Advanced Information Security Management Evaluation System

Heasuk Jo[1], Seungjoo Kim[2] and Dongho Won[3*]
[1]Authentication Service Division, Financial Security Agency,
36-1, Yoido-Dong, Youngdeungpo-Gu, Seoul, Korea
[e-mail: hsjo@fsa.or.kr]
[2]CIST (Center for Information Security Technologies), Korea University
Anam-dong, Seongbuk-gu, Seoul 136-713, Korea
[e-mail: skim71@korea.ac.kr]
[3]Information Security Group,
School of Information and Communication Engineering, Sungkyunkwan University,
300 Cheoncheon-dong, Jangan-gu, Suwon, Gyeonggi-do 440-746, Korea
[e-mail: dhwon@security.re.kr]
*Corresponding author: Dongho Won

Received January 19, 2011; revised April 19, 2011; accepted May 29, 2011; published June 28, 2011

Abstract

Information security management systems (ISMSs) are used to manage information about their customers and themselves by governments or business organizations following advances in e-commerce, open networks, mobile networks, and Internet banking. This paper explains the existing ISMSs and presents a comparative analysis. The discussion deals with different types of ISMSs. We addressed issues within the existing ISMSs via analysis. Based on these analyses, then we proposes the development of an information security management evaluation system (ISMES). The method can be applied by a self-evaluation of the organization and an evaluation of the organization by the evaluation committee. The contribution of this study enables an organization to refer to and improve its information security levels. The case study can also provide a business organization with an easy method to build ISMS and the reduce cost of information security evaluation.

Keywords: Information security management systems (ISMSs), information security evaluation, information security check, information security evaluation process.

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the "ITRC" support program supervised by the NIPA(National IT Industry Promotion Agency) (NIPA-2011-C1090-1001-0004).

DOI: 10.3837/tiis.2011.06.006

1. Introduction

Information security is an important issue in that it protects information systems from increasing levels of internal/external threats in information intensive businesses. An organization's fate depends on the levels of information technology and information protection that it possesses. For the effective management of information security in an organization, Information Security Management Systems (ISMSs) have been developed. ISMSs are capable of coping with a variety of security problems. Furthermore, these systems can also manage and operate continuous information security on the technology, management, and hardware of information systems, maintaining the most important characteristics of a secure system: confidentiality, integrity, and availability [1].

There are a number of ISMSs with related guidelines, such as the BS7799 [2][3][4][5] of England, the Common Criteria [6][7] international standard, the ISMS [8] of Korea, the DITSCAP [9][10], the Trusted Computer System Evaluation Criteria (TCSEC) [12] and the DIACAP [11][13][14] for the USA, the IT Security Evaluation Criteria (ITSEC) [15], and the IT Baseline Protection Manual [16][17][18][19] in Germany. England developed a security system for domestic use, the BS7799; however, in 2005, this system was adopted as an international standard (ISO/IEC 2700x) [5][20][21]. Systems approved using these standards are considered to be the best, most successful security management systems in terms of their best internal and external control.

However, in terms of information security evaluations of organizations with different sizes, characteristics, main business processes and assets, it is not sufficient to using only one criterion. Furthermore, the material needs protecting and the method of information protection differ according to the organization. Simply put, ISMSs have been developed by different users for various, distinct goals. For example, the ISMS of Korea, the IT baseline protection Manual of Germany, and the DITSCAP of the United State emphasize the terms of the information security technology; however, these systems are not well equipped to handle the management of information security. Conversely, England's BS7799 emphasizes information security management over the aforementioned issues. Moreover, in Korea, the ISMS based on the BS7799, ISCS, and CIIP lacks an organic, leading to issues including overlapping applications, increasing costs, and decreasing organizational and operational efficiency. Thus, an organization should specifically apply various ISMSs and guidelines in order to achieve the desired information security characteristics.

In this paper, the goal of this study is to develop an information security management evaluation system (ISMES) for governments or organizations through the integration and improvement of various existing various ISMSs. The ISMES can help to effectively manage and evaluate organizational systems, thus reducing cost. In addition, this research developed tools to help a government or organization apply the proper ISMS to improve their business and information security levels. Moreover, this study can be used as a guideline to develop new ISMSs for individual businesses. This paper is expanded and revised based on [38][43], and [44].

An organization of this paper is as follows. Section 2 outlines information security management systems. Section 3 proposes the information security management evaluation system. Section 4 presents ISMES evaluation which consists of verification of ISMES. Finally, this paper concludes in Section 5.

2. Related Work

The best-known ISMSs are the international standards BS7799/ISO17799 [2][3][4][5], Common Criteria (CC) [6][7], and ITSEC [15]. Some nations use their own ISMS, e.g., ISMS [26] of Korea, Information Security Check Service (ISCS) of Korea, Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP) [11] of USA, Defense Information Assurance Certification and Accreditation Process (DIACAP) [13] of USA, IT Baseline Protection Manual (ITBPM) [16] of Germany, ISMS [22] of Japan, Trusted Computer System Evaluation Criteria (TCSEC) [12] of USA.

Table 1. The certification structure comparison of the ISMSs

	BS7799	CC	ITSEC	ISMS
Operation Area	England	About 25 countries	European countries	Korea
Basic Structure	· 6 Management phases · 11 Security domains · 139 Control objectives · 133 Security controls	· 3 Parts · 11 Security functional requirements · 8 Assurance requirements	· 4 Phases · 6 Levels	· 5 Phases · 14 Management requirements · 137 Control objectives
Management Process	1.Define policy 2.Define scope 3.Assess risk 4.Manage risk 5.Selet controls to be implemented and applied 6.Prepare a statement of applicability	1. PP/ST introduction 2. Conformance claims 3. Security problem definition 4. Security objectives 5. Extended components definition 6. Security requirements 7. TOE summary specification	1. Requirements 2.Architectural Design 3. Detailed Design 4. Implementation	1.Establishment of information security policy 2.Range set of management system 3.Risk Management 4.Implementation 5.Post Management
Difference of Process	· Emphasis on managerial security	· Emphasis on technical security	· Emphasis on managerial security	· Emphasis on technical security
Specification Control Point	· Provide best code of practice for information security management	· Provide common set of require ments for the security functionality of IT products	· Provide common set of requirements for the security functionality of IT products	· Provide prevention and measurement against leak and damage of assets
Evaluation Method	· Use the PDAC model cycle	· Follow each certification evaluation procedure	· Follow commission of European communities	· Follow each certification evaluation procedure

Table 2. The certification structure comparison of the ISMSs

	ITBPM	DITSCAP	DIACAP	TCSEC
Operation Area	Germany	USA	USA	USA
Basic Structure	· 8 Steps · 62 Modules	· 4 Management Phases · 16 Control objectives · 39 Service units	· 5 Phases, 8 Subjects · 157 Information assurance controls	· 4 Divisions · 7 Classes
Management Process	1.Assess protection requirements 2.Security concept 3.Check basic security level 4.Define changeable checklists 5.Check reasonable level of protection	1.Definition 2.Verification 3.Validation 4.Accreditation	1. Initiate and plan IA C&A 2. Implement and validate assigned IA controls 3. Make certification determination & accreditation decisions 4.Maintain authority to operate and conduct review	1. Proposal review 2. Vender assistance 3. Design analysis 4. Rating Maintenance

	6. Identify implementation 7. Self-certification		5. Decommission	
Difference of Process	· Emphasis on technical security	· Emphasis on technical security	· Emphasis on automated support DoD interim guidance	· Emphasis on technical security
Specification Control Point	· Provide correspondence method with IT infrastructure and modules	· Protect information system and defense information infrastructure	· Provide standard DoD Automated Tool	· Protect computer operating system
Evaluation Method	· Permitted auditor by BSI certify	· Follow C&A process	· Follow C&A process	· Follow each certification evaluation procedure

Tables 1 and **2** illustrate the certification structure comparison of the ISMSs. Each standard has some problems based on the analysis and compare. BS7799 in England has not a way of pre-evaluation about assets and even though lays emphasis on the managerial security than DITSCAP, lacks emphasis on the technical security, and it also lacks mutual exchange than DITSCAP. Although DITSCAP can do mutual exchange by SSAA, it is too big documentation without its appendices. Furthermore it is a very detailed document, much of the data in the document is hardcopy format to maintain. For this reason, DIACAP solved heavy workload by automated tool. DIACAP, CC and ITSEC limited to reliable evaluate information technology products and systems, and even though lay emphasis on the technical security, lacks emphasis on the managerial security than BS7799. Moreover these systems are limited that are not all including information security management of organization. ISMS in Korea has not a way of pre-evaluation about assets and even though lays emphasis on the technical security than BS7799, lacks emphasis on the technical security than DITSCAP. And it lacks mutual exchange between an organization and an evaluation committee than DITSCAP.

3. Proposed Information Security Management Evaluation System

The goal of this study is to develop ISMES. This is difficult, because different organizations have varying sizes, characteristics, main business processes and assets; therefore, we could not use only one criterion. Furthermore, the materials that need to be protected may differ from that specified in the information protection method. Therefore, the objectives of this study are evaluation methodology and a management process for the information security evaluation levels using a checklist. We apply weights according to the information assets and value of an organization and decide on the level of target evaluation using a summation of the weights. Then, an organization is evaluated using a proposed checklist so as to overcome the weaknesses of the ISMS.

3.1 ISMES Process

This section briefly shows the management process of the ISMES before establishing a classification standard. This process can be evaluated by the organization itself and the evaluation committee. In the case of self-evaluation, the chief information officer or senior agency information security officer replaces the role of the evaluation committee.

The first step prepares the evaluation. In this step, the target level of an organization is decided. The objective of this step is to establish a suitable evaluation standard before the evaluation. The target level is the ultimate goal to be accomplished by the organization. This phase is the pre-evaluation about an organization's assets based on four categories: personal criterion, organizational reliance on hardware/software systems, organizational reliance on

network systems, and priority of handling information. Each evaluation item, hereafter Target Checklist (TC) has weight value between 1 to 3. The target level is calculated by quantitative and qualitative analysis. The factors excluded in the quantitative analysis can be added by qualitative analysis. Subsection 3.2 explains this.

The second step, problem definition phase, is defining a basis for information security evaluation of the organization. The main activities in this step are the acquisition of information necessary for information security evaluation, planning activities of evaluation and admission, making a pre-analysis documentation for information security evaluation. Collected information is described in the pre-analysis documentation; this documentation is adjusted and complemented in the entire phase of ISMS. That is, this documentation has all the information about the target. The objective of this step is to grasp the environment of the evaluating target and to define security requirements necessary for it before evaluating the target organization.

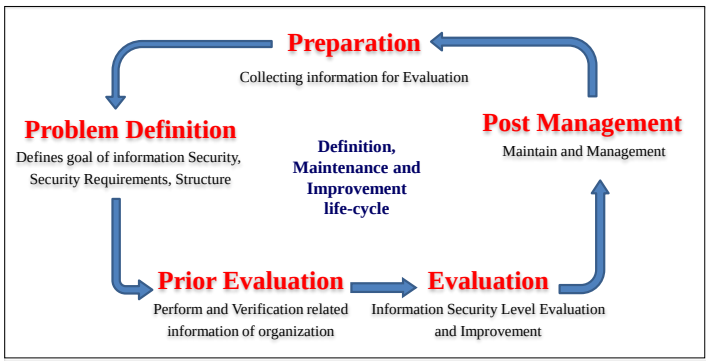

Fig. 1. Management process of ISMES

The third step, prior evaluation phase, is a series of processes of evaluating the target organization based on the pre-analysis documentation made in the previous phase. The objective of this phase, which is the early evaluation phase, is to analyze the current information security method compared to the required information security target level. The pre-analysis documentation can be adjusted via this process.

The fourth step, evaluation phase, is the actual evaluation of the information security level. In this phase, the organization is evaluated using a suitable standard based on the target level decided in the first phase. They reveal encountered risks and establish response activities to resolve them by conducting this phase. This phase evaluates the current level of information security using the evaluation checklist (EC) and pre-analysis documentation. If the information security current level of the target satisfies the target level described in the pre-analysis documentation, we can progress their process. Otherwise, we make a list of risks based on unsatisfactory items in the information security EC and eliminate risks using this. Subsection 3.3 explains this.

The last step, the post management phase, defines the procedures and methods to maintain and manage the information security level. These processes should check changes in the maintenance and management of the information security level, if changes occur; it should reveal problems and improve the procedures. This phase exists to respond to management system changes or an annual revaluation.

3.2 Information Security Management Evaluation

This subsection focuses on the standard developed to aid in organizations' target level evaluations in the preparation phases. The target level is decided using a TC (See **Table 6**). Evaluating the target level is conducted using quantitative and qualitative analysis.

Table 3. Grades of target level for self-evaluation

Target Level	Characteristic	Score Range	Score Range (%)
A	Very High Level	46 ~ 54	85% ~ 100%
B	High Level	37 ~ 45	69% ~ 84%
C	Medium Level	28 ~ 36	52% ~ 68%
D	Low Level	24 ~ 27	44% ~ 51%
E	Very Low Level	18 ~ 23	33% ~ 43%

The evaluated target level represents the ultimate goal when evaluates an organization's information security current level, for which there are two methods. One is a self-evaluation of the organization and the other is an evaluation of organization by evaluation committee. For the first method, after checking the TC, the target level is categorized into five levels (See **Table 3**). Each TC has three checklists, Low, Medium, and High, according to the importance of the information of the organization. Thus, even if a small organization were to handle a lot of personal information, the level of an organization should be measured much higher. The classifications are explained in [23][24][25][26][27][28]. The organization's target level is classified according to its total summed score and is five levels from level A to E. The very high level indicates extreme potential damage to a business in the event of asset damage; the medium level would result in a decreased efficiency of the business; the very low level would cause minor damage to the business; the high and low level are between the sides level. The total score is calculated by the summing the scores of each TC, with 54 being the highest possible score. The classifications of the score range refers to [34].

Table 4. Suggested questionnaire layout for factor comparisons

Checklist	Absolute	Very Strong	Strong	Weak	Equal	Weak	Strong	Very Strong	Absolute	Checklist
	9	**7**	**5**	**3**	**1**	**3**	**5**	**7**	**9**	
I-1							x			I-2
I-1		x								I-3
I-2			x							I-3
II-1		x								II-2
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

The second method is an evaluation methodology that is applied by the evaluation committee. This is a statistical method using AHP, K-means clustering, and SVM. Analytic Hierarchy Process (AHP) sets a weight of the TC. K-means clustering sets five target levels. Support vector machine (SVM) sets classification of an organization. Unlike self-evaluation of organization, evaluation committees can generate more reliable score range because they have much more information of several organizations and have many evaluation experts.

Table 5.Training data for SVM

No.	D1	D2	D3	D4	T_L
1	3	7	5	20	D
2	5	11	6	17	B

3	3	13	5	23	B
⋮	⋮	⋮	⋮	⋮	⋮

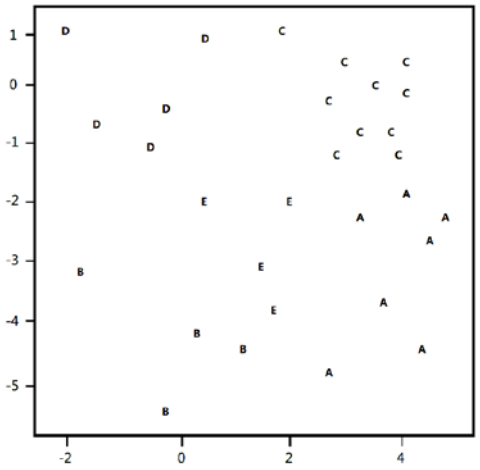

Fig. 1. K-means clustering result for organization's score set

For example, evaluation experts of evaluation committee determine a weight of the TC by AHP which is a structured technique for dealing with complex decisions. AHP systematically evaluates its various elements by comparing them to one another two at a time. **Table 4** is example of suggested questionnaire layout for TC comparisons. The evaluation experts should mark preference of either side to assess. In the **Table 4**, "Checklist" is TC's sub-category No. Then, an evaluation committee selects data components of organizations (needs a minimum of 30 organizations). Using K-means clustering, 30 organizations are divided into five target levels by total score of multiplying each TC score by a weight. **Fig. 2** shows K-means clustering result of the distribution of the total scores of the organizations in the statistical program SPSS. For the classification of target level, SVMs are a useful technique for data classification and a set of related supervised learning methods that analyze data and recognize patterns, used for classification and regression analysis [32][33]. SVM's input data for machine training is the total scores of organizations. Once SVM is analysis, the result of machine training describe a formula for classification. Thus, target level is calculated using the formula from the total score of new organization.

Table 5 is the input data D1~D4, and T_L which is TC's categories and target level from level A to E. Therefore, SVM is classifiable a target level based on D1 to D4 of input data.

Table 6 illustrates the TC used to evaluate the target level of the organization. The TC was thus designed by referencing and improving several [23][24][25][26][27][28][35][36][37].

Table 6. Checklist for target level evaluation of organization

Category	*Scoring: Low = 1, Medium = 2, or High = 3*			Score
I	Personal Criterion			
I-1	Number of Employees 1. Less than 100 employees	2. 100 to 300 employees	3. More than 300 employees	
I-2	Full Time Employee Ratio 1. Below 40%	2. Below 85%	3. More than 85%	
I-3	Inspector Ratio			

	1. Below 0.5% of employees 2. Below 2.5% 3. More than 2.5%	
II	Organizational Reliance on Hardware/Software Systems	
II-1	Dependence on Information System in Office Environment 1. A part rely on (process for personal and financial affairs in LAN environment) 2. Some part rely on (process of internal business to use mainly PC in independent PC environment) 3. Most part rely on (process of information at various levels with agencies through external network)	
II-2	Influences on Computer System Damage 1. Below 25% on the business 2. Below 75% 3. More than 75%	
II-3	Influences on Software Error 1. Below 25% on the business 2. Below 75% 3. More than 75%	
II-4	Influences on the Internal IT System in the Event of a Failure of External IT System 1. Damage ratio about 25% on the business (most of the business be damaged) 2. Damage of the only part of the related IT work 3. Connection with external system as occasion demands	
II-5	Backup Ratio of Sensitive Information 1. Below 50% of information 2. Below 75% 3. More than 75%	
III	Organizational Reliance on Network Systems	
III-1	Influences on the Task of Network Equipment 1. Below 25% on the business 2. Below 75% 3. More than 75%	
III-2	Ratio of Network Equipment (Router, Hub, Switch, Server, etc.) 1. Below 25% of total network equipment 2. Below 75% of total network equipment 3. More than 75% of total network equipment	
IV	Priority of Handling Information	
IV-1	Existence of Branch Office in Internal or External 1. Below one in Internal or External 2. Below three 3. More than three	
IV-2	Restricted Area Ratio 1. Below 25% 2. Below 75 3. More than 75%	
IV-3	Influences on Leaking Information 1. Below 25% on the business 2. Below 75% 3. More than 75%	
IV-4	Level of Handling Personal Information of the Organization 1. Anonymity assurance of online information (Homepage address, IP address, etc.) 2. Personal information (Name, Company name, Cell phone number, Telephone number, Address, Email address, etc.) 3. High level – personal financial information (Credit card numbers, account number, Social security number, Driver' s license number, etc.)	
IV-5	Dependency on Multi-site Operations 1. Little impact 2. Some impact 3. Significant impact	
IV-6	Plan for Multi-site Operations 1. Little impact 2. Some impact 3. Significant impact	
IV-7	Level of Retaining Information of Other Organizations 1. Release of the information, such as homepage and IP address, telephone number, etc. 2. Release of the information, such as annual salary, personnel plans, etc. 3. Main business information, such as original technology, business main plans, etc.	
IV-8	Influences on National Society or Economy by Leaking Information 1. Below 25% on the business 2. Below 75% 3. More than 75%	

3.3 Current Level Evaluation of Organization

This subsection details a standard for actual evaluation of information security management current levels (ISMCL). The ISMCL is determined using an EC, Appendix A-C. The ultimate goal of an organization is to have the ISMCL implement all points in the EC for safe information security management. The EC consists of three categories: managerial, technical, and physical security. Each is composed of detailed checklist items for a total of 208 items. Each EC is divided into five scoring (See **Table 7**). The scoring is dependent on the

implementation of each EC in an organization.

Table 7. Scoring of each evaluation checklist

Scoring	Implementation of Evaluation Checklist
0	Not Implemented: EC is not implemented and not existed
1	Planning Stages: EC is planning states
2	Partially Implemented: EC is partially implemented
3	Close to Completion: EC is existed and implemented but not perfectly implemented
4	Perfectly Implemented: EC is perfectly implemented

The EC is then designed to evaluate current information management system using the references and standards of [3][14][24][29][30][31][36][37][38]. Moreover the EC includes standards of ISO 27001 and ISMS of Korea, and it has been completed by add of security items and modification these references to enable an organization to increase security.

Similar to evaluation of the target level, evaluation of the ISMCL have two methods that are self-evaluation of the organization and evaluation of the organization by an evaluation committee. **Table 8** reflects the subtotal score of each category in the evaluation checklist and the total score for the entire category. For the first method, after checking the EC, the total scores are divided into three levels, ISMCL, according to the target level through a previously obtained pre-analysis: poor, needs improvement, and good (See **Table 9**). The classification refers to [34].

Table 8. Scoring of evaluation checklist

Category of Checklist	Score Range
Managerial Security	0 ~ 416
Technical Security	0 ~ 308
Physical Security	0 ~ 108
Total Score	0 ~ 832

The method is a statistical method using AHP. The evaluators in the evaluation committee determine a weight in a scale from equal, weak, strong, very strong, and absolute so that all EC comparisons are greater than or equal to one. The evaluators classify the selected data components (the used data components of the organizations in the target level) into three parts using the existing ISMS. The three parts are approve or good, needs improvement, and poor in information security management. Then, they calculate overall score of multiplying each EC score by a weight. They calculate the average of each overall score in the same target levels. The score range's boundary value in ISMCL is the average on both sides of each part's average score.

The following shows an application example of ISMES for self-evaluation by an organization. The organization (denoted as "XYZ") should comply with the management process of the ISMES that consists of 5 steps. In the preparation phase, XYZ collects basic information for target level evaluation and then the target level is determined using a target checklist that consists of personal criterion, organization reliance on hardware/software systems, organization reliance on network systems, and priority of handling information (See subsection 3.2). For the target level evaluation, after checking the TC, the target level is calculated by the weight of the selected evaluation item. If the overall score is 39, the target level is at level 'B', High level (See **Table 3**). XYZ defines security requirements and detailed information necessary for the evaluation in the problem definition phase. The collected

information is described in the pre-analysis documentation. In the previous evaluation phase, XYZ analyzes the current information security method compared to the required information security target level. In the evaluation phase, XYZ evaluates the current level using the EC. In this phase, if the total score of the current level is 532, 63%, which is the "Needs improvement" based on target level 'B', XYZ should be upgraded to "Good" by removing risk. Finally, in the post management phase, XYZ operates and manages the management system to maintain the current level.

Table 9. Scoring based on target level

Target Level	Score Range	Overall Evaluation	Target Level	Score Range	Overall Evaluation
A	0% ~ 60%	Poor	D	0% ~ 37%	Poor
	61% ~ 82%	Needs Improvement		38% ~ 60%	Needs Improvement
	83% ~ 100%	Good		61% ~ 100%	Good
B	0% ~ 52%	Poor	E	0% ~ 30%	Poor
	53% ~ 74%	Needs Improvement		31% ~ 52%	Needs Improvement
	75% ~ 100%	Good		53% ~ 100%	Good
C	0% ~ 45%	Poor			
	46% ~ 67%	Needs Improvement			
	68% ~ 100%	Good			

4. ISMES Evaluation

This section shows evaluation of the ISMES using the vulnerability/threat lists from 2007 to 2010. The verification method of the ISMES evaluation is a process in which each vulnerability/threat is listed so that organizations are aware if the issues to avoid and then an organization can keep safety by evaluation checklist in ISMES to prevent the vulnerability/ threat lists. Furthermore we analyze the major vulnerability/threats to information security management by arranging the threats in order of frequency. Finally, it explains the expected effects using the evaluation results and a comparison of ISMSs.

Business information security vulnerability was reported by KISA each year from 2007 to 2009 through a survey of about 50 companies which applied for ISMS re-evaluation or ISMS evaluation [39]. **Table 10** shows the vulnerability lists as well as an available EC of ISMES to prevent the listed vulnerability. In spite of the completed ISMS assessment by KISA, the listed vulnerabilities still exist in the organizations which are vulnerable to threats. In other words, the applied ISMS has its own flaws. Though KISA's ISMS has its own checklists against vulnerabilities, organizations do not adequately perform evaluations. However, the proposed ISMES is more secure. To prevent an organization from missing an item on the security checklist, ISMES requires a double check by necessity. For example, in the case of the first vulnerability item of 2009, KISA's ISMS does not check administrator account; however, use of the ISMES will detect the missing security through 2.2.8, 2.3.1, 2.3.2, and 2.3.3. In tables **Table 10**, No. is the number of cases of vulnerable organizations, Rate is the total percentage of the vulnerable organization, and C_ISMES is the EC which can be reviewed by the ISMES.

Table 10. Information security management vulnerability Top 10

Top10	2007, Information Security Management Vulnerability	No.	Rate	C_ISMES
1	Undefined target, cycle, and way of backup	16	40%	3.3.1, 3.3.2
2	Lacking or no procedures about an information assets classification	15	37%	1.3.1, 1.3.2
3	Insufficient management of an administrator account	12	30%	2.2.8, 2.3.1, 2.3.2, 2.3.3
4	Insufficient management of an assets change process	10	25%	1.1.1, 1.3.1, 1.3.2

5	Lack of definition, prevention, and response procedure of security accident	9	22%	1.6.1, 1.6.2
6	No implementation or no plan of information security education	9	22%	1.4.1, 1.4.3, 1.6.4
7	Undefined physical security boundary	8	20%	3.1.1, 3.3.1, 3.3.2
8	Omission or insufficient of vulnerability/threat analysis about major information assets	7	17%	1.1.1, 1.3.1, 1.3.2,1.6.7, 2.2.2, 2.2.4, 2.2.5, 3.2.1
9	No internal audit policy and no regular audit of security activities	7	17%	1.6.6, 2.3.1, 2.3.2, 2.3.3
10	No demand contract for information leakage prevention	7	17%	1.4.2
Top10	**2008, Information Security Management Vulnerability**	**No.**	**Rate**	**C_ISMES**
1	Lacking or no procedures about an information assets classification	20	34%	1.3.1, 1.3.2
2	No management procedure of user account and joint use of an administrator account	18	31%	1.4.1, 2.1.2, 2.2.8,2.3.1, 2.3.2, 2.3.3
3	No procedure of creation/change/delete about main information (password, social security number, etc)	15	25%	1.5.1
4	Undefined target, cycle, and way of backup, Insufficient management of an assets change process	13	22%	3.3.1, 3.3.2, 1.4.1, 1.3.2
5	Omission or insufficient of vulnerability/threat analysis about major information assets	13	22%	1.1.1, 1.6.7, 1.3.1,1.3.2, 2.2.2, 2.2.4, 2.2.5, 3.3.1
6	No internal audit policy and no regular audit of security activities	11	18%	1.6.6, 2.3.3
7	Insufficient management of a password or an administrator account	11	18%	2.2.8, 2.3.1, 2.3.2, 2.3.3
8	Undefined physical security boundary	11	18%	3.1.1, 3.2.1, 3.2.2
9	Lack of regular review about efficiency and propriety of ISMS according to organization's environment changes	10	17%	1.1.1
10	Lack of definition, prevention, and response procedure of security accident	9	15%	1.6.1, 1.6.2
Top10	**2009, Information Security Management Vulnerability**	**No.**	**Rate**	**C_ISMES**
1	Insufficient management of a password or an administrator account	14	28%	2.2.8, 2.3.1, 2.3.2, 2.3.3
2	Lack of legal requirements observance of personal information security	13	26%	1.1.1
3	Lack of implementation about a result of internal audit	12	24%	1.1.1
4	Unclear responsibilities and roles of information security	11	22%	1.2.3, 1.2.2, 1.5.1
5	No regular inspection of access rights of user	11	22%	2.3.1, 2.3.2
6	Lack of measures for main network protection	11	22%	1.5.1, 1.6.1, 1.6.2,2.2.3, 2.2.4, 2.2.1
7	Insufficient management of an assets change process	10	20%	1.1.1, 1.3.1, 1.3.2
8	No backup plan or guide	10	20%	3.3.1, 3.3.2
9	Lack of policy review of access control in information security system	10	20%	2.2.1 ~ 2.2.8
10	Lack of definition, prevention, and response procedure of security accident	10	20%	1.6.1, 1.6.2

Table 11 was created by the CISSP forum and the ISO27k implementers' forum [41]. It shows the top information security threats, vulnerabilities, and the available ECs of the ISMES which can be used to prevent the listed vulnerabilities.

Table 11. Top Information security threats for 2008

Top10	2008, Information Security Threats	C_ISMES
1	Imposition of legal and regulatory obligation	1.1.1
2	Organized crime or terrorist groups using identity theft and other forms of compromise or extortion to finance or support criminal activities	2.1.1, 2.1.2, 2.2.4, 2.2.5, 2.2.6
3	Cyber-criminals, either skilled Black hats themselves or able to direct or pay others to do their bidding	1.4.3, 1.5.1, 1.6.1, 1.6.2
4	Malware authors responsible for viruses, worms, Trojans (particularly key loggers)	2.4.1, 1.5.1
5	Phishers including spear phishers targeting individuals with carefully crafted attacks	1.4.1, 1.4.3, 1.5.1
6	Spammers and other obnoxious, self-serving marketers wasting network bandwidth and filling our inboxes with junk, using their botnets and malware	1.4.1, 1.4.3, 1.5.1
7	Negligent staff such as programmers, technical architects, testers and project managers	1.4.1, 1.4.3
8	Storms, tornados, floods - Acts of God or intentional acts	3.1.1, 3.1.3
9	Fraudsters who simply use IT whilst exploiting control weakness in the IT-enabled business process, etc.	2.2.1, 2.2.7, 2.2.8, 2.3.1
10	Hackers, ranging from evil Black Hats down to naive and curious Grey or White Hats	1.4.1, 1.4.2
11	Unethical competitors or foreign powers targeting commercial and national secrets through espionage, social engineering, physical/network penetration, phishing and/or malware	1.4.2, 1.4.4
12	Disgruntled/untrained/ignorant employees who make genuine if nave human errors, misuse/misconfigure system security function, or ignore security policies and good practices	1.4.1, 1.4.3
13	Saboteurs who destroy, or threaten to destroy, information assets or who deny access to same	1.6.7, 2.4.1

14	Unauthorized access to, or modification or disclosure of, information assets (hardware, software, data, information)	2.3.1, 2.3.2, 2.3.3, 3.3.2
15	Nation states with advanced information warfare capabilities attacking critical information infrastructures to cause disruption or denial of service	2.1.2, 2.3.3
16	Technical advances such as quantum computing	1.6.1, 1.6.2
Top10	**2008, Information Security vulnerabilities**	**C_ISMES**
1	Software bugs and design flaws, particularly those in mass-market software	2.2.3, 2.4.1
2	Complexity in IT, including "bloatware" and "richness" generally (modern, general purpose computers and internets are BAD for security)	1.4.1
3	Inadequate investment in appropriate information security controls, at least partly due to the apparent disconnect between solid information security and commercial success	1.1.2, 3.1.3, 3.3.1
4	Insufficient attention to human factors in systems design and implementation, including cognitive biases and "laziness"	1.4.3
5	Unwarranted confidence in inherently flawed or missing security controls, including both a general lack of awareness of the items in these lists and dependence on compliance certificates resulting from incompetent or fraudulent audits	1.4.1
6	"Management" who, in the main, still just doesn't get information security and insists that it be buried deep out of sight, out of mind in the bowels of IT	1.1.2, 3.1.3, 3.3.1
7	Ignorance, carelessness, negligence or idle curiosity by users	1.5.1
8	Poor or missing governance of information assets such as lack of accountability for their protection, incomplete/inaccurate assets inventories, lack of risk analysis and security controls design and implementation	1.1.1, 1.1.2, 1.4.1, 1.4.3
9	Frequent change in the business, IT and security arenas, leading to a degree of helplessness and consequent denial or abdication of responsibilities	1.1.1, 1.1.2, 1.1.3
10	Inadequate contingency planning and preparedness for unpredictable/unusual or extreme information security incidents	1.4.2, 1.4.4
11	Legacy systems (eg. SCADA, safety-certified medical, space, aerospace & other systems) running on legacy platforms, often unsupported and no longer security patched, that form part of a critical business process/data chain	1.6.1, 1.6.2, 1.6.7, 2.4.1
12	Bugs in microprocessor designs and microcode that create opportunities for hackers to subvert trusted kernel routines including encryption and virtualization	1.4.1
13	Lack of will, concern and/or ability to impress the need for information security on youngsters and young adults	1.1.1, 1.1.2, 1.4.1

"Top 10 Information Security Threats for 2010" [42] was published by Perimeter E-Security. **Table 12** shows the ten information security threats and the available ECs of the ISMES capable of preventing the listed vulnerabilities.

Table 12. Top 10 information security threats for 2010

Top10	**Information Security Threat**	**C_ISMES**
1	Malware of many methods to install malware on systems, including the use of client-side software vulnerabilities	1.4.1, 1.4.3, 2.4.1
2	Malicious insiders who expose critical information of an organization	1.1.1, 1.4.1, 1.4.3
3	Exploited vulnerabilities such as data breaches, Worms, viruses, malware, and a host of other attack types	2.2.3, 2.4.1
4	Careless employees who are duped or fall prey to social engineering type attacks and malicious employees	1.1.1, 1.1.3, 1.4.1, 1.4.3
5	Mobile devices such as iPhone and laptop that exposed sensitive data because of stealing, public disclosure, or iPhone worm	1.3.1, 1.3.2
6	Social networking such as Facebook, MySpace, Twitter and others have changed the way people communicate with each other but that can be grounds for SPAM, scams	1.4.1, 1.4.3, 1.5.1
7	Social engineering by cyber criminals and phishing is a popular method for doing just that	1.4.1, 1.4.3, 1.5.1
8	Zero-day exploits to compromise a system based on a know vulnerability but no patch or fix exists, and it has become a very serious threat to information security	1.1.1, 1.6.1, 1.6.2, 2.4.1
9	Cloud computing security threats such as abuse and nefarious use, malicious insiders, and data loss and leakage	1.4.1, 1.4.3
10	Cyber espionage to act obtaining secrets without the permission of the holder of the sensitive information	1.3.2, 1.4.1, 1.4.3

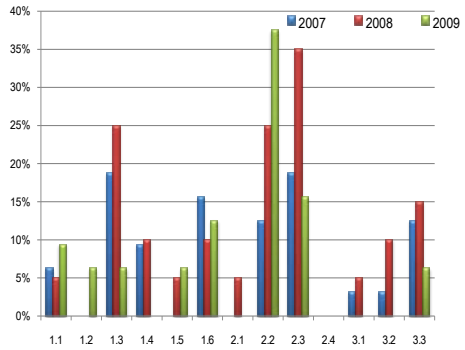

Fig. 2. Vulnerability distribution of organization, KISA orgnaization

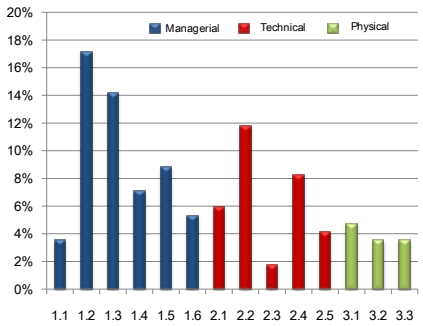

Fig. 3.Vulnerability distribution of from 2007 to 2010

We compiled a vulnerability distribution of organizations that implemented or planned to apply KISA's ISMS from 2007 to 2009 (See **Fig. 3**). The highest increase was observed in the 2.2 in EC's sub-category. Physical security vulnerabilities have decrease; however, managerial security vulnerabilities have been increasing steadily for the past three years. Especially, sub-categories 1.1, 1.3, 1.6, 2.2, 2.3, and 3.3 have be repeatedly pointed out. And sub-categories 1.1, 1.5, and 2.2 have increased every year. Therefore, various vulnerabilities and threats can be protected through the sub-categories. **Fig. 4** shows vulnerability distribution resulting from vulnerability/threat lists reported by [40][41][42] in the last three years. As **Fig. 3**, **Fig 4** has had similar results that sub-category 1.1, 1.3, 1.4, 1.6, 2.2, and 2.3 are highly vulnerable. Consequently, our analysis shows that it's not only about the security of the technical category as the generally occurred vulnerability/threat, but the security of management category, including information security policy and process, management and plans for incident response, and employee education, is more important. The highest rate was assigned to management vulnerability 56%, followed by technical vulnerability 34%, and physical vulnerability 10% in the vulnerability/threat distribution based on top lists from 2007 to 2010.

The proposed ISMES provides countermeasures to prevent vulnerabilities in each category as follows.

- *Imposition of legal and regulatory obligations:* It establishes an information security policy detailing the goal, scope, and responsibility of information security, regularly reviews imposition and information security policy plans, and establishes practical information security guidelines. It manages and updates practical information security guidelines and replaces or changes related laws, regulations, and equipment.
- *Management and education of administrator/users:* It trains regular employees and relation workers on information security (basic training for all employees and external professional training for managers to learn new security trends). It establishes processes, policies, and reviews of administrator/user accounts and passwords.
- *Management and plans of incident responses:* It establishes recovery plans, including the definition and scope of an incident, emergency contact systems, reports and recovery procedures, and education against incidents. It is education to prevent subsequent security incidents, and has a recovery system for immediate reactions to security incidents. It reports malfunctions and security weaknesses of systems/networks.
- *Information security system:* It checks potential vulnerability in packets, such as firewall or IPS/IDS, regularly checks security function of information security systems, and tests vulnerabilities of information systems and then obviates found vulnerabilities.

This highlights the expected effects of the comparison and analysis results of the proposed ISMES with previous ISMSs. It consists of the followings.

- *Target Level of Organization:* BS7799 and ISMS of Korea use the qualitative analysis for pre-evaluation about assets by evaluators. But, this evaluation is subjective due to the ambiguities in deciding which factors to evaluate. Furthermore, when an organization wants self-evaluation, there are imponderables because it is full of ambiguities deciding factors to evaluate assets. However ISMES uses qualitative and quantitative analysis for pre-evaluate using the target checklist.
- *Simple Documentation:* The DITSCAP of the USA has issues in terms of its large amount of documentation. In this research, however, a pre-analysis documentation was created, adjusted, and complemented through the ISMES. Thus the ISMES can inherit documentation approved by an authorized committee so as to improve its documentation efficiency.
- *Self-Evaluation:* The existing ISMSs are difficult to self-evaluate because it is hard to determine their assets and risks without an external evaluator. Therefore we advise that evaluation be calculated according to a target checklist and evaluation checklist.
- *Evaluation Checklist Supplements:* The abilities of the existing ISMSs are limited because the technical aspects is being rapidly developed. However, technical security can be complemented by management security. In this paper, we proposed the evaluation checklist to emphasize both management security and technical security. Therefore, the proposed evaluation checklist can place greater emphasis on risk factors in management security.
- *Revision of* [38],[43], *and* [44]: In this paper, new revision is as follows: an added and modified checklist(TC and EC), an application of quantitative and qualitative analysis methodology, a separated application of self-evaluation and evaluation committee for information security management evaluation, and an evaluation of ISMES.

The best method of ISMES evaluation is a uniform application throughout the real organization. However in a real organization, information security-related data is confidential. Thus, the ISMES was evaluated using a preventable evaluation checklist of the existing threats and vulnerabilities.

5. Conclusion

This paper examined a variety of systems, the CC, BS7799, IT baseline protection manual, ISMS of Korea, ISMS of Japan, DITSCAP, DIACAP, TCSEC, and ITSEC. Furthermore, it found weaknesses in the existing ISMSs through a comparative analysis of the ISMSs. Based on these analyses, we proposed a new ISMES, the process of which consists of five phases. This study also evaluated the proposed ISMES in light of the vulnerability/threat lists published from 2007 to 2010, showing the expected effects of the ISMES through the comparison and analysis results. This study provides that a government or business organization with a process to verify their information security so as to improve the information security of the organizations. The case study used in this research can also contribute to the establishment of an ISMS in a business organization.

References

[1] Thuy Nguyen and Grenville Armitage, “A survey of techniques for Internet traffic classification using machine learning,” *IEEE Communications Surveys and Tutorials*, pp. 56-76, Nov. 2008. http://dx.doi.org/10.1109/SURV.2008.080406

[2] BSI, "Code of Practice for Information Security Management," *British Standards Institute*, 1999. Article (CrossRef Link)
[3] ISO, International Standards ISO/IEC27001:2005, ISO/IEC27002:2005, ISO/IEC 22399:2007, "Information Technology Security Techniques," 2005. Article (CrossRef Link)
[4] ISO, BS 25999-1:2006/BS 25999-1:2006, "Business Continuity Management Part1, Part2," 2006. Article (CrossRef Link)
[5] http://www.iso27001security.com/html/27000.html. Article (CrossRef Link)
[6] International Standard ISO/IEC 15408, "Common Methodology for Information Technology Security Evaluation," Version 3.1, 2006.10. Article (CrossRef Link)
[7] International Standard ISO/IEC 15408, "Common Criteria, Part1, 2, 3," Version 3.1, 2006.10 . Article (CrossRef Link)
[8] Korea Communications Commission, "Certification of Information Security Management System," 2008.5. Article (CrossRef Link)
[9] Department of Defense, "5810.1-M:DITSCAP Application Manual", 2001. Article (CrossRef Link)
[10] Anthony M.Valletta, "DoD Instruction", 1997. Article (CrossRef Link)
[11] DC: DoD PKI C & A Working Group, "DIACAP Knowledge Base Overview," Mar. 2005. Article (CrossRef Link)
[12] DoD, "Department of Defense Trusted Computer System Evaluation Criteria, 8500.01E," 2002. Article (CrossRef Link)
[13] Lunarline.Inc, "DIACAP," Mar. 2006. Article (CrossRef Link)
[14] Department of Defense, "DIACAP", Nov. 2007. Article (CrossRef Link)
[15] Department of Trade and Industry, "Information Technology Security Evaluation Criteria," 1991. Article (CrossRef Link)
[16] BIS, "IT Baseline Protection Manual," 2004. Article (CrossRef Link)
[17] BIS, "IT Baseline protection Manual Layer model". Article (CrossRef Link)
[18] S Weiss, O Weissmann, F Dressler, "A Comprehensive and Comparative Metric for Information Security," in *Proc. of IFIP International Conference*, 2005. Article (CrossRef Link)
[19] BSI, "BSI-Standard 100-1 Information Security Management Systems", Version 1.5, 2008. Article (CrossRef Link)
[20] "The ISO 27000 Directory". Article (CrossRef Link)
[21] Pounder, C., "The Revised Version of BS7799-So What's New," *Computer and Security*, vol.18, 1999, pp.307-311. http://dx.doi.org/10.1016/S0167-4048(99)80075-3
[22] Japan Information processing development corporation, "JIS Q 27001 (ISO/IEC 27001: 2005) Information security management system conformity assessment scheme," 2006. Article (CrossRef Link)
[23] JIPDEC, http://www.isms.jipdec.jp/en/index.html. Article (CrossRef Link)
[24] KISA, "Guidelines for the vulnerability analysis and evaluation," 2004. Article (CrossRef Link)
[25] KISA, "Information Security Safety Checklist," 2001. Article (CrossRef Link)
[26] KISA, "Self Test of Information Security Level for small and medium enterprises," 2008. Article (CrossRef Link)
[27] KISA, "Information Security Management System," 2010. Article (CrossRef Link)
[28] KISA, "Information Security Evaluation Methodology," 3. 2010. Article (CrossRef Link)
[29] Kim I, Chung Y, Lee Y, et al., "Information system modeling for analysis of propagation effects and levels of damage," in *Proc. of ICCSA 2006*, vol. 3982,54-63, 2006 Article (CrossRef Link)
[30] Kim Y, Nam T, Won D, "2-Way text classification for harmful Web documents," in *Proc. of ICCSA 2006*, vol. 3981,545-551, 2006 Article (CrossRef Link)
[31] Kwak J, Rhee K, Oh S, et al., "RFID system with fairness within the framework of security and privacy," *LNCS*, vol.3813, 142-152, 2005. Article (CrossRef Link)
[32] National Intelligence Service, "Assessment of Information Security Management Handbook," 2007. Article (CrossRef Link)
[33] Chih-Wei Hsu, et al., "A Practical Guide to Support Vector Classification," 2003. Article (CrossRef Link)

[34] Corinna Cortes and V. Vapnik, "Support-Vector Networks," *Machine Learning*, 20, 1995. Article (CrossRef Link)
[35] California office of Information Security and Privacy protection, "Information Security Assessment Tool for State Agencies," 4. 2008. Article (CrossRef Link)
[36] Gwangyeom Kim, "Construction of controlled model for self-assessment through Information Security Management System," *Daejeon Univ*.10. 2009. Article (CrossRef Link)
[37] U.S Cyber Consequence Unit, "The US-CCU Cyber-Security Check List," 2007. Article (CrossRef Link)
[38] SH Hur et al., "A Study on Development of Information Security Evaluation Model," KIPS, ISSN 1598-2858, 2008. Article (CrossRef Link)
[39] Korea Internet and Security Agency, "ISMS Authentication Example". Article (CrossRef Link)
[40] KISA, "Information Security Management Vulnerability Top 10," 2007-2009. Article (CrossRef Link)
[41] CISSP forum, ISO27k forum, "Top Information Security Risks for 2008," Dec. 2007. Article (CrossRef Link)
[42] Permeter E-Security, "Top 10 Information Security threats for 2010," 2010. Article (CrossRef Link)
[43] Heasuk Jo, Seungjoo Kim, and Dongho Won, "A Study on Comparative Analysis of the Information Security Management Systems," in *Proc. of ICCSA 2009*, LNCS6019 pp. 510-519, Mar. 2010. Article (CrossRef Link)
[44] Ministry of Information and Communication Republic of Korea, "A Development of Information Security Evaluation Model," 2007. Article (CrossRef Link)

Appendix

Appendix A. Managerial Security Checklist

Checklist	Questions
1.1.1	**Planning of Information Security Policy**
1.1.1.1	Does an organization establish an information security policy that includes goal, scope, and responsibility of information security?
1.1.1.2	Do top executives (above the layer of management) approve the information security policy?
1.1.1.3	Has the information security policy been announced and is it observed by all employees?
1.1.1.4	Is the information security policy renewed and reviewed periodically?
1.1.1.5	Is convenient access to the information security policy offered to all employees?
1.1.1.6	Do top executives adhere to the goal of information security policy?
1.1.1.7	Do various communication mechanisms, such as brochures, and electronic documents, announce the information security policy use?
1.1.1.8	Is the information security policy prescribed by national laws or regulations related to business?
1.1.1.9	Does the information security policy include strategic and systematic risk management?
1.1.1.10	Does the information security policy deal with the appropriate scope?
1.1.1.11	Does it reflect the analysis of the audit of last year's information security activity?
1.1.1.12	Has a cost been assigned to the loss of assets?
1.1.1.13	Is the analysis reflected in the information security management when or new policies are developed or policies are updated?
1.1.2	**Execution of the Information Security Plan**
1.1.2.1	Does the information security execution plan include budget, work schedule, etc. based on the information security policy planned for this year?
1.1.2.2	Do top executives approve the information security execution plan?
1.1.2.3	Does the manager responsible for information security check the information security execution plan each quarter?
1.1.2.4	Does the information security execution plan include a stability evaluation of information security management?
1.1.2.5	Does it closely connect the information security execution plan and the information security policy?
1.1.3	**Practical Guidelines on Information Security**
1.1.3.1	Are the information security guidelines practical to implement as detailed methods and is the process to pursue the information security policy and execution plan planned?
1.1.3.2	Do the information security practical guidelines include appropriate methods to protect managerial, physical, and technical aspects?
1.1.3.3	Does the manager responsible for information security approve the information security practical guidelines?
1.1.3.4	Are the information security practical guidelines periodically reviewed and renewed?
1.1.3.5	Are the information security practical guidelines distributed to all employees and observed by them?
1.2.1	**Organizational Structure**
1.2.1.1	Does an organization consisting of a responsible manager for information security, an information security manager, and information security staff operate?
1.2.1.2	Is the information security manager who does the working-level security management posted?
1.2.1.3	Is information security working-level staff for a main facility and a sensitive information property posted?
1.2.1.4	Does a dedicated section or team operate who focus on information security management?
1.2.1.5	Are the information security manager and the information security staff who can have a dual role posted separately?
1.2.1.6	Does the organization seek outside professional support for sensitive information security management?
1.2.1.7	Does the outside professional have sufficient experience, knowledge, and technology of the information security management system?
1.2.2	**Selection of Information Security Manager**
1.2.2.1	Is the information security manager responsible for all of information security posted?
1.2.2.2	Has the manager responsible for information security been announced to all employees by the CEO?
1.2.2.3	Does the manager responsible for information security have the right to organize a special response team in the event of a security incident?
1.2.2.4	Does the manager responsible for information have sufficient experience, knowledge, and technology of a security action and task?
1.2.2.5	Is the manager responsible for the information position of director, such as the Chief Information Officer or Chief Security Officer, announced?
1.2.3	**Role and Responsibility for Employees**
1.2.3.1	Is there a document for the duty assignment of the responsible manager, security manager, and staff?
1.2.3.2	Does the document specify roles and responsibilities of each position?
1.2.3.3	Are the recorded duties and the real duties for each position identical?
1.2.3.4	Are roles and responsibilities of each position in the form of practical guidelines reflected in the details of the real duty?
1.2.3.5	Is the document for duty assignment renewed and reviewed every year?
1.3.1	**Assets Management**
1.3.1.1	Are the assets classified and recorded according to the importance of assets by a policy?
1.3.1.2	Are the classified assets set and managed by an appropriate level grant?
1.3.1.3	Are the manager, owner, and user of the classified assets defined?
1.3.1.4	Does it have countermeasures according to the importance of assets?
1.3.1.5	Do procedures and policies for recording and destruction of information assets exist in a document?
1.3.1.6	Do procedures and policies for confirming and checking information assets destruction exist?

1.3.1.7	Does it judge the effectiveness of the information security management system in the case of changing assets or facility?
1.3.1.8	Is there a policy to backup information assets, such as main information and software?
1.3.2	**Facility Management**
1.3.2.1	Is the structure of the information communication networks managed?
1.3.2.2	Is the list of information communication network facilities managed?
1.3.2.3	Is the list the most recent list of the information communication network facilities?
1.3.2.4	Are assets, owner, administer, use, identification ID, and location marked in the list of information communication network facilities?
1.3.2.5	Has risk analysis been conducted for property using the list of information communication network facilities?
1.3.2.6	Does a policy about management of portable storage facilities (USB, cell phone, PDA, Laptop computer) exist?
1.3.2.7	Does the organization perform a safety check of facilities in case of insoluble treatment of facilities?
1.4.1	**Internal Personal Management**
1.4.1.1	Is the access control of an account removed when employees transfer or retire?
1.4.1.2	Do promotional campaigns run to raise awareness of information security?
1.4.1.3	Are all employees trained by regular education about information security?
1.4.1.4	Does information security education include content on personal information security?
1.4.1.5	Do managers dealing with information security attend external professional training or seminars?
1.4.2	**External Personal Management**
1.4.2.1	Does the screening for eligible employment include identity, education level, work experience, checks etc of applicants when an organization employs contract workers or temporary employees?
1.4.2.2	Do external employees dealing with the sensitive information inform (or swear) agreement to not divulge the business's proprietary information?
1.4.2.3	Is there an access control policy for external personal management?
1.4.2.4	Is the responsibility of eligible employment stipulated in the contract with the service company, in case employees are employed by a service company?
1.4.3	**Management of the Head of Main/sensitive Business**
1.4.3.1	Is there a definition of main/sensitive business?
1.4.3.2	Does an organization have a career aptitude test for the head of main/sensitive business?
1.4.3.3	Do employees dealing with sensitive information inform agreement to not divulge business proprietary information?
1.4.3.4	Is there education on crisis management for the head of main/sensitive business?
1.4.4	**Security Guidelines for Outsourcing**
1.4.4.1	Are obligations about information security stipulated in the contract with an outsourcer?
1.4.4.2	Are there emergency measures on shutting down of outsourcing in case of outsourcing of computer-related work?
1.4.4.3	Does the contract or service agreement address legal information on security?
1.4.4.4	Are there work procedures for a periodic check of information security in the contract or service agreement?
1.5.1	**Providing Guidelines**
1.5.1.1	Does it offer "personal information protection policy", "security vulnerability", and "risk management of account and password" to the user?
1.5.1.2	Does it provide secure encryption standard guidelines when dealing with sensitive information of the user?
1.5.1.3	Does an organization urge employees to safely manage information, such as main documents, storage, or printed materials on a desk when they are away?
1.5.1.4	Does it often and periodically offer information security matters by E-mail, Homepage, or SMS?
1.5.1.5	Do the user contact details provide information?
1.5.1.6	Do managers exist to provide information security to user?
1.5.1.7	Does the Help Desk operate to provide answers on information security?
1.6.1	**Incident Prevention**
1.6.1.1	Are the security threats, vulnerabilities, and impacts and risks list managed for security incident prevention?
1.6.1.2	Is a security check (threats, vulnerabilities, impacts, risks) of assets for security incident prevention regularly conducted?
1.6.2	**Planning status of Incident Recovery**
1.6.2.1	Does it have recovery plan for security incidents?
1.6.2.2	Are security incidents classified by importance and defined by the reporting process?
1.6.2.3	Is the incident recovery plan consistent with the continuous business plan?
1.6.3	**Recovery System**
1.6.3.1	Does it have a centralized recovery system to respond to and a monitor a security incident?
1.6.3.2	Does it cooperate with an external expert, professional organization, government agency related to monitoring and recovery & procedures of security incidents?
1.6.4	**Efforts to Prevent Similar Incidents**
1.6.4.1	Does it conduct and plan regular education for responses, plans, procedures, tests, etc. about security incidents?
1.6.4.2	Are employees trained and educated to prevent similar security incident?
1.6.4.3	Has the organization conducted a risk assessment within the last two years to identify information security?
1.6.5	**Record and Management**
1.6.5.1	Is there an immediate report according to the defined security report process when a security incident or sign occurs?
1.6.5.2	Is there a written security incident report about a security incident or sign?
1.6.5.3	Is a major security incident specified reported quickly to the CEO?
1.6.5.4	Is an internal security incident reported in case an organization has rules or regulations about the report of security incidents to authority?

1.6.5.5	Are software malfunctions and security weaknesses of the system/network reported?
1.6.6	**Recovery**
1.6.6.1	Do recovery procedures and processes of security incidents exist?
1.6.6.2	Does the report reflect the security incident and recovery according to the process?
1.6.6.3	Are security incidents reported and audited from start to finish?
1.6.7	**Prevention Planning to Prevent Similar Incidents**
1.6.7.1	Is the security incident analyzed from multiple viewpoints, such as patterns of incidents, frequency of similar incidents, and cost of incidents?
1.6.7.2	Do related organizations and staff share weaknesses and information of security incidents?
1.6.7.3	Do countermeasures exist to prevent recurrence based on analyzed information of the security incident?
1.6.7.4	Is a process modified where necessary when the process changes the recovery procedure and recovery policy?
1.7.1	**Business Continuity Planning**
1.7.1.1	Are there risk assessment and planning for BCM?
1.7.1.2	Are all employees trained for seamless business?
1.7.1.3	Is there a BCP audit when the planning is updated and changed and is it reflected in past audit information?

Appendix B. Technical Security Checklist

Checklist	Questions
2.1.1	**Traffic Monitoring**
2.1.1.1	Is traffic in major internal nodes monitored using a network monitoring tool?
2.1.1.2	Is the backbone used in connection with an external network monitored using a network monitoring tool?
2.1.1.3	Does it have ways to revert to normal operation when strange events (hacking or errors with the facilities) for network traffic monitoring occur?
2.1.1.4	Are strange event detected by monitoring reported to the manager by SMS, e-mail, or an alarm?
2.1.1.5	Does it have a policy for load balancing of the information communication network facilities?
2.1.2	**Wireless Security Service**
2.1.2.1	Do security measures exist for user using a wireless service?
2.1.2.2	Does it have security measures against eavesdropping and spill over when a wireless service is provided?
2.1.2.3	Do security measures, such as data encryption, exist for connecting information security?
2.1.2.4	Do the rules, such as security measures, processes, user authentication, data encryption, wireless LAN equipment, etc. exist about the wireless service?
2.1.2.5	Do security measures check the wireless service regularly?
2.2.1	**Installation and Operation of Information Security System**
2.2.1.1	Does it use a certified/approved information security system that satisfies the security requirements?
2.2.1.2	Does the operation of an intrusion detection system (IDS) exist in all sections connected to the external network?
2.2.1.3	Does the operation of an IDS or intrusion prevention system (IPS) exist in major nodes connected to the external network?
2.2.1.4	Does it configure no low quality transmission speed by installation of IDS or IPS?
2.2.1.5	Does it install and operate virtual private network (VPN), firewall, etc.?
2.2.2	**Security of Information Security System**
2.2.2.1	Does it operate a warning function in the event of failures in the information security system?
2.2.2.2	Is the information security system updated to detect new attack methods?
2.2.2.3	Does it check the functioning of the security function and the information security system routinely?
2.2.2.4	Does it regularly checkup the log data of the information security system?
2.2.3	**Vulnerability Testing**
2.2.3.1	Does a vulnerability testing policy exist?
2.2.3.2	Is vulnerability testing operated and updated regularly?
2.2.3.3	Are weakness and testing results reported to the security manager?
2.2.3.4	Does the recovery system operate in response to weaknesses detected by vulnerability testing?
2.2.3.5	Is the result of vulnerability testing recorded in a database, documentation, etc.?
2.2.3.6	Are parts of vulnerability testing divided into information system, network, database, web service, etc?
2.2.3.7	Is vulnerability testing conducted using an automated tool?
2.2.3.8	Does it consign vulnerability testing for objective criteria to an external professional organization?
2.2.4	**Web Server Security**
2.2.4.1	Does the web server perform a unilateral operation?
2.2.4.2	Are well-known weaknesses removed from the web server?
2.2.4.3	Does a web server exist in the DMZ (demilitarized zone) separated from the internal network?
2.2.4.4	Is unnecessary traffic limited by an intrusion prevention system (IPS) from accessing the web server?
2.2.4.5	Does it check the working security function of an information security system regularly?
2.2.4.6	Does it check web hacking using web weaknesses and has it security measures?
2.2.5	**DNS Server Security**
2.2.5.1	Are CPU usage, memory usage, and traffic monitoring of DNS server measured regularly?

2.2.5.2	Is the DNS server configured to withstand overload?
2.2.5.3	Are setting of files and environment variables of the DNS server updated regularly?
2.2.5.4	Is it possible that another DNS server provides service, if it does not have DNS server access?
2.2.6	**DHCP Server Security**
2.2.6.1	Is the DHCP (Dynamic Host Configuration Protocol) server configured to withstand overload?
2.2.6.2	Are CPU usage, memory usage, and traffic monitoring of DHCP server measured regularly?
2.2.6.3	Are file settings and environmental variables of the DHCP server updated regularly?
2.2.6.4	Is the assigned IP address, MAC address, using time, etc. of each user recorded?
2.2.6.4	Are external IP denied by the IPS from accessing the DHCP?
2.2.6.5	Is the vulnerability of the DHCP server checked regularly?
2.2.7	**DB Server Security**
2.2.7.1	Does the DB server perform a unilateral operation?
2.2.7.2	Are well-known weaknesses removed from the DB server?
2.2.7.3	Does a web server exist in the DMZ (demilitarized zone) separated from the internal network?
2.2.7.4	Is unnecessary traffic limited by an IPS from accessing the web server?
2.2.7.5	Does it check the operation of the security function of an information security system regularly?
2.2.7.6	Does it check web hacking using web weaknesses and does it have security measures?
2.2.7.7	Does it monitor/recode log information of the DB server by access and change the data?
2.2.8	**Router/Switch Security**
2.2.8.1	Does it have an access control feature, such as ACL (Access Control List), in the Router/Switch equipment?
2.2.8.2	Does the access control feature of the Router/Switch limit access to unauthorized users and has unnecessary traffic and protocol filtering?
2.2.8.3	Are well-known weaknesses removed in the Router/Switch?
2.2.8.4	Does it reset factory default settings of the Router/Switch equipment?
2.2.8.5	Is the Router/Switch firmware patched and updated regularly?
2.3.1	**Access Control Management**
2.3.1.1	Can an authorized user in the network access just authorized systems or networks?
2.3.1.2	Are access rights of users regularly checked?
2.3.1.3	Does it regularly check that only authorized users can access the information communication facility?
2.3.1.4	Does it confirm if it is a trusted connection in case of accessing the external network?
2.3.1.5	Is there an authentication process and policy in case of remote access of users?
2.3.1.6	Is it internally cut off from other protocols and services, except the protocol for access control?
2.3.1.7	Is there a policy for mobile device access?
2.3.1.8	Is there a policy for hand-held computers, personal digital assistants (PDA), or USBs?
2.3.2	**Administrator/User Account Management**
2.3.2.1	Does it have process and policy for administrator/user account management?
2.3.2.2	Does it confirm the identity of the administrator/user in the case of account issue?
2.3.2.3	Does the administrator/user change the account password at least every three months?
2.2.2.4	Does it provide and advise how to create passwords for administrator/user accounts?
2.3.2.5	Does it have an operation and approval procedure for passwords and administrator accounts?
2.3.2.6	Is the password changed immediately after termination of an employee who knew the password of an administrator account?
2.3.3	**User Identification and Authentication**
2.3.3.1	Is it using a proven authentication mechanism to provide important services in case of user authentication?
2.3.3.2	Does it use an electronic signature authentication system?
2.3.3.3	Does it specify the reaction to authentication failure?
2.3.3.4	Is the number of authentication failure attempts limited?
2.3.3.5	Are authentication recodes managed and maintained?
2.4.1	**Patch Management**
2.4.1.1	Does it have process and policy for applying security patches?
2.4.1.2	Does it check regularly that employees are applying notified patch information?
2.4.1.3	Does it have a practical alternative to unsupported software or to no longer security-patched software?
2.4.1.4	Is security patch information for the operating system or major programs notified, monitored, and patched regularly?

Appendix C. Physical Security Checklist

Checklist	Questions
3.1.1	**Location and Structure of Physical Scope**
3.1.1.1	Is structural and locational safety of the physical scope considered?
3.1.1.2	Does an emergency measure exist against fire or flood?
3.1.1.3	Do safety facilities and equipment exist to minimize risk and prevent disasters?
3.1.2	**Safe Destruction and Policies for Equipment**
3.1.2.1	Does it confirm and check before destroying equipment?
3.1.2.2	Do procedures and policies of confirming and checking destroyed equipment exist?

3.1.2.3	Are destroyed equipment regularly checked?
3.1.3	**Maintenance and Management**
3.1.3.1	Was an appropriation for maintenance and management of equipment budgeted?
3.1.3.2	Do policies about maintenance and management of equipment exist?
3.1.3.3	Are destroyed equipment regularly checked?
3.1.4	**Access Control of Item Delivery and Receipt**
3.1.4.1	Is access control of item delivery and receipt managed and recorded?
3.1.4.2	Does a procedure for access control of item delivery and receipt exist?
3.1.5	**Security of Power Supply and Lines of Communication**
3.1.5.1	Is a security measure for power supply and lines of communication established?
3.1.5.2	Is the power supply and line of communication regularly checked?
3.2.1	**Security Guidelines and Definitions of Physical Scope and Boundary**
3.2.1.1	Is the physical scope and boundary to be protected defined?
3.2.1.2	Are security measures of physical scope and boundaries established?
3.2.1.3	Are security measures of physical scope and boundaries classified by the significance of the information?
3.2.2	**Access Control of Physical Scope**
3.2.2.1	Does a policy about access control of the physical scope exist?
3.2.2.2	Is an admission procedure followed for the physical facility, documentation, or media?
3.2.2.3	Is information about the admission procedure in physical scope recorded?
3.2.2.4	Is enforcement history about access control of the physical scope regularly checked?
3.2.2.5	Is there a process for keys, codes, or cards and background check of physical scope?
3.3.1	**Backup Equipment in Physical Scope**
3.3.1.1	Does backup equipment exist?
3.3.1.2	Is backup equipment classified according to their significant in the physical scope?
3.3.1.3	Are backup equipment within the physical scope regularly checked?
3.3.2	**Backup and Recovery Procedure of Physical Scope**
3.3.2.1	Do backup and recovery procedures exist?
3.3.2.2	Are backup and recovery procedures classified according to their significant in the physical scope?
3.3.2.3	Are backup and recovery procedures regularly checked?

Heasuk Jo received her B.S. in computer engineering from Hansung University, Korea, in 2003, M.S. degree in computer engineering, and Ph.D. degree in electrical and computer engineering from Sungkyunkwan University (SKKU), Korea, in 2005 and 2010, respectively. She is a researcher at Financial Security Agency (FSA). Her current research interests include cryptography, information security and assurance, and mobile security.

Seungjoo Kim received his B.S. (1994), M.S. (1996), and Ph.D. (1999) in information engineering from Sungkyunkwan University (SKKU) in Korea. Prior to joining the faculty at Korea University (KU) in 2011, He served as Associate Professor of School of Information and Communication Engineering at SKKU for 7 years. Before that, He served as Director of the Cryptographic Technology Team and the (CC-based) IT Security Evaluation Team of the Korea Information Security Agency (KISA) for 5 years. Now He is Associate Professor of Center for Information Security Technologies (CIST) at KU. Also, He have served as an executive committee member of Korean E-Government, and advisory committee members of several public and private organizations such as National Intelligence Service of Korea, Digital Investigation Advisory Committee of Supreme Prosecutors' Office, Ministry of Justice, The Bank of Korea, ETRI(Electronic and Telecommunication Research Institute), and KISA(Korea Information Security Agency), etc. His research interests include cryptography, information security and information assurance.

Dongho Won received his B.E., M.E., and Ph.D. degrees from Sungkyunkwan University in 1976, 1978, and 1988, respectively. After working at the Electronics & Telecommunications Research Institute (ETRI) from 1978 to 1980, he joined Sungkyunkwan University in 1982, where he is currently a Professor of the School of Information and Communication Engineering. His interests are cryptology and information security. He was the president of the Korea Institute of Information Security & Cryptology (KIISC) in 2002.