A Study on the Impact Analysis of Security Flaws between Security Controls: An Empirical Analysis of K-ISMS using Case-Control Study

Hwankuk Kim[1], Kyungho Lee[2], and Jongin Lim[2]
[1]Security R&D Team, Korea Internet & Security Agency (KISA), Seoul 05717, Republic of Korea
[e-mail: rinyfeel@kisa.or.kr]
[2]Graduate School of Information Security, Korea University, Seoul 136-701, Republic of Korea
[e-mail: kevinlee@korea.ac.kr, jilim@korea.ac.kr]
*Corresponding author: Jongin Lim

Received October 3, 2016; revised February 10, 2017; accepted May 2, 2017; published September 30, 2017

Abstract

The measurement of information security levels is a very important but difficult task. So far, various measurement methods have studied the development of new indices. Note, however, that researches have focused on the problem of attaining a certain level but largely neglecting research focused on the issue of how different types of possible flaws in security controls affect each other and which flaws are more critical because of these effects. Furthermore, applying the same weight across the board to these flaws has made it difficult to identify the relative importance. In this paper, the interrelationships among security flaws that occurred in the security controls of K-ISMS were analyzed, and the relative impact of each security control was measured. Additionally, a case-control study was applied using empirical data to eliminate subjective bias as a shortcoming of expert surveys and comparative studies. The security controls were divided into 2 groups depending on whether or not a security flaw occurs. The experimental results show the impact relationship and the severity among security flaws. We expect these results to be applied as good reference indices when making decisions on the removal of security flaws in an enterprise

Keywords: Information Security Management, ISMS, Risk Management, Case-Control Study, Security

1. Introduction

As an ultra-connected society -- wherein all things are connected to the Internet -- is about to dawn on the world, diverse industries from telecom through finance to medicine have become increasingly reliant on ICT (Information & Communication Technology). This has led to a rapid escalation in the number of information leaks, service losses, and cyber intrusions produced by organized cyber-attacks such as APT (Advanced Persistent Threat) attacks, malware, and DDoS (Distributed Denial of Service) attacks. Whenever companies need to identify their important information assets, diagnose their current security level, or determine the current state of affairs in order to establish policies, make investments, form organizations, and carry out other forms of systematic management of their information security, the task of analyzing the current level of information security becomes very important. Note, however, that measuring a company's information protection level is a very difficult task. The environments surrounding enterprises differ, which means that the targets and areas that have to be protected are constantly expanding. This imposes severe restrictions when determining which indices to use to measure information security. The lack of chronological statistical data, divergent information security measurement indices, and other factors make it difficult to identify a uniform standard and the relative importance among the items for measurement. Nevertheless, research efforts have continued with regard to the development and comparative analysis and development of level evaluation indices for measuring enterprise security levels, analysis of security level evaluation programs in Korea and abroad, evaluation of importance of security control items, and economic analysis [1] [2] [3].

According to Baker [4], the maturity of enterprise information protection management refers to the type and quality of security control. Enterprise information protection management is not a technical problem but is defined as a social and organizational factor. Baker concluded that control quality and implementation quality change depending on the size of the organization through a survey method developed based on the technical, managerial, and operational security control classifications of NIST(National Institute of Standards and Technology). H. Lee et al. [5] proposed a total of 27 measurement indices for information protection level measurement by classifying the ISO(International Organization for Standardization) 27001 control items into 3 index groups (base index, execution index, and result index) of the BSC (Balanced Score Card) method. M. Ko et al. [6] proposed 11 detailed measurement items by classifying enterprise information protection maturity evaluation into learning, internal process, user, and management results. Hsu [7] examined variations in framings between employees, managers, and certification teams during the implementation of an IS (Information System) security certification process. K. Kim et al. [8] [9] proposed evaluation criteria for information protection management suitable for the cloud and smart grid environment by comparing K-ISMS(Korea's Information Security Management System) security control items. Using surveys conducted among information protection experts, C. Lee et al. [10] performed comparative analysis of the importance and investment priorities on 13 security control items of the information protection management system. They found the important items to be intrusion response, access control, and personnel security in decreasing order. Otero [11] developed a fuzzy set theory-based assessment methodology that provides for a thorough evaluation of information security controls in organizations.

Similar studies published include [2] [3]; "Impact of Investments on Information Security and Decision to Invest" [12] [13] [14] [15]; "Information Security Index and Quantification

Research" [16] [17]; "Information Security and Security Policy Compliance" [18] [19] [20] [21], and; "Management of Information Security and Risk Management" [22] [23]

Despite these issues, studies on the methods of measuring security levels in an enterprise have been carried out continuously. Such methods focus on the problem of what framework to apply when investigating the information protection level, and they are proposed as mere model or guideline for measuring the quantitative level. Thus, cases wherein the methods are actually applied are rare, and divergent indices have limited their widespread adoption. Second, most of the indices were created to measure whether a target level of security has been reached and are not focused on the flaws themselves for the purpose of removing them. Third, despite the varying degrees of importance of the items for measurement, uniform weight was applied across the board (1/N), or they were processed as simple summations, resulting in measured items of equal importance. Thus, the contributions of each item were not taken into account. Furthermore, in this scheme, if the number of items for measurement increases, the relative weight of an item for measurement is reduced. Lastly, studies on the relative importance and weights of information security controls were carried out using surveys by industry experts, so the results of such analyses have the limitation of subjective bias.

Therefore, the purpose of this research is to analyze the impacts of information security controls wherein flaws have been detected and to determine the severity and relative weights of the flaws. The results of the research could then be used to analyze the security level of an enterprise and as a support tool when making business decisions. For this purpose, actual data from the K-ISMS certifications [24], which are based on the ISO 27001 model [25], were used in this research. K-ISMS is a program for certifying the safety of information assets held by an enterprise. It used 104 certification criteria to evaluate whether an enterprise has in place an integrated information security management system consisting of managerial, technical, and physical protection measures. Korea has been operating K-ISMS since it adopted the program in 2002. In 2013, the K-ISMS certification was made mandatory by law for enterprises of a certain size. As of today, approximately 366 enterprises have been certified, making it possible to obtain actual analysis and statistical data.

The rest of this paper is organized as follows: Chapter 2 examines the research trends related to security level measurements and the theoretical background of case-control study; Chapter 3 explains the targets of empirical analysis and the methods; Chapter 4 describes the results of the experiments; finally, Chapter 5 presents the implications of the research results.

2. Theoretical Background

2.1 Method of Measuring the Security Level and Security Controls Model

Research has been conducted continuously on formalized methods derived from surveys and interviews, in order to evaluate and measure the information protection levels of enterprises. For instance, when researchers attempt to estimate the information protection level of a given enterprise using survey methods, they are handicapped by the subjective judgments of the respondents. The most objective way of evaluating the information protection management system and information protective measures of an enterprise involves using external standards such as the international ISO 27001 (1999) and NIST SP (Special Publication) 800-53A standards [26]. These are widely used because of the objectivity and reliability of the systemized inspection items [27]. Note, however, that this approach has its limitations because there are no evaluation criteria for evaluating information protection activities against a quantified ranking system. For this reason, security levels are hard to measure.

The objectives of the information security control model are to maintain (availability) the operation of the information system in an organization (enterprise, bank etc.), prevent (confidentiality) the disclosure or leaks of information assets belonging to the organization, and preserve (integrity) the accuracy of important information held by the organization.

Everything that interferes with this is a risk factor, so all information security programs and responses required to sustain the organization must be set up so that all risks can be brought under control. Still, the level of information protection is bound to decline if there is insufficient awareness of these risks or if the assortment of controls (measures) for minimizing damage is inadequate. Risk awareness and measures could be separated into the managerial, physical, and technical aspects. Representative models built along these lines include ISO 27001 and NIST risk management framework in the United States, which are considered to be much systemized. Other countries such as Korea (K-ISMS, ISO 27001), Japan (ISO 27001), UK (ISO 27001, BS(British Standard)7799 Part I/Part II), Germany (British Standard Institute IT Baseline Protection Manual, 2001), and Canada (Information Technology Infrastructure Security & Protection Service) have implemented them. Various countries have established standards that are suitable for their environments or adopted the international standard. Security control and certification programs are identical or similar to ISO-ISMS, though partial differences remain in the details. In addition, the standards for the maturity of information protection management in an enterprise are ISM3 (Information Security Management Maturity Model) [28], BCMM (Business Continuity Maturity Model) [29], and ISO27004 [30]. The models for measuring security levels are summarized in **Table 1**.

Table 1. Information Security Management System and Maturity Model

Category	Description
ISO 27001 ISMS (2005, ISO-ISMS)	An international standard used worldwide for information security management, which is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. As of 2013, over 22,000 companies have received ISO 27001 certifications. In accordance with PDCA cycles in quality management covered by ISO 9000, ISO-ISMS includes processes for planning and executing security policies and for checking that the policies are implemented correctly. Finally, the acting stage in which the results of an evaluation are reflected in the improvement plans at the future planning stage. Repeating the PDCA cycles in this way results in enhancements of security management. The ISO-ISMS control list comprises 14 areas, 39 objectives and 114 items (revised in 2013)
NIST SP-800	Based on the Federal Information Security Management Act (FISMA, 2003), the US government stipulates that the operation of the federal information system shall abide by a minimum set of security requirements. NIST has proposed a risk management framework (SP800-53A) for the federal information system. This framework requires an organization to go through the following steps: classification of information systems; section of information security restrictions; implementation of information security restrictions; evaluation of information security restrictions; certification of information security; and monitoring of information security restrictions. The security control category is composed of 3 classes (Technical Controls, Operational Controls, and Management Controls) and provides guidelines on 256 security controls organized into 18 families
ISM3 (2009)	Based on the SW quality assurance criteria, this model uses the normal process-based approach towards information protection. This standard is divided into 4 areas and measures the maturity of an enterprise's security in 7 categories (including report to management, resource assignment, development security, access control, forensics, and intelligence) using 5 grade levels
BCMM (2001)	Developed to measure the continuity of an organization's tasks, this model consists of 8 measured items (leadership, employee awareness, BC program structure, program

Category	Description
	dissemination, scale, resource support, external cooperation, BC contents), and is used to measure the maturity level of an enterprise according to one of 6 grades.
ISO 27004 (2009):	This model proposes a method of measuring the maturity level of an enterprise in steps, according to the PDCA of ISO27001. Major items are classified as risk management (business risk, input/output management, risk evaluation), management system efficiency (security policy, organization, security requirements, information supply, sustained improvement, training, etc.), economic outputs (increased organization value, cost reduction, increased revenue, etc.), and legal compliance (security audit, compliance with legal contracts, regulation on protection).

2.2 Case-control Study and Measures of Association

In a case-control study [31], the subjects for analysis are classified either as a case group or as a control group depending on the outcome, and each group being compared is analyzed to determine whether it possessed a specific factor in the past. Case-control studies relies on observation and has the characteristics of a retrospective study, a type of research wherein the direction of progress runs from "result" to "cause". This method is mainly used in epidemiologic areas.

Measures of Association is used to evaluate the impact of a risk factor on the results, i.e., it is a test for determining the root cause or a correlation. It is a numerical representation of the result of comparing the characteristics among comparison groups, whereas effect size (in this paper, effect size and impact size were used in the same meaning) is a quantitative index for measuring the strength of the relationship between two variables. In order to see the differences or correlations between comparison groups, the results have to be interpreted, compared, and consolidated. Summarizing the results in the form of standardized scales makes this easy to do. In other words, an effect size of zero means that there is no difference (or correlation) between the compared groups; under the null hypothesis, the effect size is equal to zero.

The advantage in using effect size is that, first, the results of research can be interpreted not as a dichotomous value but on a continuous scale. The p-value can only be used to determine whether "a difference is significant or not significant" between groups being compared, based on a pre-determined criterion (usually the significant level). With effect size, however, it is possible to express "how much of a difference (or a correlation) there is" through a specific numerical value. Second, unlike the *p*-value, the effect size is not affected by the sample size.

When the sample (size) is small, the statistical power of p-value testing is reduced, and it can lead to an insignificant result. In contrast, when the sample (size) is large, a result that is not very significant could be interpreted to be statistically significant. Third, when effect size is used, results of various forms can be converted into common units that can be compared. When a secondary analysis is to be performed on the results obtained through different statistical methods, effect size can be used as a common scale [32]. Case-control studies are usually calculaed using the 2 × 2 table, shown in **Table 2**.

Table 2. The Basic model for 2x2 contingency table of Case-Control Study

Class		**Outcome(Result) Variable**		**Total**
		Case Group(t)	Control Group(c)	
Risk(Cause) Variable	Exposed Group(y)	a	b	a + b
	Non-exposed Group(n)	c	d	c + d
	Total	a + c	b + d	a + b + c + d

Some types of effect size are *d family (differences between standardized averages)*, *odds ratio family*, and *r family (coefficient of correlation)*. The effect size of a discrete variable can be defined using the odds ratio (OR), relative risk (RR), and risk difference (RD). The odds ratio, risk ratio, and risk scales used in this research are defined as follows.

2.2.1 Risk Ratio: Ratio of Probability of an Incident in the Two Groups

In this paper, the outcome variable is divided into a case group and a control group according to the occurrence of a security flaw. Risk Ratio (RR) is the ratio of probability of an event occurring in an exposed group to the probability of the event occurring in a comparison, non-exposed group. In other words, RR measures how many times the security flaw in the outcome variable has occurred according to whether the risk variable is exposed (Exposed, Yes or No).

In Table 2, the probability (p^y) of an incident occurring in the exposed group is a/(a+b), and the probability (p^n) of an incident occurring in the non-exposed group is $c/(c+d)$. If RR is greater (less) than 1, then it means higher rate of incidents in the exposed group (less) than that of the non-exposed group.

$$RR(risk\ ratio) = \frac{p^y}{p^n} = \frac{\frac{a}{a+b}}{\frac{c}{c+d}} = \frac{(c+d)\times a}{(a+b)\times c} \quad (1)$$

2.2.2 Odds Ratio: Ratio of Odds of Incident in the Two Groups

Odds can be defined as the ratio of the success rate (probability of an incident occurring) to the failure rate (probability of an incident not occurring). In this case, the sum of probability of an incident happening and the probability of it not happening is equal to 1. If the probability of an incident happening is assumed to be p, the probability of an incident not happening can be deduced to be $1-p$. The odds of the incident happening become $p/(1-p)$.

The probability (p^t) of an incident occurring in the case group is a/(a+c), so the $odds^t$ of an incident in the case group are as follows:

$$odds^t = \frac{p^t}{1-p^t} = \frac{\frac{a}{a+c}}{1-\frac{a}{a+c}} = \frac{\frac{a}{a+c}}{\frac{c}{a+c}} = \frac{a}{c} \quad (2), \quad odds\ ratio(OR) = \frac{odds^t}{odds^c} = \frac{\frac{a}{c}}{\frac{b}{d}} = \frac{a\times d}{b\times c} \quad (3)$$

The probability of an incident in the control group (p^c) is $b/(b+d)$; thus, the $odds^n$ of the incident happening can be calculated using the same approach. As such, the ratio of the incident *odds (odds ratio, OR)* in the two groups is as follows: If OR is larger (smaller) than 1, it means that the odds of the case group are greater (smaller) than those of the control group.

3. Research Methodology

3.1 Study Model

This research applied the case-control study method to investigate the impact of a flaw in a security control category on other control categories and the corresponding effect sizes. This research is based on the K-ISMS security control category, a category affiliated with the ISO 27001 standard for measuring the level of information protection management in enterprises. As for the study model, two models were selected to describe the impact of the occurrence of a flaw among the security control categories, and the relative effect sizes were then derived for

each model. The objective was to determine whether a flaw in the security management process (SMP) and a flaw in the security countermeasure process (SCP) could be interrelated. If there was a relationship, did the occurrence of a flaw in SMP increase the risk of a flaw occurring in SCP? What would be the size of this risk? Conversely, how great would the impact of a flaw in SCP be on a flaw in SMP? Providing answers to these issues was an additional objective of this analysis.

(Model 1) Flaw in the subgroup variable of SMP ⇒ Impacts flaw in SCP

(Model 2) Flaw in the subgroup variable of SCP ⇒ Impacts flaw in SMP

3.2 Analysis Method

3.2.1 Data collection process

The data collected in this study are the security flaw statistics data of 183 companies certified by KISA (Korea Information Security Agency) in 2013. We used the meta information of security flaw occurrence statistics (number of flaws per control item) for each security control item.

The observational variables for the analyzed data are described in **Table 3**. We divided the 104 security control items into SMP Class and SCP Class and divided the observational variables into 18 security control groups. First, the observational variable for the security management process is organized into 5 sub-variable classifications that are defined as follows:

① Establishment of Security Policies & Setting of ISMS Scope (M_EP), ② Responsibility and Security Organization (M_MR), ③ Risk Management (M_RM), ④ Implementation of Security Countermeasures (M_IC), and ⑤ Post Management (M_PM).

Second, the observational variable for the security countermeasure process is organized into 13 sub-variable classifications that are defined as follows:

① Security Policies (C_SP), ② Security Organization (C_SO), ③ Security of External Parties (C_EP), ④ Information Asset Classification (C_CL), ⑤ Education and Training on Information Security (C_ET), ⑥ Personal Security (C_PS), ⑦ Physical Security (C_PH), ⑧ System Development Security (C_DS), ⑨ Cryptography Security (C_CC), ⑩ Access Control (C_AC), ⑪ Operations Security (C_OS), ⑫ Intrusion Incident Handing (C_IH), ⑬ Disaster Recovery (C_DR).

The security flaw statistical data gathered on the 183 companies are a record of security flaws measured for each security control item (1 if a flaw occurred, 0 if no flaw occurred). These measured values were then used in calculating the average security flaw ratio for each of the 18 security control groups as shown in equation (4).

$$the\ flaw\ ratio\ of\ \ i_{th}\ \text{security control group}\ = \frac{\sum_{i=1}^{n} f_i}{n_i} \tag{4}$$

Here, f_i is the number of flaw occurrences for the i_{th} security control group, and n_i is the number of control items for the i_{th} security control group. In addition, the average security flaw ratio of the 183 companies is 11.68%. In the case of SMP, the average security flaw ratio becomes 12.25% (average number of security flaw cases: 1.47 cases). In the case of SCP, the average security flaw ratio was 11.58% (average number of security flaw cases: 10.65 cases).

Table 3. Security Controls of K-ISMS(IS = Information Security)

Class	Control Group & Acronym		Definition	# of Controls
Security Management Process (SMP)	M_EP	Establishment of Security Polices & Setting ISMS Scope	- Establish the IS policies for the organization and Set the scope of the IS management system	2
	M_MR	Responsibility and Security Organization	- Set the duties of the execution team for IS, report to management and set up decision making system	2
	M_RM	Risk Management	- Risk management method and planning, Risk identification and risk evaluation, counter measure selection	3
	M_IC	Implementation of Security Countermeasures	- Devise IS measures and verify implementation thereof, Communicate internally and educate	2
	M_PM	Post Management	- Review compliance with legal requirements - Manage K-ISMS operation, conduct regular internal audits.	3
Security Counter measure Process (SCP)	C_SP	Security Policies	- Approval of policies and notifications - Policy system & maintenance management	6
	C_SO	Security Organization	- Roles, responsibilities and systems of the organization	4
	C_EP	Security of External Parties	- Define security requirements for external parties, implement security	3
	C_CL	Information Asset Classification	- Identification of information assets & responsibilities. - Classification of information assets & handling	3
	C_ET	Education and Training on Information Security	- Education program creation, operation and evaluation	4
	C_PS	Personal Security	- IS responsibilities, human affairs regulations	5
	C_PH	Physical Security	- Physical protection, system protection, office security.	9
	C_DS	System Development Security	- Analysis & design management, implementation & transfer security, 3rd party development security.	10
	C_CC	Cryptography Security	- Password policy, password key management.	2
	C_AC	Access Control	- Access restriction policy, access authority management. - User certification and identification, access restricted areas.	14
	C_OS	Operations Security	- Operational procedures/change management, system/service operation security, Electronic commerce/transmission security, media security, login management.	22
	C_IH	Intrusion Incident Handing	- Intrusion incident response procedure, system, response & recovery.	7
	C_DR	IT Disaster Recovery Planning	- Disaster recovery system setup, countermeasure implementation.	3

3.3.2 Analysis Process

The procedures for analyzing the flaw impact size for the security control categories are as follows:

[Step 1] Selection of Case Group & Control Group: In order to create the 2x2 contingency table needed for computing the effect size, the table was divided into "case group" and "control group" according to the analysis model, as shown in **Table 4**.

In the case group, a flaw has occurred in a particular control category; in the control group, however, a flaw has not occurred in that control category.

Table 4. Selection of Case Group and Control Group (2x2 contingency table)

Model (Risk → Outcome)	Risk Variable		Outcome Variables	
	Positive	Negative	Case Group	Control Group
SCP → SMP	5 Control Groups of SCP		13 Control Groups of SMP	
	Exposed of Risk	Non-exposed	flaw	Not flaw
SMP → SCP	13 Control Groups of SMP		5 Control Groups of SCP	
	Exposed of Risk	Non-exposed	flaw	Not flaw

** SMP = Security Management Group, SCP = Security Countermeasure Process, Population at risk = 183 Samples*

In the first model (SCP → SMP), 5-Control Groups of the SMP class were selected as the outcome variables, and 13-Control Groups of the SCP class, as the risk variables. Based on the flaw occurrence in 5-Control Groups of SMP, the data were divided into the case group (a flaw occurred) or the control group (no flaw occurred). In the second model (SMP → SCP), 13-Control Groups of the SCP class were selected as the outcome variables, and 5-Control Groups of the SMP class, as the risk variables.

[Step 2] Measure of Association (Effect Size): To compute the relative flaw effect sizes, the most widely used risk scales such as odds ratio and PAR (Population at Risk) were measured. The odds ratio is an index that represents the correlation between two binary variables (column variable and row variable). If the odds ratio is close to 1, it means there is no correlation; if it is close to zero or very large, it means there is high correlation.

[Step 3] Pooled Estimation and Model Evaluation: First (test of homogeneity on the analysis model), in order to determine whether the effect sizes of individual researches were values derived from the same sample group, a test of homogeneity was performed. Statistical heterogeneity means that the measurements of the research results' process effects are statistically different from the confidence interval summary data sizes. Mixing together the research results with these characteristics could produce confounding variables in the results. Therefore, the Chi - square test was used to test the significance in the Q statistic. If the analysis relies on a small number of researches, the power of the statistical testing is reduced. Thus, the significance level must be raised; if the p value of the Q statistic is less than 0.10, it can be concluded that there is statistical heterogeneity in the researches [33]. Another way to test for heterogeneity is Higgin's statistic (I^2, [34]), which is a statistic that quantifies the degree of heterogeneity. I^2 statistic has a characteristic that is insensitive to both scale and number of studies unlike the Q statistic. I^2 has a value of 0% ~ 100%; if there is no heterogeneity, the value is 0 %. The I^2 value is increased as the heterogeneity increases.

Second, consolidation of the research results that were measured using categorical variables can be accomplished using the Mantel-Hanszel method and Logit estimation. In the Mantel-Hanszel method, the risk factor data are assumed to be a stratified sample in the analysis, and Logit estimation converts the odds ratio from each stratum into logarithmic values that are then averaged. In this paper, the Mantel-Hanszel method was applied; because

the data satisfied the heterogeneity requirement, the pooled estimate value was computed through the fixed effect model [35].

4. Result of Research

4.1 Relative Flaw Impact of Model 1 (SCP class → SMP class)

4.1.1 Flaw Effect Size of Risk Factors under the SCP Class

Table 7-(a) shows the results obtained by analyzing the effect size of the flaws for each SCP class risk factor that affects the flaws in the SMP class. In the first case, i.e., risk factors that affect the flaws in the M_EP (Establishment of Security Policies) control category, the risk factors were arranged in order of increasing flaw impact as follows: C_ET(OR:9.33), C_DR(OR:3.87), C_PH(OR:3.23), and C_EP(OR:2.48). Compared to the group where there was no occurrence of a C_ET (Education and Training on Information Security) flaw as a risk factor, for the group where the C_ET flaw occurred, the probability of M_ET flaw occurring was 9.3 times higher. Moreover, the OR (odds risk) risk scale has a confidence interval of 95% (usually based on 95% confidence interval). If a confidence interval value of 1 is included, then the null hypothesis could be established wherein OR is equal to 1 in the sample group.

Therefore, the risk factor in question can be considered to have no impact on the flaw. If a confidence interval value of 1 is not included, the impact can be said to be statistically significant. A PAR (population attributable risk) value of 75.8% means that, among the 13 risk factors affecting a flaw in the M_EP control group, C_ET has weight of 75.8%.

In the second case, i.e., flaws in M_RO (Responsibility and Organization), risk factors C_IH (Intrusion Handling) and C_DS (System Development Security) were found to affect M_RO flaws greatly, affecting them by 3.84 times and 3.34 times, respectively.

In the third case, i.e., flaws in M_RM (Risk Management), risk factors C_AC (Access Control) and C_ET (Education and Training) were found to affect M_RM flaws greatly, affecting them by 5.4 times and 1.1 times, respectively. In the fourth case, i.e., flaws in M_IC (Implementation Countermeasures), risk factor C_SO (Security Organization) was found to affect flaws greatly, affecting M_IC (Implementation Countermeasures) by 5 times. The risk factors affecting M_PM (Post Management) were found to be C_DS (System Development Security), C_SP (Security Policies), and C_PH (Physical Security) in order of decreasing impact. Note, however, that their impacts fell short of having any statistical significance.

4.1.2 Pooled Average Effect Size and Test of Homogeneity

In order to analyze the relationship model for flaws occurring between SCP ⇒ SMP, the first model, random effect model, and fixed effect model were used to test for homogeneity. The results revealed a Q statistic value of 58.76 ($p = .6818$, $df = 64$). The data from each case were judged to have been sorted systematically rather than indiscriminately. The value of I2, which measures heterogeneity, was 0%, so the model was found to be homogeneous ($p>.10$). Therefore, the fixed effect model was found to be more suitable for consolidation and was consequently selected. Based on this model, the odds ratio (OR), 95% confidence interval, and average odds ratio for each control category group were computed and tabulated in <Table 5>.

As shown in **Table 5**, the pooled average flaw effect size was 1.4, and the 95% confidence interval of this total effect size was 1.25~1.6. This is a statistically significant result that can be interpreted to mean that the SCP class flaw group has 1.4 times the effect on the SMP class

flaw. To elaborate, the SCP class flaw was found to affect the M_EP control group by 1.94 times, the M_PM control group by 1.43 times, the M_MR control group by 1.41 times, and the MR_RM control group by 1.23 times.

Table 5. Summary of the result of homogeneity test related to SMP class

Risk ⇒ Outcome		Pooled Effect Size		Test for effect size	Test for Homogeneity	
		OR	*95% CI*	*Z(p)*	*Q(p)*	I^2
SCP ⇒	M_EP	*1.94*	*[1.37; 2.74]*	*3.74 (p = .00)*	*11.76(.4653)*	*0%*
	M_RO	*1.41*	*[0.99; 2.01]*	*1.92 (p = .05)*	*10.70(.5550)*	*0%*
	M_RM	*1.23*	*[1.01; 1.49]*	*2.08 (p = .03)*	*16.10(.1869)*	*25.4%*
	M_IC	*1.38*	*[0.85; 2.23]*	*1.30 (p = .19)*	*9.22(.6839)*	*0.0%*
	M_PM	*1.43*	*[1.19 1.73]*	*3.76 (p = .00)*	*5.80(.0957)*	*0%*
Overall (Fixed effects)		*1.40*	*[1.25; 1.6]*	*5.72(p <.0001)*	*58.76(.6618)*	*0%*

** OR = Odds Ratio; CI = Confidence Level, Q = Q statistics, I^2 =Higgin's statistics, Z = Z-value, P =p-value*

4.2 Relative Flaw Impact of Model 2 (SMP class → SCP class)

4.2.1 Flaw Effect Size of Risk Factors under the SCP Class

Table 7-(b) shows the results obtained by analyzing the effect size of flaws for each of the 5 risk factors belonging to the SMP class and affecting flaws in the SCP class. The case groups that showed statistically significant results ($p < 0.05$, inclusion of 1 in the 95% confidence interval) were C_SO (Security Organization), C_ET (Security of External Parties), C_PH (Physical Security), C_DS (System Development Security), C_AC (Access Control), C_IH (Incident Handling), and C_DR (Disaster Recovery).

The M_IC (Implementation of Security Countermeasures) flaw was found to be a risk factor that was highly correlated with flaws in the C_SO control group. The effect size on the C_SO flaw was 7.46 times, having flaw impact weight of 12.2%.

M_EP (Establishment of Security Policies & Setting of ISMS Scope) and M_RM (Risk Management) were the flaws that were found to be the risk factors with the closest correlation with flaws in the C_ET control group. The effect sizes on the C_ET flaw were 18.46 times and 2.19 times, respectively. The flaw impact weights were computed to be 36.5% and 16.3%, respectively, showing that their influence is strong.

M_EP (Establishment of Security Policies & Setting of ISMS Scope, OR=4.77) and M_PM (Risk Management, OR=2.07) were the flaws that were found to be the risk factors with the closest correlation with flaws in the C_PH control group. The flaw impact weights were M_PM (Par=17.1%) and M_EP (PAR=13.9%), indicating strong influence. The effect sizes of the risk factors on the C_DS control group flaws were found to be M_RO (Management Responsibility and Organization, OR=5) and M_PM (Post Management, OR= 1.99). The flaw impact weights were M_PM (PAR=15%) and M_RO (PAR=13.9%), indicating strong influence.

The M_RM (Risk Management) flaw was found to be a risk factor having close correlation with flaws in the C_AC control group. The effect size on the C_AC flaw was 8.91 times, and the flaw impact weight was 53.8%, again showing high degree of influence. The M_RO

(Management Responsibility and Organization) flaw was found to be a risk factor having close correlation with flaws in the C_IH control group. The effect size on the C_IH flaw was 3.94 times, and the flaw impact weight was 13.6%.

The effect sizes of the risk factors on the C_DR control group flaws were found to be M_EP (Establishment of Security Policies & Setting of ISMS Scope, OR=4. 39) and M_RM (Risk Management, OR= 2.69). The flaw impact weights were M_RM (PAR=17. 2%) and M_EP (PAR=16. 1%), respectively, indicating strong influence.

4.2.2 Pooled Average Effect Size & Test of Homogeneity

The analysis of the impacts relationship for flaws occurring between SMP ⇒ SCP as the second model (**Table 6**) revealed a Q statistic value of 76.3(p=.1394, df=64). The value of I^2, which measures heterogeneity, was 16.1%, so the model was found to be homogeneous (p>0.10). Therefore, the fixed effect model was more suitable for consolidation and was selected accordingly. As shown in **Table 6**, the pooled average effect size for model 2 was 1.37, with the 95% confidence level computed to be 1.19~1.56. This total OR risk estimation value was a statistically significant result. When the flaw effect size of the SCP class was analyzed using (Z = 4.63, P <.01), the risk factors were found to be C_ET (Education and Training, OR=1. 94), C_PH (Physical Security, OR=1. 83), and C_DR (IT Disaster Recovery Planning, OR=1. 70), in decreasing order of influence.

Table 6. Summary of the result of homogeneity test related to SCP class

Risk ⇒ Outcome		Pooled Effect Size		Test for effect size	Test for Homogeneity	
		OR	*95% CI*	*Z(p)*	*Q(p)*	*I2*
SMP ⇒	C_SP	*1.31*	*[0.88; 1.95]*	*1.33(p=0.1824)*	*0.86(0.7866)*	*0.0%*
	C_SO	*1.53*	*[1.00; 2.35]*	*1.97(p=0.0489)*	*2.97(0.5633)*	*0.0%*
	C_EP	*1.29*	*[0.88; 1.91]*	*1.30(p=0.1936)*	*3.77(0.4383)*	*0.0%*
	C_CL	*1.21*	*[0.83; 1.77]*	*1.0(p=0.3110)*	*2.17(0.7037)*	*0.0%*
	C_ET	*1.94*	*[1.18; 3.21]*	*2.59(p=0.0096)*	*5.85(0.2109)*	*31.6%*
	C_PS	*1.15*	*[0.77; 1.71]*	*0.69(p=0.4911)*	*3.48(0.4806)*	*0.0%*
	C_PH	*1.83*	*[1.25; 2.68]*	*3.11(p=0.0019)*	*2.87(0.5806)*	*0.0%*
	C_DS	*1.15*	*[0.79; 1.68]*	*0.56(p=0.5738)*	*14.54(0.0057)*	*72.5%*
	C_CC	*0.92*	*[0.65; 1.31]*	*-0.24(p=0.8131)*	*5.99(0.1996)*	*33.3%*
	C_AC	*1.58*	*[0.74; 3.36]*	*0.68(p=0.4958)*	*7.43(0.1146)*	*46.2%*
	C_OS	*1.07*	*[0.43; 2.64]*	*0.15(p=0.8845)*	*1.63(0.8041)*	*0%*
	C_IH	*1.48*	*[0.94; 2.35]*	*1.68(p=0.0927)*	*4.62(0.3280)*	*13.5%*
	C_DR	*1.70*	*[1.07; 2.70]*	*1.56(p=0.1179)*	*6.82(0.1458)*	*41.3%*
Total (Fixed effects)		*1.37*	*[1.19;1.56]*	*4.63(p=0.0001)*	*76.3(0.1394)*	*16.1%*

** OR = Odds Ratio; CI = Confidence Level, Q = Q statistics, I^2 =Higgin's statistics, Z = Z-value P =p-value*

Table 7-(a). The results by analyzing the effect size of the flaws for each SCP class risk factor that impacts the flaws in the SMP class

* *OR = Odds Ratio; CI = Confidence Interval(Significance level 95%); PAR=Population Attributable Risk; M_EP = Establishment of security policies and scope; M_MR = Responsibility and Organization; M_RM = Risk Management; M_IC = Implementation of Countermeasures; M_PM = Post Management; C_SP = Security Policies; C_SO = Security Organizations; C_EP = Security of External Parties; C_CL = Information Asset Classification; C_ET = Education and training on Information Security; C_PS = Personal Security; C_PH = Physical Security; C_DS = System Development Security; C_CC = Cryptography Security; C_AC= Access Control; C_O = Operations Security; C_IH= Intrusion Incident Handling; C_DR = IT Disaster Recovery Planning*

Types of Control-case	Outcome Variable														
	Case 1: M_EP			Case2: M_RO			Case3: M_RM			Case4: M_IC			Case5: M_PM		
	OR	95% CI	PAR	OR	95% CI	PAR	OR	95% CI	PAR	OR	95% CI	PAR	OR	95% CI	PAR
Risk(Cause) variables															
C_SP	1.21	[0.39~3.74]	0.054	0.95	[0.29~3.18]	-0.013	1.2	[0.62~2.33]	0.021	1.84	[0.40~8.51]	0.189	1.78	[0.93~3.42]	0.079
C_SO	1.29	[0.39~4.28]	0.055	2.05	[0.65~6.50]	0.172	1.1	[0.53~2.25]	0.008	5.01	[1.07~23.37]	0.448	1.73	[0.85~3.54]	0.057
C_BP	2.48	[0.85~7.20]	0.3	0.52	[0.14~1.95]	-0.179	1.15	[0.61~2.17]	0.018	1.53	[0.33~7.04]	0.143	1.59	[0.85~2.97]	0.072
C_CL	1.74	[0.53~5.68]	0.293	1.1	[0.35~3.42]	0.053	1.17	[0.63~2.16]	0.038	0.8	[0.17~3.69]	-0.137	0.96	[0.53~1.75]	-0.012
C_ET	9.33	[2.04~42.65]	0.758	1.25	[0.42~3.73]	0.094	2.02	[1.09~3.74]	0.118	1.68	[0.36~7.70]	0.223	1.25	[0.70~2.25]	0.047
C_PS	2.47	[0.84~7.20]	0.261	0.69	[0.18~2.57]	-0.089	1.06	[0.54~2.07]	0.006	2	[0.43~9.27]	0.208	1	[0.52~1.90]	0
C_PH	3.23	[0.88~11.85]	0.531	1.95	[0.59~6.46]	0.33	1.35	[0.74~2.46]	0.066	4.67	[0.55~39.58]	0.665	1.77	[0.98~3.20]	0.153
C_DS	1.78	[0.59~ 5.42]	0.274	3.38	[0.91~12.53]	0.533	0.62	[0.34~1.13]	-0.099	0.63	[0.13~2.88]	-0.245	1.79	[0.99~3.21]	0.147
C_CC	0.75	[0.26~ 2.20]	-0.12	2.2	[0.71~6.85]	0.333	0.87	[0.48~1.58]	-0.025	1.56	[0.34~7.19]	0.2	1.7	[0.94~3.05]	0.114
C_AC	∞	[0.4~43.87]	-	0.91	[0.11~7.57]	-0.089	5.41	[1.41~20.73]	0.595	0.4	[0.04~3.62]	-1.179	1.63	[0.50~5.34]	0.214
C_OS	∞	[0.08~26.42]	-	0.48	[0.05~4.28]	-0.867	1.22	[0.26~5.62]	0.075	-	[0.03~12.74]	-	1.53	[0.33~7.03]	0.191
C_IH	1.02	[0.27~3.83]	0.004	3.48	[1.12~10.75]	0.289	1.79	[0.81~3.99]	0.042	0.67	[0.08~5.76]	-0.067	1.14	[0.55~2.36]	0.012
C_DR	3.87	[1.30~11.46]	0.327	1.04	[0.28~3.95]	0.008	1.98	[0.89~4.37]	0.051	0	[0.01~4.29]	-0.262	1.28	[0.62~2.64]	0.024

Table 7-(b). The results by analyzing the effect size of the flaws for each SMP class risk factor that impacts the flaws in the SCP class

① Case 1~5: C_SP, C_SO, C_EP, C_CL, C_ET

Types of Control-case		Outcome Variable														
		Case 1: C_SP			Case 2: C_SO			Case 3: C_EP			Case 4: C_CL			Case 5: C_ET		
		OR	95% CI	PAR	OR	95% CI	R ¬	OR	95% CI	PAR	OR	95% CI	PAR	OR	95% CI	PAR
Risk variables	M_EP	1.34	[0.43~4.12]	1.6%	1.41	[0.42~4.67]	2.1%	2.87	[0.99~8.32]	9.5%	2.28	[0.7~7.46]	5.2%	18.46	[4.04~84.43]	36.5%
	M_RO	1.05	[0.31~3.5]	-0.3%	2.29	[0.72~7.26]	6.6%	0.57	[0.15~2.12]	-3.6%	1.35	[0.43~4.21]	0.7%	1.45	[0.49~4.31]	1.7%
	M_RM	1.15	[0.59~2.27]	3.3%	1.3	[0.61~2.77]	5.7%	1.06	[0.55~2.04]	1.6%	1.59	[0.85~2.97]	10.7%	2.19	[1.15~4.16]	16.3%
	M_IC	2.43	[0.53~11.25]	2.9%	7.46	[1.6~34.8]	12.2%	2.02	[0.44~9.31]	1.9%	1.18	[0.26~5.45]	-0.7%	2.49	[0.54~11.44]	2.4%
	M_PM	1.56	[0.8~3.05	9.8%	1.29	[0.62~2.66]	5.8%	1.46	[0.77~2.79]	8.7%	0.91	[0.49~1.69]	-1.8%	1.42	[0.78~2.6]	8.2%

② Case 6~10: C_PS, C_PH, C_DS, C_CC, C_AC

Types of Control-case		Case 6: C_PS			Case 7: C_PH			Case 8: C_DS			Case 9: C_CC				
		OR	95% CI	PAR	OR	95% CI	PAR	OR	95% CI	PAR	OR	95% CI	PAR	OR	95% CI
Risk variables	M_EP	2.8	[0.96~8.16]	9.4%	4.77	[1.3~17.54]	13.9%	2.19	[0.72~6.68]	5.4%	0.69	[0.24~2.03]	-2.7%	-1.06	-
	M_RO	0.75	[0.2~2.81]	-2.3%	2.56	[0.77~8.49]	6.2%	5	[1.35~18.56]	13.9%	2.25	[0.73~6.97]	5.0%	∞	-
	M_RM	0.91	[0.46~1.79]	-2.0%	1.27	[0.69~2.36]	5.7%	0.46	[0.24~0.86]	16.9%	0.57	[0.32~1.01]	-13.2%	8.91	[2.32~34.22]
	M_IC	2.65	[0.57~12.26]	3.5%	∞	-	11.7%	0.82	[0.18~3.79]	-1.4%	1.94	[0.42~8.89]	1.0%	∞	-
	M_PM	1.09	[0.56~2.12]	2.1%	2.07	[1.13~3.79]	17.%	1.99	[1.09~3.64]	16.0%	1.29	[0.74~2.26]	6.3%	0.68	[0.2~2.35]

③ Case 11~13: C_OS, C_IH, C_DR

Types of Control-case		Outcome Variable								
		Case 11: C_OS			Case 12: C_IH			Case 13: C_DR		
		OR	95% CI	PAR	OR	95% CI	PAR	OR	95% CI	PAR
Risk variables	M_EP	-0.56	-	-	1.11	[0.3~4.15]	0.2%	4.39	[1.48~13.01]	16.1%
	M_RO	∞	-	-3.8%	3.94	[1.27~12.2]	13.6%	1.14	[0.3~4.31]	0.3%
	M_RM	0.48	[0.09~2.57]	-5.4%	2.02	[0.86~4.74]	13.2%	2.69	[1.11~6.52]	17.2%
	M_IC	-0.25	-	-	0.8	[0.09~6.86]	-1.2%	0	-	-4.0%
	M_PM	2.44	[0.53~11.24]	21.4%	0.99	[0.47~2.09]	-0.1%	1.1	[0.53~2.31]	2.4%

5. Conclusion

5.1 Result Analysis

The IT environment surrounding an enterprise is dynamic and is constantly changing, and these conditions give rise to a unique combination of characteristics for each enterprise. This produces different risk sizes faced by each enterprise, even for the most accurate security control item. Traditional information protection level measurement methods such as ISO27001 can only determine the existence of flaws for each security area and measure the security protection level, and only when a certain level has been attained. Thus, the internalized risks and levels existing in enterprises cannot be reflected on its measurement despite the diverse IT environments faced by enterprises.

This research analyzed the sizes and importance of relative flaw impact among security control items in order to establish a basis for making correct investment decisions on security policies, budget, and investments in human resources. Instead of developing new measurement indices, this paper examined the empirical data (consolidated statistical meta-data of 183 companies) on the flaws affiliated with K-ISMS, which falls under ISO 27001 as the most widely used standard. The main results of this research can be summarized in **Fig. 1**:

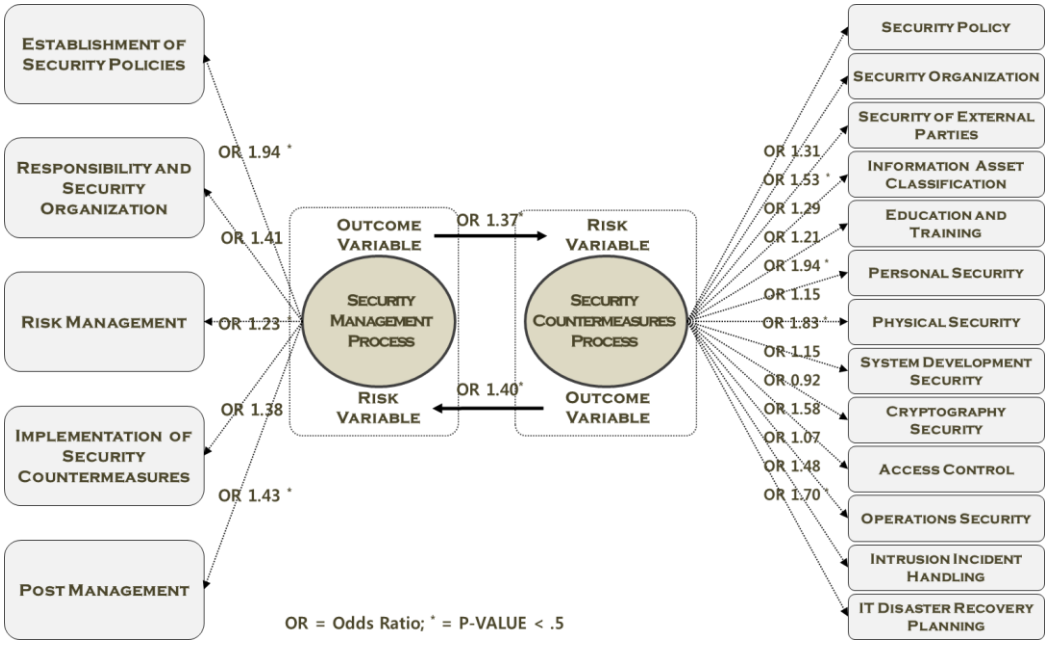

Fig 1. Results of the effect model of flaws between SMP class and SCP class

First, investigation of the flaw impact between SMP class and SCP class revealed 13 risk factors in the SCP class to be the causal factors for 5 SMP class flaws, with the pooled average effect size equal to 1.4 times. In detail, the SCP class flaw was found to affect the M_EP control group by 1.94 times, the M_PM control group by 1.43 times, the M_MR control group by 1.41 times, and the MR_RM control group by 1.23 times. Inversely, 5 risk factors in the SMP class were the causal factors for 13 SCP class flaws, with the pooled average effect size

equal to 1.37 times. To elaborate, the SMP class flaws were in order of C_ET (Education and Training, OR=1. 94), C_PH (Physical Security, OR=1. 83), and C_DR (IT Disaster Recovery Planning, OR=1. 70).

Second, when the results of this research were compared with previous research results [10] (since the research objectives and methodologies were different, direct comparison was difficult, and only the results were compared), differences were found in the experts' analysis of security control items, investment priorities, and flaw impact sizes. For example, experts judged intrusion incidents to be most important, yet in reality, investments in disaster response were given the highest priority. Still, the research results indicated that the size of effect of the risk factor on the security control flaw was the biggest and most critical element in education and training. This implies that enterprises should manage flaws by considering flaw impacts and criticality and stop focusing on setting quality targets for information security levels.

Table 8. Comparison with previous research results using AHP [10] in terms of importance (The order of importance (these research results) was determined based on the flaw effect size from the Model1 analysis results: the order of effect sizes when Model1 (SCP ⇒ SMP) = SCP class is a risk factor for SMP class flaws, ES=Effect Size, Overall ES=average flaw effect size.)

13 Groups of Security Control Group in SCP Class	The result of AHP		These results			
			Model1			Model2
	Expert Priority	Investment Priority	Priority	ES	Related SMP	Average ES
Security Policies	7	13	11	1.84	M_IC	7(1.31)
Security Organization	10	11	3	5.01	M_IC	5(1.53)
Security of External Parties	11	8	8	2.48	M_EP	8(1.29)
Information Asset Classification	12	10	12	1.74	M_EP	9(1.21)
Education and training	5	12	1	9.33	M_EP	1(1.94)
Personal Security	3	9	9	2.47	M_EP	10(1.15)
Physical Security	6	3	4	4.67	M_IC	2(1.83)
System Development Security	8	6	7	3.38	M_RO	10(1.15)
Cryptography Security	13	7	10	2.20	M_RO	13(0.92)
Access Control	2	2	2	5.41	M_IC	4(1.58)
Operations Security	9	5	13	1.53	M_PM	12(1.07)
Intrusion Incident handing	1	4	6	3.48	M_RO	6(1.48)
IT Disaster Recovery Planning	4	1	5	3.87	M_EP	3(1.70)

* 'Model1' values are extracted from Table 7-a, and 'Model2' values are extracted from Table 6.

5.2 Application of Results and Discussions

Through the proposed model, first, statistical methods and empirical data were applied in quantifying the impacts of a flaw on security controls. This approach prevented the subjective judgment of experts from adding bias when determining the relative impacts (or weights) of the items for measurement. Second, the problem of security level measurement was approached not as an issue of quality but as an inherent flaw in security control. Individual weights were calculated for each type of flaw so that an objective method of making measurements could be proposed along with the empirical data. Third, the priority level of flaws could be ascertained when faced with the problem of managing the security control flaws in an enterprise. This is expected to be able to help in the selective removal of flaws.

The following suggestions can be made regarding the significance of this research and its applications.

First, the 104 certification criteria of K-ISMS (used in Korea for general purposes) were used to measure the information protection level rather than develop a new security control item or a measurement index. These criteria are closely related not only with Korea's K-ISMS certification program but also with ISO 27001. Therefore, the criteria can easily be adopted by other certification programs.

Normally, in the K-ISMS certification audit scenario, the certification audit team carries out a documentary audit and a field audit at the same time. These audits follow the certification criteria for the information protection management system (104 security control items). Based on examinations of the company's policies concerning the information protection management system, corroborating documents, and field audits, the auditors review each security control item to see if a flaw had occurred. The auditors then discuss the number of flaw cases and severity of the cases in order to prepare a report. The methodologies used in this research and its results could be utilized when writing this report. To put it in another way, when evaluating the results of the certification audit, in most cases, auditors today simply assign the same relative weight to all the security control items for which a flaw has occurred or rely on their subjective judgements when assigning values to the relative weights. Still, a security flaw may have important attributes that can be overlooked. The analysis of the relative influences of a flaw on other security control items could be carried out insufficiently. In such situations, the relative weights derived through this research could be applied in producing results that could be more meaningful.

Secondly, the research could be used as objective backup evidence when establishing national policies on information protection. For example, there could be times when common certification criteria for consolidating several different certification criteria must be derived, and a new set of security control items must be developed for a specific field. Instead of looking for security control items that could be overlapping, the security control items could be analyzed for influential relationships in order to derive commonalities. This way, when an overlap is found, the control item could be included in the commonalities. This idea could be illustrated by taking the example of personal information leaks. Personal information leaks that occur today are caused most of the time by problems with access control. The results of this research showed that access control was ranked 2^{nd} in terms of its influence among security control items. Access control is also the area examined most closely during certification audits. The results of this research could be used as basis for making the policy decision to include access control in the commonalities.

Third, it is possible to establish a system for continually measuring the relative weights of the security control items. Currently, once the criteria used in certification audits are firmly established, they are continually used without undergoing any significant revisions. There is always the risk that a security control item could be given diverging assessments tinted by subjective biases. Together, these conditions make it very difficult to manage security flaws and quality at a level commensurate with the results of the certification audit. Consequently, responding immediately to the latest security threat changes becomes difficult. If the changes in the relative weights of the information protection certification criteria (or security control items) are measured annually and publicized, such could become an effective decision making tool (for example, to determine the ranking of security flaws) for auditors.

Fourth, guidelines have to be developed, and long-term investigation has to be launched to study cases involving deficiencies in the current information protection certification scheme.

Many different factors could be at play when a security flaw occurs in a company environment. To prevent recurrences of similar cases, the company must be constantly monitored by auditors; presently, however, each audit agency internally manages the certification audit results and chooses not to disclose them. Under these circumstances, it becomes impossible to build upon previous audit experiences. If case analysis results and data on security flaw cases can be made available in the form of guidelines to the extent that they will not include confidential company information, then it will become possible to do better research such as identifying the areas in the certification scheme that are in need of improvements.

5.3 Limitations and Future Research

The purpose of this research was to find a way to remove the subjective biases of the auditors and prevent the use of the same relative weight for all the security control items when analyzing the effect of occurrence of a security flaw on other K-ISMS security control items. For this purpose, a statistical method based on probability (case-control technique) was applied to obtain some objective means of determining the relative weights with which the occurrence of a security flaw affects the other security control items. Note, however, that this research paper has the following limitations, so additional research must be done:

First, the data collected and analyzed in this research were obtained from the K-ISMS certification audit carried out in 2013. The sourced data come from part of the statistical data (number of flaws occurring for each security control item). Even this data set was used on a limited basis. Such usage limitation was due to the fact that the certification audit results were considered a company's confidential information. Since data were insufficient for a detailed analysis, it was difficult to evaluate in depth the effectiveness of the proposed model using only the meta-statistics. For further research, the different cases of security flaws should be classified according to the type of business, and then the flaw types and relative weights must be studied. The results must then be applied to sample cases of cyber security breaches in companies so that the effectiveness of the research results could be validated.

Second, this research lacks chronological analysis that uses data from several years past. This research is meaningful because the proposed method of analysis provides an objective rationale. On the other hand, the results lack consistency because the small sample size produces too much deviations.

Therefore, additional research in the future must focus on improving the accuracy and reliability of the method proposed in this paper. This can be accomplished by measuring the relative weights of flaws for each year, and then performing a chronological study of how the values of the weights change over time. Continually updating the relative weights of the security control items is a very important task since they can be used as objective justifications by companies managing their information protection levels.

References

[1] S. Jang, "Analysis of International and Korea trend ralated to Information Security Level Assessment," *IITP Weekly Report*, pp. 15-22, Decemver 2011. Article (CrossRef Link)

[2] K. Yoon, "Developing Policy Alternatives to Improve information security system in public sector," *Korea Institute of Public Administration*, 2013. Article (CrossRef Link)

[3] Y. Back, "A Study on Inspection Method of Vulnerability related to Information Systems in the Public Sector," *Audit and Inspection Research Institute*, April 2015. Article (CrossRef Link)

[4] W. H. Baker and L. Wallace, "Is Information Security under control?: Investing Quality in Information Security Management," *IEEE Security & Privacy*, vol. 5, no. 1, pp. 36-44, 2007. Article (CrossRef Link)

[5] H. Lee and J. Lim, "A Study on the development of corporate information security level assessment models," *Journal of The Korea Institute of Information Security and Cryptology*, vol. 18, no. 5, pp. 161-170, October 2008. Article (CrossRef Link)

[6] M. Ko and T. Kim, "Using a Balanced Scorecard Framework to Evaluate Corporate Information Security Level," in *Proc. of the conference AMCIS*, 2009. Article (CrossRef Link)

[7] C. W. Hsu, "Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in and Organization," *European Journal of Information Systems*, vol. 18, no. 2, pp. 140-150, March 2009. Article (CrossRef Link)

[8] K. Kim and S. Kim, "Evaluation Criteria for Korean Smart Grid based on K-ISMS," *Journal of The Korea Institute of Information Security and Cryptology*, vol. 22, no. 6, pp. 1375-1391, December 2012. Article (CrossRef Link)

[9] K. Kim, O. Heo and S. Kim, "A Security Evaluation Criteria for Korean Cloud Computing Service," *Journal of The Korea Institute of Information Security and Cryptology*, vol. 23, no. 2, pp. 3-17, April 2013. Article (CrossRef Link)

[10] C. Lee, J. Kim and C. Lee, "A comparative study on the priorities between perceived importance and investment of the areas for Information Security Management System," *Journal of The Korea Institute of Information Security & Cryptology*, vol. 24, no. 5, pp. 919-929, October 2014. Article (CrossRef Link)

[11] A. R. Otero, "An information security control assessment methodology for organizations' financial information," *International Journal of Accounting Information Systems*, vol. 18, pp. 26-45, September 2015. Article (CrossRef Link)

[12] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438-457, Nov. 2012. Article (CrossRef Link)

[13] A. Gupta and R. Hammond, "Information Systems Security Issues and Decisions for Small Business: An Empirical Examinations," *Information Management & Computer Security*, vol. 13, no. 4, pp. 297-310, 2005. Article (CrossRef Link)

[14] S. Jang, S. Lee and B. Noh, "The effects of the operation of an information security management system on the performance of information security," *Journal of The Korea Institute of Information Security & Cryptology*, vol. 22, no. 5, pp. 1123-1132, October 2012. Article (CrossRef Link)

[15] K. Kong, S. Jung and S. Yeon, "Information Security and Organizational Performance: Empirical Study of Korean Securities Industry," *ETRI Journal*, vol. 37, no. 2, pp. 428-437, April 2015. Article (CrossRef Link)

[16] S. Ransbotham and S. Mitra, "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research*, vol. 20, no. 1, pp. 121-139, 2009. Article (CrossRef Link)

[17] H. Jo, S. Kim and D. Won, "Advanced Information Security Management Evaluation System," *KSII Transactions on Internet and Information Systems*, vol. 5, no. 6, pp. 1192-1213, June 2011. Article (CrossRef Link)

[18] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler and R. W. Boss, "If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security," *European Journal of Information Systems*, vol. 18, no. 2, pp. 151-164, 2009. Article (CrossRef Link)

[19] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality based Beliefs and Information Security Awareness," *MIS Quartely*, vol. 34, no. 3, pp. 523-548, 2010. Article (CrossRef Link)

[20] J. H. Hall, S. Sarkani and T. A. Mazzuchi, "Impacts of organizational capabilities in information security," *Information Management & Computer Security*, vol. 19, no. 3, pp. 155-176, 2011. Article (CrossRef Link)

[21] S. Kim, K. Yang and S. Park, "An Integrative Behavioral Model of Information Security Policy Compliance," *The Scientific World Journal*, vol. 2014, pp. 1-12, 2009. Article (CrossRef Link)

[22] J. L. Spears and H. Barki, "User Participation in Information Systems Security Risk Management," *MIS Quartely*, vol. 34, no. 3, pp. 503-522, 2010. Article (CrossRef Link)

[23] H. Kim, K. Lee and J. Lim, "A Study of K-ISMS Fault Analysis for Constructing Secure Internet of Things Service," *International Journal of Distributed Sensor Networks*, vol. 11, no. 9, pp. 1-12, September 2015. Article (CrossRef Link)

[24] KISA, "The Guide of Information Security Management System in Korea(K-ISMS)," *Korea Information&Security Agency*, 2014. Article (CrossRef Link)

[25] ISO/IEC JTC1 SC27, "ISO 27001:2013 Information technology - Information Security Management System," *ISO/IEC*, 2013. Article (CrossRef Link)

[26] NIST, "SP 800-53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations," *National Institute of Standards and Technology*, December 2014. Article (CrossRef Link)

[27] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Information & Management*, vol. 46, no. 5, pp. 267-270, June 2009. Article (CrossRef Link)

[28] ISM3 Consortium, "ISM3: Information Security Management Maturity Model," *Open Group*, 2009. Article (CrossRef Link)

[29] Virtual Corporation, "BCMM: Business Continity Maturity Model," *Virtual Corporation*, 2007. Article (CrossRef Link)

[30] ISO/IEC JTC1 SC27, "ISO 27004: ISMS Measurement," *ISO/IEC*, 2009. Article (CrossRef Link)

[31] Wikipedia, "Case-Control Study," [Online]. Available: Article (CrossRef Link).

[32] H. Kang, "Statistical Consideration in Meta-Analysis," *Hangyang Medical Reviews*, pp. 23-26, 2015. Article (CrossRef Link)

[33] R. Robert and R. B. Donald, "Comparing effect sizes of idependent studies," *Psychological Bulletin*, vol. 92, no. 2, pp. 500-504, September 1982. Article (CrossRef Link)

[34] J. P. Higgins, S. G. Thompson, J. J. Deeks and D. G. Altman, "Measuring inconsistency in meta-analyses," *British Medical Journal*, vol. 327, no. 7414, pp. 557-560, September 2003. Article (CrossRef Link)

[35] J. Lau, J. PA and C. HS, "Quantit ativ e Synth esis in Sy st emic Reviews," *Annals of Int ern al Medicin e*, vol. 127, no. 9, pp. 820-826, 1997. Article (CrossRef Link)

Hwankuk Kim received the B.S. and M.S. degrees in computer engineering from Hankuk Aviation University, Korea, in 1998 and 2001. and Ph.D. in the graduate school of Information Security at Korea University, in 2017. He was as a researcher at ETRI until 2006 and currently is a team manager in Cyber Security R&D at KISA. His current research interesting include ISMS, IoT Security, Vulnerability analysis, wireless network secrity and its application, etc.

Kyungho Lee received his Ph.D. degree from Korea University. He is now a Professor in the Graduate School of Information Security at Korea University, and leading the Risk management Laboratory in Korea University since 2011. He has a high level of theoretical principles as well as on-site experience. He was a former CISO in Naver corporation and the CEO of SecuBase corporation. His research interests include information security management system(ISMS), risk management, information security consulting, privacy policy, and privacy impact assessment(PIA).

Jongin Lim received the BS, MS, and Ph.D. degrees in the Department of Mathematics at Korea University. Seoul in 1980, 1982 and 1986. Currently he is a professor of the Graduate School of Information Security at Korea University. Also, he served as a Special Advisor to the President for National Security, Republic of Korea in 2015. His main research interest include National Cyber Security Policy, Cyber Warfare, Convergence Security, and Privacy.