International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.147-160
http://dx.doi.org/10.14257/ijsia.2014.8.6.14

Study on Financial-sector Information Security Level Assessment and Improvement Anticipation Model

Young-Rai Park[1], Yoon-Chul Choy[2] and Won-Sung Shon[3]

[1]Dept. of Computer Science, Yonsei University, Seoul, Korea,
pyr20210@naver.com
[2]Dept. of Computer Science, Yonsei University, Seoul, Korea,
ycchoy@rainbow.yonsei.ac.kr
[3]Dept. of Computer Education, Gyeongin National University of Education, Incheon,
Korea, sohnws@gmail.com

Abstract

Infringement threats to the financial sector have become more sophisticated and intelligent. In order to more effectively respond to such threats, the financial sector faces the need to perform the assessment of information security maturity level on a voluntary basis in order to better understand organizational information security situation and improve own vulnerabilities to reinforce information security. The study, in reflection of financial industrial environmental characteristics, builds a comprehensive and systematic information security assessment indices specialized in the financial sector while presenting an information security maturity level assessment model based on the indices as well as an information security improvement anticipation model through vulnerability remedy. The quantification of vulnerability levels of the control item suggested herein and the improvement anticipation model based on vulnerability correction, in particular, supports an organization under the assessment to address its vulnerabilities to effectively enhance organizational information security. In the absence of such an information security assessment model, the financial sector has poorly performed in assessing own information security activities. With the models suggested herein being in place, the sector is expected to make an active use of it to facilitate information security assessment and improve the general information security maturity level of individual financial institutions and the financial industry as a whole

Keywords: *information security, information security maturity level, assessment indices, information security management systems*

1. Introduction

Recently, the financial sector, in step with the information communication technology (ICT) development, has seen rapidly surging number of Internet Banking and other types of electric financial transactions. As an adverse effect of this trend, infringement accidents have become more and more frequent such as massive personal information leakage, customer PC and financial company PC hacking accidents, DDOS (distributed denial of service) attack-caused business suspension, *etc.*, The South Korean government, to secure the stability and reliability of electronic financial transactions, has amended electronic finance-related laws and regulations including the Electronic Financial Transaction Act to require the financial industry to reinforce its information security measures. The financial sector has engaged in

ISSN: 1738-9976 IJSIA

much effort in terms of management, physical resources and technological protection. However infringement accidents have continued and such efforts have been less than expectation.

To effectively respond to the ever-sophisticating and smarter threats, it is all the more important for the financial sector to continue to evaluate the application extent of its information security measures applied to organizations and address vulnerabilities for enhanced information protection. In this sense, the financial supervisory authority has actively recommended to assess financial information security levels on the voluntary basis of the financial sector. But as there is no information security assessment tool optimized for the financial sector, financial industrial assessment performance has been very low, failing to meet the expected level given the investment in information security. Recent South Korean information security assessment activities have been stimulated in governmental and public organization under the lead of the government. But in the private sector, such efforts have been insignificant due to the lack of appropriate assessment tool. For information security assessment promotion, the communication, national defense and education sectors have actively performed studies on building sector-specific assessment indices and an information security assessment model. However, the existing information security assessment models have only much specialized evaluation indices only to the individual corresponding segment, posing many difficulties in applying to the financial sector as they are. Also the existing assessment models tend to focus on assessing information security levels while not suggesting how to address vulnerabilities and leaving it to subject organization for its own. For these reasons, they are limited in enhancing information security at a more practical level.

In this study, we place our priority consideration on the environmental characteristics of South Korean financial industry where the compliance of information protection measures in electronic finance-related laws and regulations are strongly required in structuring financial-sector information security assessment indices reflecting the information-security control items of related domestic laws as well as standard control items of internal/external information protection management systems. Furthermore, based on the indices, we plan to suggest an information security level improvement model through proper treatment of vulnerabilities and information security assessment with a view to laying a foundation for activated financial-industry information security assessment.

Following this, in Chapter 2, financial-sector information security assessment indices are explained. Chapter 3 deals with information security maturity levels and its improvement assessment model. Chapter 4 verifies the model effectiveness through cases of actual application and concludes in Chapter 5.

2. Designing Financial-sector Information Security Assessment Indices

For the assessment indices suggested in this research, financial sector-specific information security control items were selected for evaluation in reflection of the information security control items of ISO 27001 – internal/external standard information security management system (ISMS) – and K-ISMS (Korean version of ISMS) within the scope of the domestic electronic finance-related laws and regulations on information security [1-3]. First, financial information security control items (223 sub-areas in 7 areas) were identified in the process of literature review on applicable laws such as the electronic financial transactions act and electronic financial supervisory rules to be complied with by South Korean financial institutions. Since the information security control items in applicable laws define the minimum necessary items required for the stability of electronic financial transactions, these, alone, are limited in more comprehensive and systemized information security in the financial sector. Therefore, to supplement them, we compared and examined information security control items applied to internal/external standard information security management systems and identified indispensable items for financial-sector information security to add to the financial-sector information security assessment indices [16]. The final results are shown in Figure 1. Establishment process of financial-sector Information Security Assessment Indices.

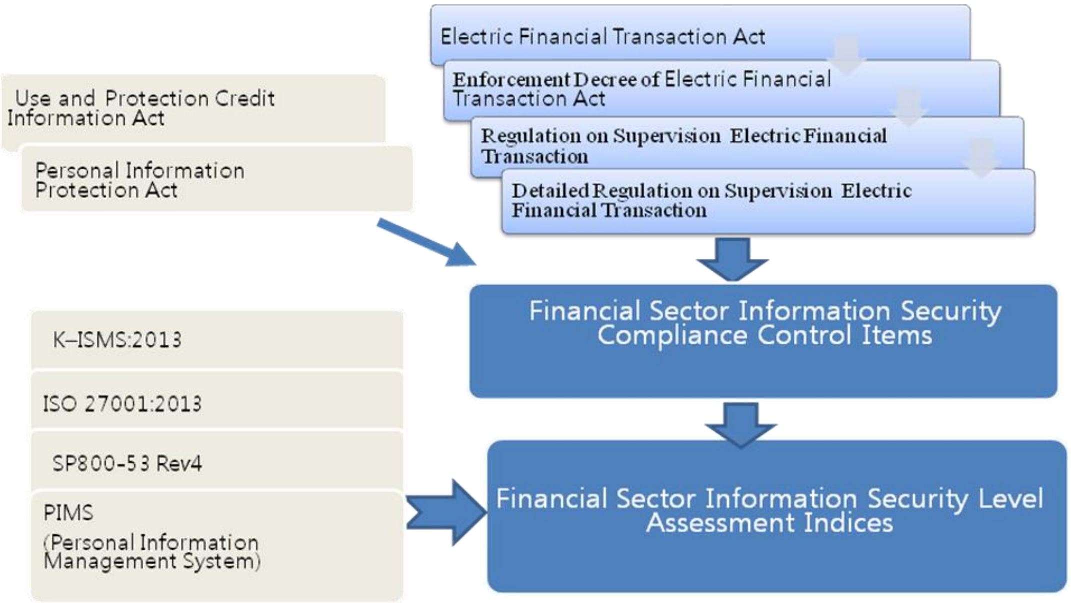
Electric Financial Transaction Act
Enforcement Decree of Electric Financial Transaction Act
Regulation on Supervision Electric Financial Transaction
Detailed Regulation on Supervision Electric Financial Transaction
Use and Protection Credit Information Act
Personal Information Protection Act
Financial Sector Information Security Compliance Control Items
K–ISMS:2013
ISO 27001:2013
SP800-53 Rev4
PIMS
(Personal Information Management System)
Financial Sector Information Security Level Assessment Indices

Figure 1. To Explain the Assessment Indices Establishment Process in Diagrams

2.1. Structure of Financial-sector Information Security Assessment Indices

For the appropriateness and reliability test of the produced assessment indices as well as its evaluation item-specific weighting, we surveyed information security and IT experts in the domestic financial sector. The assessment indices was stratified into 3 tiers by dividing the 14 control domains in reference to SP800-12 – the NIST security handbook applied to US federal governments - into 3 areas [10]. The constructed assessment indices structure is shown in Figure 2. Also to enhance the assessment reliability, AHP (analytic hierarchy process) determining significance based on item-specific comparisons was applied to the top two tiers of control domains and control field to calculate proper weight. The calculated weighted values are factored in the information security maturity level assessment and control item vulnerability level estimation in order to achieve improved assessment reliability.

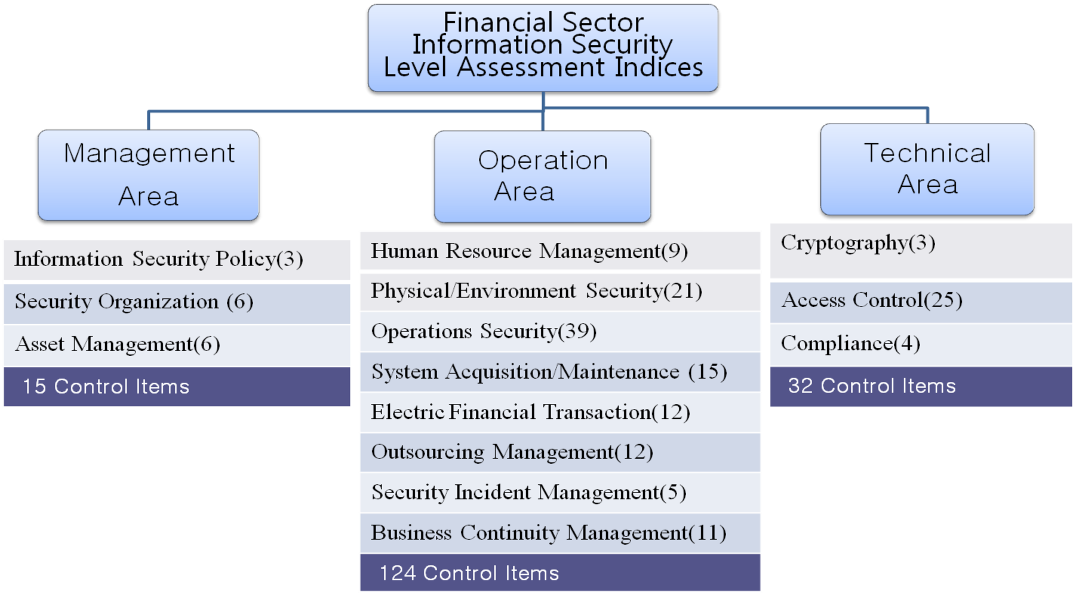
Financial Sector Information Security Level Assessment Indices
Management Area
Operation Area
Technical Area
Information Security Policy(3)
Security Organization (6)
Asset Management(6)
15 Control Items
Human Resource Management(9)
Physical/Environment Security(21)
Operations Security(39)
System Acquisition/Maintenance (15)
Electric Financial Transaction(12)
Outsourcing Management(12)
Security Incident Management(5)
Business Continuity Management(11)
124 Control Items
Cryptography(3)
Access Control(25)
Compliance(4)
32 Control Items

Figure 2. Hierarchical Structure of Assessment Indices

3. Designing of Information Security Maturity Level Assessment and Improvement Anticipation Model

The evaluation of information security maturity levels is to assess the extent of application of information security control items applied to organizations to gauge the organization’s information security status and address and correct the identified vulnerable control items with a view to lowering risk levels to an acceptable level while increasing information security to an upper-tier maturity level [8]. Extant assessment model or studies focused on assessment indices development and organization information security evaluation to diagnose an organization’s maturity level while presenting no measure of improvement through vulnerability amendment. However, the present study establishes financial sector-specific assessment indices and presents double models of an information security maturity level assessment model together with an improvement anticipation model based on addressed vulnerabilities. Figure 3 shows the overview of the suggested model herein.

The information security assessment model adds the control domain-specific weighted values in its individual assessment item values to calculate organizational maturity and according to the produced results, it grants a corresponding phase among the 5 phases of maturity. Following the maturity level assessment, the improvement model sets a targeted maturity level and based on the assessment results, identifies vulnerable control items showing results lower than the targeted level and grants vulnerability level assessment values. It, then adds weights to the vulnerability assessment values to estimate the vulnerability level of corresponding control items. The estimated vulnerability levels, in other words, could function to lower an organization’s maturity level so it could also mean the size of quality improvement when the vulnerability level is upgraded to a targeted level. If this value is added to the already-evaluated information security maturity level, the figure represents an expected information security maturity level when the vulnerability is improved to the target level. By using the suggested model herein, organizations would become able to effectively elevate information security as they could estimate specific improvement effects in advance from the planning stage [15].

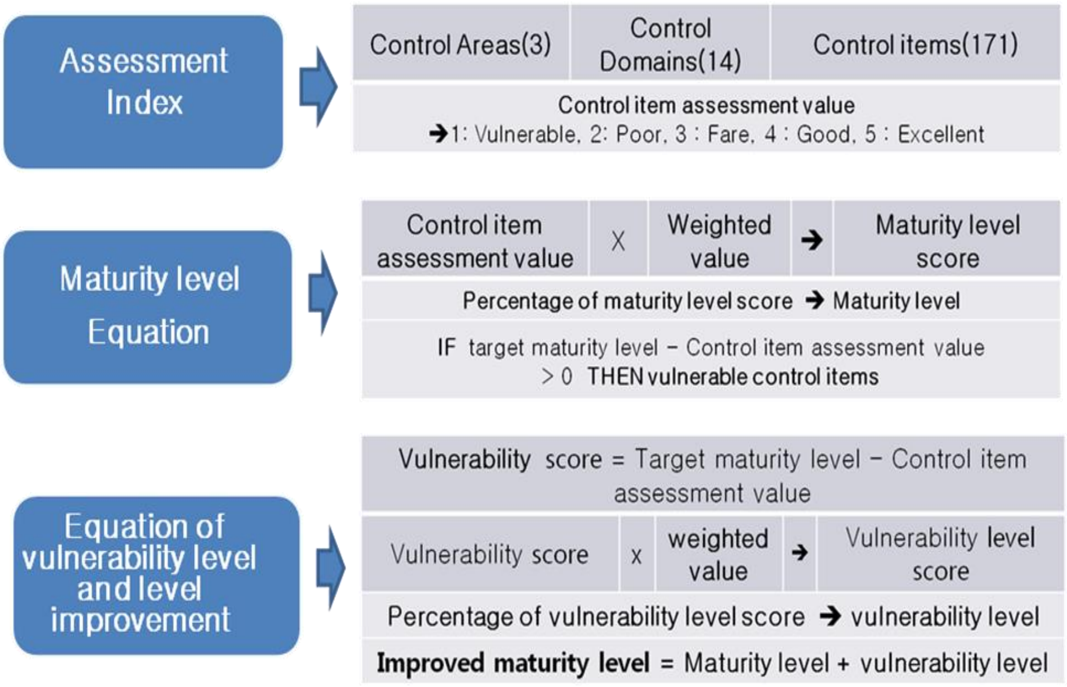
Assessment Index
Control Areas(3)
Control Domains(14)
Control items(171)
Control item assessment value
➔1: Vulnerable, 2: Poor, 3 : Fare, 4 : Good, 5 : Excellent
Maturity level Equation
Control item assessment value
X
Weighted value
➔
Maturity level score
Percentage of maturity level score ➔ Maturity level
IF target maturity level – Control item assessment value > 0 THEN vulnerable control items
Equation of vulnerability level and level improvement
Vulnerability score = Target maturity level – Control item assessment value
Vulnerability score
x
weighted value
➔
Vulnerability level score
Percentage of vulnerability level score ➔ vulnerability level
Improved maturity level = Maturity level + vulnerability level

Figure 3. Overview of Information Security Maturity Level Assessment

3.1. Definition of Maturity Level Phases and Assessment Criteria

SSM-CMM (System Security Engineering-Capability Maturity Model) or ISM3 (Information Security Management Maturity Model) applied as the standard of information security maturity models, base on processes to measure information security maturity levels. And they grants a certain maturity level phase when every condition of process defined for a specific capacity level is met [4, 11, 12]. On the other hand, the Security self-assessment guide for information technology systems(NIST SP800-26(FITSAF) utilizes questionnaires to evaluate the application extant of information security control items applied to federal organizations and aggregates the results to grade an organization's information security level (5-phased maturity level framework) [5, 13]. As the suggested model measures a maturity level based on information security control item assessment just as SP800-26, its 5-phased maturity model was applied to the information security maturity model

The 5 maturity phases and their criteria are defined as follows: The first phase is where only documented policies exist for control items. This is defined to have a 'Vulnerable' information security level. The second phase is where both documented policies and documented procedures exist to be defined as a 'poor' level. And the third phase is where the documented procedures and controls are implemented to be defined as 'fair'. The fourth phase has tested and reviewed procedures and controls to be defined as 'good'. Lastly, the fifth phase has fully integrated procedures and controls to be defined as 'excellent'. Table 1 displays the 5 phases of financial-sector information security maturity model applied in the suggested model herein.

Table 1. 5 Phases of Financial-sector Information Security Maturity

Levels	Level 1	Level 2	Level 3	Level 4	Level 5
Maturity Definition	Documented Policy	Documented Procedures	Implemented Procedures and Controls	Tested and Reviewed Procedures and Controls	Fully Integrated Procedures and Controls
	Vulnerable	Poor	Fare	Good	Excellent
Score Range(%)	Score < 40	40 <= Score < 60	60 <= Score < 80	80 <= Score < 100	Score = 100
Score Calculation Formula		Score / perfect point * 100			

The suggested model's information security level assessment procedure grants points (1~5) to individual assessment items in line with the criteria described in Table 2. Once all of the items are evaluated, the whole assessment points are summed and the percentage of the sum against the total point becomes the maturity level of the corresponding organization.

The existing information security assessment model [14] uses the lowest value of the control item results in a specific control item to represent the corresponding area's maturity level. But this method incurs a problem that even though an organization's general security level is higher thanks to lots of security investment, one single poorly-performed area could determine the whole security situation. To address this problem, this study calculated the sum of the total assessment item points and produced its percentage rate against the total point to determine the overall maturity level. And when the maturity level (expressed in percentage) meets a certain threshold of the upper level, we made the model grant a higher-notch maturity level.

Therefore, the maturity elevation criteria of the suggested model, as described in Table 1, are as follows: if the produced maturity result in percentage (maturity level) is less than 40%, it corresponds to the 1st phase; between 40% and 60%, 2nd phase; between 60% and 80%, 4th phase; between 80% and 100%, 4th phase; and 100%, 5th phase.

Table 2. Control Item-specific Assessment Criteria

5 Point	**1ponit**	**2 point**	**3 point**	**4 point**	**5 point**
Point Definition	Documented Policy	Documented Procedures	Implemented Procedures and Controls	Tested and Reviewed Procedures and Controls	Fully Integrated Procedures and Controls
	Vulnerable	Poor	Fare	Good	Excellent

3.2. Method to Calculate Information Security Maturity Level

The assessment of information security maturity level is conducted by an evaluator following the assessment criteria defined in Table 3.2 regarding the application extant for the 171 assessment items of financial-sector information security level assessment indices. Once the whole items are assessed, the procedures explained below are followed to calculate information security maturity level. Detailed maturity level calculation procedures are as follows:

First, the evaluator independently evaluates in line with assessment criteria by using the application extant for the 171 control items – the lowest phase of financial-sector information security assessment indices system – by relying on interview with relevant officials, documentary investigation, test, *etc.*, The evaluator, then, score the assessment items.

E_{ij}: assessment result of control item j in control domain I

Second, calculate the sum of the control item values in a control domain and factor in the corresponding domain's weighted value to produce its maturity level score (E_i).

Total point of E_{ij}

$$E_i = \sum_{j=1}^{n} E_{ij} \times w_i \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \quad (1)$$

$$TP = \sum_{i=1}^{14} (\sum_{j=1}^{n} \text{perfect score of } E_{ij}) \times w_i$$

$$PE_i = \frac{E_i}{TP} \times 100$$

Converse the control-domain maturity point (E_i) into a percentage Figure against the total point (TP) to produce the maturity level of the corresponding control domain (PE_i). This is expressed in formula 1.

$$TE = \sum_{i=1}^{n} E_i \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \quad (2)$$

$$ML = \frac{TE}{TP} \times 100$$

Third, sum the total point (TE) of the maturity level points in the control domain and converse the number into a percentage figure against the entire control domains (TP) to produce an organizational information security maturity level (ML). This is expressed in formula 2.

3.3. Method for Information Security Improvement Calculation based on Redressed vulnerability

Assessing an organization's information security maturity level is to evaluate the application extant of control items applied to organizations for the purpose of information protection, grasp the general organizational information security level, identify and remedy vulnerabilities and elevate the organization's information security a notch higher [12]. However, extant information security assessment models or studies only perform information security assessment and present its status quo while exposing a serious lack of researches on vulnerability redressing for enhanced information security.

Vulnerabilities are defined as a kind of potential nature of assets exposed to the risk of abuse but sometimes defined as a possibility of failed control against a dangerous attack due to insufficient or lack of information protective measures [6, 9]. In this study, we define vulnerability as the absence or weakness of information security control items. If the result of assessment falls short of an organizational target level, the corresponding control item is viewed as a vulnerable control item. And the difference between the target level and vulnerable control item point is defined as a vulnerability level of the control item.

The higher the vulnerability level, the riskier the corresponding control item is exposed to threat. And it causes the organizational information security maturity level to drop. In this sense, organizations can remove risky factors by identifying and improving the situation with a high vulnerability level and successfully elevate its information security level [6, 7]. This research helps organizations set up effective plans and improve information security by calculating the vulnerability level of control items and providing information on anticipated level upgrade to be completed after specific control item vulnerability is redressed.

First, for calculating the vulnerability level of control items, the assessed organization's maturity level is turned to specific scores (GL) (1st phase: 1 point, 2nd phase: 2 points; 3rd phase: 3 points, 4th phase: 4 points, and 5th phase: 5 points). From *GL*, a control item assessment result (E_{ij}) is subtracted. If the balance is larger than 0, the corresponding control item (that is, targeted maturity level > control item assessment result) is viewed vulnerable. And by adding a weighted value (w_i) of the corresponding control domain to the difference, we can produce the control item's vulnerability level point (VE_{ij}). This is expressed in the formula 3.

$$VE_{ij} = (GL - E_{ij}) \times w_i \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \quad (3)$$

The vulnerability level points calculated by the equation 3-3 are summed according to control domains to calculate control-domain vulnerability level point (VE_i). By adding the control-domain vulnerability level point to the control-domain maturity level point (E_i) calculated in the previous stage, we can produce an estimated maturity level point after vulnerability redress (SVE_i). If converted into a percentage number, this can produce the control-domain estimated maturity level (PVE_i) to determine a maturity level. This is expressed in the formula 4.

$$VE_i = \sum_{j=1}^{n} VE_{ij} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \quad (4)$$

$$SVE_i = E_i + VE_i$$

$$PVE_i = \frac{SVE_i}{TP} \times 100$$

If the estimated maturity level point after vulnerability redress (SVE_i) is added up to the whole control domain, it produces an organizational information security maturity level point expected after vulnerability redress (*TVE*). If this figure is turned in a percentage number, an organizational information security maturity level expected after redressing the whole vulnerable control items (*EML*) is produced and a maturity level is determined. This is expressed in the formula 5.

$$TVE = \sum_{i=1}^{14} SVE_i \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \quad (5)$$

$$EML = \frac{TVE}{TP} \times 100$$

If the suggested model is applied, an assessed organization become able to quantify not only the organizational information security maturity level but also the vulnerability level of control items identified by the information security level assessment, opening up the possibility of anticipating expected information protection upgrade extant when establishing vulnerability-addressing plans. Such an organization could also identify the effects of its vulnerability correction efforts to prioritize their improvement attempts for higher effectiveness in information security upgrade. Control items with a high vulnerability level have a high risk of infringement accidents as well as a considerable incentive to violate applicable regulations on financial-sector electronic finance. In this sense, it is desirable to give a high priority to such items.

4. Effectiveness Verification via Actual Case Application

There has been no comprehensive and systematic information security level assessment model specialized for the South Korean financial sector. Moreover, the sector has no organization to conduct information security level assessment. In this situation, comparing the suggested model herein with other information security assessment model is simply impossible. Thus, we applied the suggested model to a financial institution A in the domestic market to see its operation in an actual environment and test its effectiveness. To ensure the test accuracy and reliability, we gave full explanation to the company on the financial-sector information security assessment indices and its assessment methods. Also since information security assessment requires a considerable level of expertise, we gained cooperation from the company's information security managers and officials so that they performed the assessment themselves.

4.1. A Results of Assessing the Financial Firm's Information Security Maturity Level

The firm A conducted the assessment under the criteria in Table 2 for the entire 171 control items of the financial-sector information security level assessment indices suggested herein. As a result of applying the suggested model, it was found that the firm A's total score of information security maturity was 42.937 and its final information security maturity level converted into a percentage against the total point (59.517) reflecting weighted values was 72.14%. If the produced maturity level (72.14%) is applied to the maturity model of Table 1, the firm A's maturity level falls under the 3rd phase (60% <= maturity level < 80%). The firm A's assessment results are detailed in Table 3.

Looking more closely at the firm A's control-domain maturity levels, we can find that its organization of information security stands at 86.67%, corresponding to the level 4 of 'good' status. On the other hand, its asset management was found to be 50% in its maturity, belonging to the level 2 (60%<=maturity level<80%) to be 'poor'. Of the 12 control domains falling under the level 3 maturity level, the access control (78.40%) and business continuity management (61.82%), in particular, show a large gap though the two are within level 3. In other words, the access control domain is near level 4 to be easily elevated to level 4 with fewer amount of effort (1.6% improvement). On the other hand, business continuity management requires far much effort to improve to the level 4 (18.8% improvement).

Table 3. Results of the Firm A's Information Security Maturity Level Assessment

Control Area	Control Domain	Weight Value	Assessment value	Assessment score	Domain Maturity Level		Maturity Level
Management	Information Security Policy	0.124	10	1.238	66.67	3	71.69
	Information Security Organization	0.122	26	3.168	86.67	4	
	Asset Management	0.070	15	1.046	50.00	2	
operation	Human Resource Management	0.068	28	1.910	62.22	3	70.66
	Physical and Environment Security	0.037	73	2.735	69.52	3	
	c	0.040	47	1.891	62.67	3	
	Operations Security	0.070	146	10.154	74.87	3	
	Electric Financial Transaction	0.118	47	5.560	78.33	3	
	Information Security Incident Management	0.048	38	1.824	63.33	3	
	Outsourcing Management	0.077	18	1.388	72.00	3	

	Business Continuity Management	0.079	34	2.699	61.82	3	
Technical	Cryptography	0.029	10	0.290	66.67	3	77.33
	Access Control	0.088	98	8.656	78.40	3	
	Compliance	0.029	13	0.377	65.00	3	
total		1.000	603	42.937	72.14	3	72.14

The asset management domain in the level 2 is 'poor' lower than the firm A's organizational maturity level (level 3). So the area needs to be considered first in the firm's planning stage. Consequentially, it was found that an organization receiving the assessment can easily identify not only its overall organizational maturity level but also more detailed maturity levels and vulnerability levels to enjoy effective planning for improvement and information security upgrade estimation.

4.2. A Results of Improvement after the Firm's Vulnerability Redress

As the firm A's maturity level assessment indicated level 3, for its phased improvement in this regard, the firm A's target was set as level 4. The firm's target levels and control item assessment points were compared to identify vulnerable control items with points under the target and add weighted values to the difference between the two values to calculate vulnerability level points.

As a result of analyzing vulnerable control items, of the 171 items, 90 were found to have results falling short of the target. The suggested model calculated that the vulnerability level point of the 90 items was 6.28 (out of the total of 59.517). In terms of percentage, this vulnerability level becomes 10.552%. Also, if the firm A's vulnerability level point is added to the maturity level point (42.937), its expected maturity level point after vulnerability redress becomes 82.70% to reach the target (level 4: 80%). Table 4 explains in details the results of improvement after vulnerability redress to be performed in the phase.

Table 4. A Results of Maturity Level Improvement after the Firm A's Vulnerability Redress

Control Area	Control Domain	Assessment Scores	Vulnerab-ility scores	Improved scores	Improved level	Maturity level
Management	Information Security Policy	1.238	0.248	1.485	80.00	83.20
	Information Security Organization	3.168	0.000	3.168	86.67	
	Asset Management	1.046	0.628	1.674	80.00	
operation	Human Resource Management	1.910	0.546	2.456	80.00	82.08
	Physical/Environment Security	2.735	0.450	3.184	80.95	
	System Acquisition/ Development/ Maintenance	1.891	0.523	2.415	80.00	
	Operations Security	10.154	1.252	11.406	84.10	
	Electric Financial Transaction	5.560	0.355	5.915	83.33	
	Information Security Incident	1.824	0.480	2.304	80.00	

	Management					
	Outsourcing Management	1.388	0.154	1.542	80.00	
	Business Continuity Management	2.699	0.794	3.493	80.00	
Technical	Cryptography	0.290	0.058	0.348	80.00	84.04
	Access Control	8.656	0.707	9.362	84.80	
	Compliance	0.377	0.087	0.464	80.00	
	total	42.937	6.280	49.218		82.70

By using the suggested model, we can understand the seriousness of control items by calculating vulnerability level based on the control items identified as vulnerable in the previous assessment stage before conducting actual vulnerability redressing efforts. Also, by checking organizational information security upgrade effect in advance after vulnerability redress, the corresponding organization could effectively set up plans and achieve information security upgrade. Unlike other previous information security assessment studies concentrating on evaluating only information security levels of a certain enterprise and organization, the present study suggests double models of a maturity level assessing model and vulnerability-based improvement estimation model to suggest where to improve along with the status quo in terms of information security.

5. Conclusion

The study reflected in the requirements of the South Korean information security-related laws and regulations for the financial sector and the information security control items of internal/external standard information security management system in order to suggest a comprehensive information security assessment indices and criteria optimized for the financial sector. The suggested model in this research, structured based on this, has a dual system of a information security maturity level assessment model and an upgrade estimation model according to vulnerability redress, maximizing the effects of improvement from information security maturity assessment.

By applying the AHP technique, the weighted value of upper-level (control domain, control field) items of the assessment indices was calculated according to their significance. Then the value was reflected in the production of maturity level and vulnerability level. Moreover, the comprehensively structured assessment indices specialized in the financial sector reflected in the survey of information security and IT experts in the financial sector along with its statistical verification to enhance its appropriateness and reliability. For these reasons, the indices can also be utilized as finance-sector standard information security control items for a financial institution pursuing the introduction of and information security management system in addition for the purpose of assessment indices.

The suggested model quantifies control-item vulnerability levels which have not been dealt with in extant models or researches so that an assessed organization can anticipate the resulting effects of its vulnerability redress before actual task performance. Thus, such an organization considers its own control-item vulnerability levels and vulnerability redressing effect in advance in its improvement planning to effectively achieve mature information security. With the suggested model in place, the financial sector which has performed at a low level for organizational information security maturity assessment due to the lack of comprehensive and well-structured information security assessment model specialized for the financial sector, is now expected to more actively evaluate its information security levels. In this manner, it is hoped that the suggested model will deeply contribute to elevated information security performance of individual organization and the industry as a whole.

Acknowledgement

This paper is a revised and expanded version of a paper entitled Study on Development of Security Level Enhancing Prediction Model through Measuring Maturity level of Information Security and Improving Vulnerability at International Conference on Next Generation Computer and Information Technology 2014(NGCIT 2014), Hochimin, Vietnam, 10.24-26, 2014.

References

[1] "Finance Committee", the Electronic Financial Transactions Act, **(2012)**.
[2] "Korea Internet &Security Agency", guide of information security management system (ISMS) certification system 2013.6.
[3] "ISO, ISO/IEC 27001", Information technology - Security techniques- Information Security Management Systems- Requirement, ISO/IEC, 2013.10.
[4] "ISO, ISO/IEC 21827", Information technology - Security techniques –Systems Security Engineering-Capability Maturity Model (SSE-CMM), 2008.10.
[5] "NIST", Special Publication 800-26 Revision 4, NIST, 2013.4.
[6] K. Kim and G. Nah, "Quantification of information security indices based on vulnerability assessment: Weighted value on information asset act", Journal of Communication Information Security, vol. 10, no. 1, **(2000),** pp. 51-62.
[7] "Korea Internet Security Association", Guide for risk management in information security management system, **(2004)**, pp. 12.
[8] S.-M. Hwang, S.-S. Kim and H.-C. Chae, "Treat Prediction Model for Information Protection Improvement", KIISE Fall Conference, vol. 35, no. 2(B), **(2008)**.
[9] S. Guarro, "Analytical and Decision Models of the Livermore Risk Analysis Methodology (LRAM)", Proceedings of the 1988 Computer Security Risk Management Model Builders Workshop, **(1988),** pp. 49-72.
[10] "NIST, Special Publication 800-12", an Introduction to Computer Security", The NIST Handbook, **(1995),** pp. 10.
[11] V. A. Canal, "Usefulness of an Information Security Management Maturity Model", Information System Control Journal, vol. 2, **(2008).**
[12] "The Open Group", Open Information Standard Management Maturity Model (O-ISM3), **(2011)**.
[13] "NIST", Fderal Information Technology Security Assessment Framework, **(2000)**.
[14] "Korean Internet Security Association", Guidebook on methodology of information security assessment, **(2010).**
[15] Y.-R. Park, Y.-C. Choy and W.-S. Sohn, "Study on Development of Security Level Enhancing Prediction Model through Measuring Maturity Level of Information Security and Improving Vulnerability", Advanced Science and Technology Letters NGCIT, vol. 63, **(2014)**, pp. 240-243.
[16] F. T. B. Muhaya, "Approach for the Development of National Information Security Policy", International Journal of Advanced Science and Technology, vol. 21, **(2010)**.

Authors

Young-Rai Park, he received BS degree from Konkuk University in 1985, MS degree in Graduate school of Engineering, Yonsei University in 1993. Now, he is PhD. Student in Department of Computer Science from Yonsei University.

Yoon-Chul Choy, he received his BS degree from Seoul National University in 1973, and MS and PhD degrees from the University of California, Berkeley in 1976 and 1979 respectively. He worked as a senior researcher at Lockheed and Rockwell International from 1979 to 1982. He has been with the Department of Computer Science at Yonsei University, Seoul, Korea, where he is currently a Professor since 1984. He was the president of Korea Multimedia Society and the director of Software Application Research Institute. He was also a Visiting Professor at the University of Massachusetts and Keio University, Japan. His research interests include computer graphics, user interface (such as sketch-based interface) and mobile multimedia

Won-Sung Sohn, he received the B.S. and M.S. degrees in Department of Computer Engineering from Dongguk University in 1998 and 2000 and the Ph.D degree in Department of Computer Science from Yonsei University in 2004. From 2004 to 2006 he was a postdoctoral associate in the Computational Design Laboratory at Carnegie Mellon University. He is currently a professor at Department of Computer Education, Gyeongin National University of Education. His research interests include educational design research, human-computer interaction and computer education.