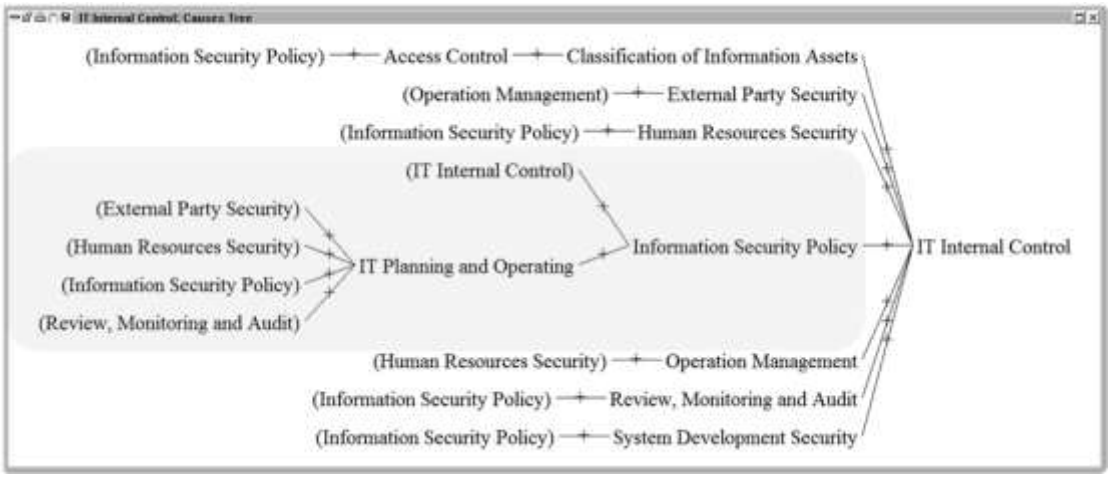

Figure 4. Causes Tree Structure: 'IT Internal Control' (ranked 1st)

From the analysis results of Figure 4, 'Information Security Policy' is found to be the cause that has the largest effect on 'IT Internal Control', and the analysis results of Figure 5 revealed that 'Access Control' area is the cause that has the largest effect on 'Hacking, Incident Protection Countermeasures'. From the analysis results of Figure 6, 'IT Planning and Operating' is identified to be affected most by 'Information Security Policy'.

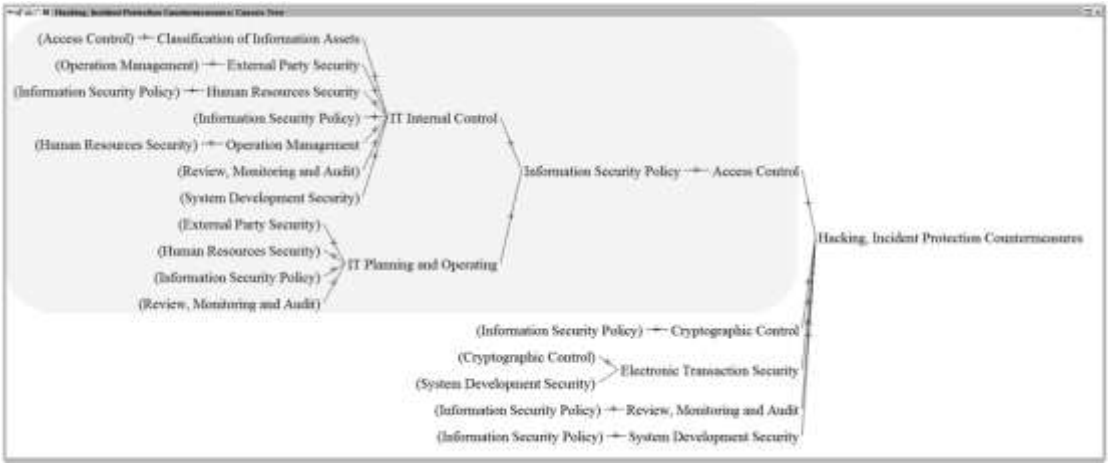

Figure 5. Causes Tree Structure:
'Hacking, Incident Protection Countermeasures' (ranked 2nd)

Figure 6. Causes Tree Structure: 'IT Planning and Operating' (ranked 3rd)

In this regard, the utilization of system dynamics techniques to strengthen the security measures of Access Control when costs are not considered helps to establish risk mitigation strategies by making complex causal relationship between the factors known intuitively. In this study, it is concluded from the case connected with FISS that security measures of 'Access Control' and 'Information Security Policy' should be strengthened.

3.3. Policy Assessment

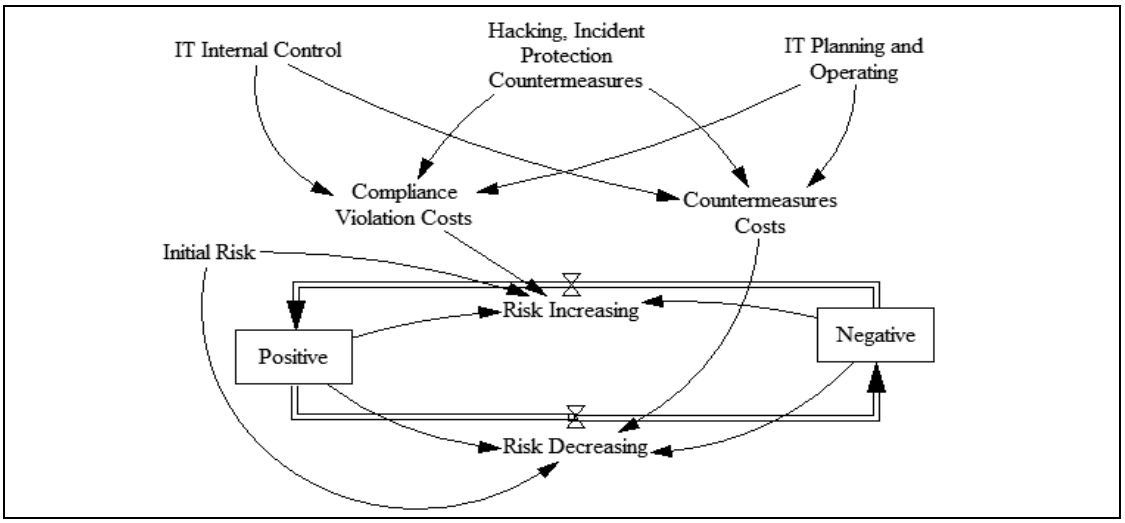

Figure 7. Simple Policy Assessment Analysis Model

Figure 7 illustrates the simple policy assessment analysis model to compare the policy each other. It can be used as correlation analysis between countermeasure costs and compliance violation costs that established by the three main security control areas. Each weight of security controls is on the basis of the defect ratio [2]; the value of results depends on the costs. However, this applied model in accordance with the security countermeasures does not reflect the variety costs. A simple cost-effectiveness analysis has limitations.

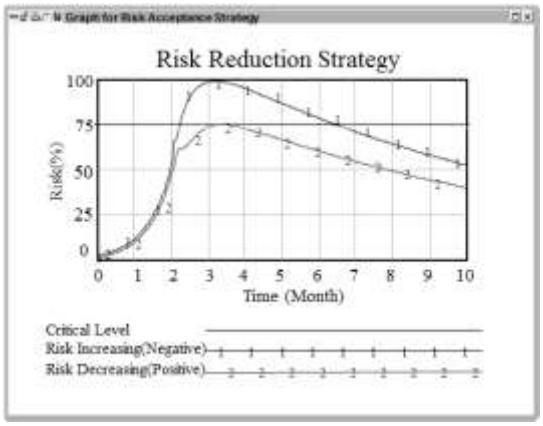

Figure 8. Graph for Risk Reduction Strategy

Figure 9. Graph for Risk Acceptance Strategy

From the analysis results of Figure 8, 9, when the critical level (75 Points) is reached, the risk for the common 'Risk Decreasing (Positive)' has shown a steady decline by the security countermeasures. In this model, the cycle of applied security countermeasures is about 10 months, the risk is found to coverage to 30 Points (%). Therefore, Depending on risk management strategy and 'Negative' selection, the transition of a risk indicator is a little different. In Figure 8 (Risk Reduction Strategy), the risk continuously decreased by applying security countermeasures, but the risk increased exponentially after 2 months, in Figure 9 (Risk Acceptance Strategy). In conclusion, financial companies should improving act three main security control areas (IT Internal Control, Hacking and Incident Protection Countermeasures, IT Planning and Operating) in an interval of at least 10 months continuously.

4. Conclusion and Future Work

We focus on compliance-oriented risk assessment of financial companies. Basic-data used to implement the analysis was based on the defect cases before 2008 found in KISA ISMS certification of private institutions. If this study is carried out based on the recent IT audit result data on the financial companies, more significant results will be deduced. However, this study has its significance in that we propose the new risk assessment methods specialized for financial companies through attempting to integrate different information security standards. Therefore, The FSS will perform to audit depending on the compliance assessment results. Additionally, Security managers and executives of financial companies will strive to comply with information security from high-risk portions depending on the situations of each organization.

In the future, it is required to research GRC (Governance, Risk Management and Compliance) integration and execution methods of [10] as extended models through specifying the previously presented causal relationship-centered risk assessment measures into the case studies on the financial company's risk management practices considering the cost.

Acknowledgments

This work is supported by the Korea Information Security Agency (H2101-12-1001).

References

[1] J. S. Kim, S. Y. Lee and J. I. Lim, "Comparison of the ISMS Difference for Private and Public Sector", Journal of the Korea Institute of Information Security and Cryptology, vol. 20, no. 2, **(2010).**

[2] H. M. Ko, J. S. Kim and S. S. Jang, "Analysis on a case study of the defects that appear typically build upon Information Security Management System (ISMS)", Korea Information Security Journal, vol. 17, no. 4, **(2007).**

[3] Electronic Financial Transaction (EFT) Act, Korea, **(2012).**

[4] Electronic Financial Transaction (EFT) Supervision and Regulations, Financial Supervisory Service, Korea, **(2011).**

[5] Act on Promotion of Information and Communications Network Utilization and Information Protection (ICI), Korea, **(2012).**

[6] JTC 1/SC 27 IT Security Techniques, "Standards for the establishment, implementation, control and improvement of the Information Security Management System", ISO/IEC 27001, Geneva, **(2005).**

[7] JTC 1/SC 27 IT Security Techniques, "Code of the practice providing good practice advice on ISMS", ISO/IEC 27002, Geneva, **(2005).**

[8] NIST, "Risk Management Guideline for Information Technology Systems", NIST Special Publication 800-39, Rev. 3, Gaithersburg, National Institute of Standards and Technology, **(2011).**

[9] W. Boehmer, "Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001", Proceedings of the 2009 International Conference on Availability, Reliability and Security (ARES), **(2009)** March 16-19, Fukuoka, Japan.

[10] D. Cheremushkin, N. Andreeva and S. Shustikov, "Information Security Integral Engineering Technique and its Application in ISMS Design", Proceedings of the 2011 International Conference on Availability, Reliability and Security (ARES), **(2011)** August 22-26, Vienna, Austria.

Authors

Ae Chan Kim

He is a Masters Course Student at Graduate School of Information Security (GSIS) in Korea University. He received B.S degree in Industrial and Information Systems Engineering from Seoul National University of Science and Technology (Seoultech) in 2009. He served as Intelligence and Communication Officer, 1LT in the Republic of Korea Army (ROKA) from 2009 to 2011. His current interests are Financial Information Security, IT Auditing Techniques and Hacking/Virus.

Su Mi Lee

She is a Team Leader at Financial Security Agency (FSA) in Korea. She received M.S. and Ph.D. degrees in Information Security at Graduate School of Information Security (GSIS) from Korea University in 2003, 2007 respectively. Since 2007, she has been a Researcher at FSA. Her current interests are Financial Information Security, Encryption Protocols and Information Security Evaluation.

Dong Hoon Lee

He is a Full Professor and Vice President at Graduate School of Information Security (GSIS). He received B.S degree in Economics from Korea University in 1983 and his M.S. and Ph. D. degrees in Computer Science from University of Oklahoma in 1987, 1992 respectively. He worked as Assistant Professor at Department of Computer Science in Korea University from 1993 to 1997. Also, he worked as Associate Professor at Department of Computer Science in Korea University from 1997 to 2001. Since 2001, he has been a Full Professor at GSIS in Korea University. His research interests include Encryption Protocol, Cryptology and Embedded Security.