Advanced assessment model for improving effectiveness of information security measurement

Junseob Yoon and Kyungho Lee*

Korea University Information Security
Graduate School Risk Management Lab,
Robot Convergence Hall 401,
Anam Campus, Anam-dong 5-ga,
Seongbuk-gu, Seoul, 02841, South Korea
Email: yoon0209@korea.ac.kr
Email: kevinlee@korea.ac.kr
*Corresponding author

Abstract: Information security management system (ISMS) has been used throughout most of the industry. It was made for the purpose of improvement of security and reliability. In addition, ISMS reconsiders awareness of information security in the organisation. A factor of Reliability inhibition in information security is a human error. Human error decreases assessment reliability of checklist-based assessment. This study suggests consistency test used in Minnesota multiphasic personality inventory (MMPI) and newly improved re-survey process. Consistency test detects a false response of respondents. The improved process includes the assessment method to give a penalty to the existing method. Advanced assessment model is applied to a checklist of energy industry to verify the effectiveness. Through the proposed method for human error and to increase the effectiveness of the evaluation.

Keywords: information security management system; ISMS; Minnesota multiphasic personality inventory; MMPI; consistency test; human error detection; risk assessment; security measurement.

Reference to this paper should be made as follows: Yoon, J. and Lee, K. (2016) 'Advanced assessment model for improving effectiveness of information security measurement', *Int. J. Advanced Media and Communication*, Vol. 6, No. 1, pp.4–19.

Biographical notes: Junseob Yoon got his graduation from Chung-Ang University of Seoul, South Korea, in 2014. After graduation, he is studying master course in Korea University. His major is information security. Now, he is working on Researcher belongs to Center for Information Security Technologies. His research area is information security management system, privacy policy, cyber defence, information security education, healthcare security and information system audit.

Kyungho Lee received his PhD degree from Korea University. He is now a Professor in 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).

This paper is a revised and expanded version of a paper entitled ‘Questionnaire assessment methodology for improved reliability of information security measurement’ presented at *2015 International Conference on Platform Technology and Service (PlatCon-15)*, International Convention Center, Jeju, Korea, 26–28 January, 2015.

1 Introduction

The check-list-based information security management system (ISMS) is used in various areas. As cyber attacks increase, the importance of ISMS certification has been increasing. In the case of South Korea in 2013, number of ISMS certification obligation target organisations was only 250. However, it was increased by 50% in 2014 (i.e., 377).

Human error is one of the obstacles that prevent the successful certification of ISMS. Human error in the respondent is a very important factor in ISMS. Since the response to the hundreds of different check items, Respondent could commit human error. Human error caused by misunderstanding or mistake of respondents is able to keep assessment does not reflect the actual compliance status. The checklist consists of a sequence of existing international standards items difficult to solve this problem.

This study introduces a standard checklist and development process for use in existing ISMS. This study applies to the consistency test used in Minnesota multiphasic personality inventory (MMPI), which is one of psychological tests and re-survey process to detect a false answer based on the ISMS survey targeted at energy industry in South Korea and check the concordance of the actual compliance status and surveys and to demonstrate the effectiveness of the study.

2 Previous research

ISMS is a system that has been granted certification by the organisation about the suitability of the system established to protect critical assets, manage and operate from a variety of threats. Organisation that provide financial, educational, medical service could be carried out for. Risk assessment questionnaire consists of ISMS based on the checklist.

In South Korea, K-ISMS is based on the “Promotion of Information and Communications Network utilisation and Information Protection Act”. K-ISMS is composed of 137 items of information protection. Refer to the Information Security Management Evaluation Criteria of NIS (Korean National Intelligence Service) and Major telecommunications infrastructure vulnerability analysis assessment note of MSIP (Korean Ministry of Science, ICT and Future Planning) was creating a checklist questions based on K-ISMS. Domain of NIS is shown in Table 1 and Domain of MSIP is shown in Table 2.

The check list consists of energy industry specific 14 domains and 324 detail items. Each of domains is shown in Table 3.

ISMS certification carried out on the basis of this questionnaire. The following is a flow chart of ISMS certification process. Flow chart of ISMS certification process is shown in Figure 1.

Table 1 Information security management evaluation criteria

Domain	*Evaluation indicator*	*Item No.*
1. Information security policy (20)	1.1 Information security policy and planning	3
	1.2 Information security organisation and staff	5
	1.3 Information security basic activities	6
	1.4 Concern degree of chief officer	3
	1.5 Main telecommunication infrastructure protection	3
2. Information assets security management (23)	2.1 Approval and management of information assets	4
	2.2 Business service management	9
	2.3 National security system	3
	2.4 Protection area management	4
	2.5 Mobile storage media management	3
3. Human security (14)	3.1 Internal personnel security	2
	3.2 External personnel security	5
	3.3 Information security education	7
4. Cyber crisis management (16)	4.1 Cyber crisis management system construction	2
	4.2 Prevention activities	5
	4.3 Cyber crisis response training	5
	4.4 Cyber incident response and recovery	4
5. Electronic information security (26)	5.1 Electronic management of secrets	4
	5.2 Email security	3
	5.3 Web services security	6
	5.4 Electronic information leak prevention	7
	5.5 User authentication	4
	5.6 Cloud computing security	2
6. Information system security (30)	6.1 Information security system	6
	6.2 Wireless LAN security	3
	6.3 Network security	4
	6.4 Information system operation and management	6
	6.5 PC security	7
	6.6 Log and backup	4
Total	*29 indicators*	*129*

The feedback is made in Step 4 (Certification Audit) and Step 5 (Submission of remedied results), human errors also occur. In step of certification audit time, it is necessary measurement methods with cost-effectiveness measure. If the measurement is not accurate, then the organisation receives the certification cannot guarantee the reliability of ISMS and it has to pay fines of 10 million won in 2015.

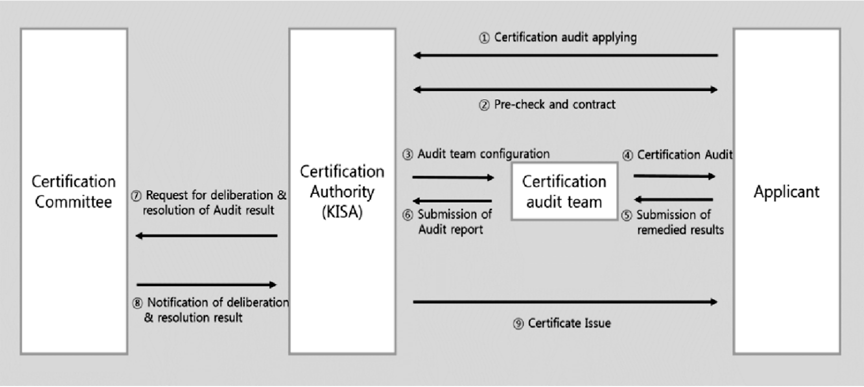
Table 2 Major telecommunications infrastructure vulnerability analysis assessment notice

Domain	*Category*	*Item No.*
Administrative are (A)		114
Physical area (P)		26
Technical area (T)	UNIX (U)	73
	Windows (W)	82
	Security device (S)	26
	Network device (N)	38
	Control system (CS)	22
	PC (PC)	20
	Database (D)	24

Table 3 Domain overview

Domain	*Domain theme*
D.1	Security policy
D.2	Organising information security
D.3	Human resource security
D.4	Information security training
D.5	Asset classification and control
D.6	Physical and environmental security
D.7	Operational security
D.8	Access control
D.9	System development and maintenance
D.10	Password management
D.11	Contingency planning
D.12	Incident response
D.13	Compliance
D.14	External party security

Figure 1 ISMS certification flow chart


Certification Committee
Certification Authority (KISA)
Applicant
① Certification audit applying
② Pre-check and contract
③ Audit team configuration
Certification audit team
④ Certification Audit
⑤ Submission of remedied results
⑥ Submission of Audit report
⑦ Request for deliberation & resolution of Audit result
⑧ Notification of deliberation & resolution result
⑨ Certificate Issue

3 Risk assessment in control-based ISMS

Control-based ISMS use a method of writing by checking whether a control is that each compliance detail items. The response of each item is ‘Yes’, ‘N/A’, ‘No’, ‘Partial’. Assigned score for each response is shown in Table 4.

Table 4 Survey response score

Answer	*Score*	*Description*
Yes	1	Compliance
N/A (not applicable)	–	Can not apply to target organisation
No	0	Non-compliance
Partial	0.5	Incomplete compliance

Assessed risk is reduced if organisation is applying certain security controls to its assets. ISMS target organisation is aware of the organisation’s security vulnerabilities through assessment results and take cost-effective control with appropriate security countermeasures for organisation, or can invest in concentrated critical vulnerabilities. In this study, we adopted a method of classifying rate using classification by business impact (C.B.I.) method for detail items of given checklist.

Each weight of detail is applied considering the related law or the environment of the target organisation. Detail items are classified in accordance with the importance to *M* (Mandatory), *SR* (Strongly Recommended) and *R* (Recommended) grade. ‘Mandatory’ importance is given to the measured items that can be critical risk in legal problem. If Mandatory item that including ‘No’ or ‘Partial’ response exists, then the domain score is zero. ‘Mandatory’ item is given the highest weight of the three importance. ‘Strongly recommended’ item is granted *SR* importance and ‘Recommended’ item is granted *R* importance.

The formula to obtain the domain score with a weighted score as follows:

$$\text{Domain Score} = \frac{w_m \cdot \sum \text{Score of } M \text{ item} + w_{sr} \cdot \sum \text{Score of } SR \text{ item} + w_r \cdot \sum \text{Score of } R \text{ item}}{\text{Perfect score of the domain (All detail checked Yes)}}$$

$$(w_m = \text{weight of madatory}, w_{sr} = \text{weight of strongly recommended}, w_r = \text{weight of recommended})$$

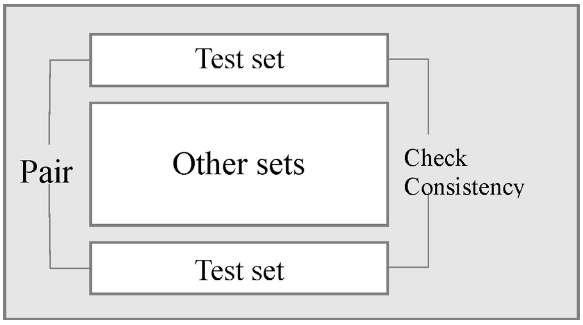
If scores are calculated for all the domains, then total assessment score is transferred to organisation. Accordingly, the decision-makers of the organisation are to take countermeasures to reduce the deduction factor applied to control for the unsatisfactory item. In this case, there is a problem that domain score cannot be calculated accurately due to human error. According to existing process ISMS found to reflect the Human error and fix it to wait until the next ISMS response. How to solve this problem, this study propose a new consistency test using pair set.

4 Methodology

MMPI was designed to examine personality tests used in clinical medicine and mental health. These days, MMPI-2, revision of MMPI, and MMPI-A for youth have been used.

MMPI is used to measure characteristics of a normal character, the emotional level of adaptation, an inner region, such as hearing examination attitudes to quantitatively. In this study, applying some scales used in MMPI to question item configuration is to design the survey. Test–retest (TR) scale and Carelessness (Ca) scale in MMPI is used to make up consistency test. TR scale is the sum of the opposite respondents answered of 16 repeated questions in MMPI. This scale has used to measure the validity of the tests attitude of the patient. TR scale is average 2.29 (standard deviation = 1.58) in case of normal group, average 2.17 (standard deviation = 1.80) in case of anxiety patient's group, average 3.58 (standard deviation = 1.65) in case of psychosis patient's group. Ca scale serves to detect test inability and lack of motivation that is another problem not proven in a consistent response from TR scale. Concept of consistency test is shown in Figure 2.

Figure 2 Concept of consistency test



The scale used directly is TR scale in consistency test. To implement the consistency test, two or three pair set is made for one of the questions in the same domain. Pair set is group of the sentence that asking the same compliance status.

Vocabulary of each sentence is different, but intent is same. When survey details are configured, the numbers of standard aggregates are generated by deriving a common entry. In accordance with the process in reverse order, it can be configured sentence that its vocabularies are different but intent is same. For example, for the sentence: "When cyber incident occurs, do you manage and maintain related documents such as accident investigation details? (including electronic documents)", pair set of sentences such as "Security incidents type, scope and analysis of security incidents are recorded and managed? (including the impact)" can be constructed. Table 5 is an example of existing domain item in the 'incident response'.

By adding pair set to existing checklist items. It can be constitutes the following new domain in Table 6.

The number of items in the 'incident response' domain was increased to 28 items from the existing 21 items due to the addition of six pair set. Table 7 is information of pair set (incident response).

To make up above pair set, K-ISMS (ISO27001:2013 based) checklist of Korea Internet & Security Agency (KISA), Korea National Intelligence Service (NIS) standard, notification of Korea Ministry of Science, ICT and Future Planning (MSIP) are referred. Disassemble the existing entries in each reference, the sentence was re-creation.

Table 5 Domain example (incident response)

Domain		*Detail code*	*Question*	*Importance*
Incident response (21)	1. Process and system (7)	1.1	Incident response procedures have been established? Response procedure include the following: • Definition and scope of the incident (including the significance and type) • Incident declared procedures and method • Emergency contacting system • Incident occurred, recording and reporting procedure • Incident reporting and notification procedures (authority, user, etc.) • Incident report creation • Incident response and recovery procedure • Construction, responsibility and role of incident recovery organisation • Incident recovery equipment and resourcing • Incident response and recovery training, training scenario • Use of external experts and professional organisations • Required for other security incident prevention, and recovery	M
		1.2	Cyber incident response system has been established?	M
		1.3	The incident has been classified according to the type and significance and reporting system is defined in accordance with that classification?	SR
		1.4	Do introduce and conduct information security management systems for distributed denial of service (DDoS) prevention?	SR
		1.5	If you deploy and operate an incident response system via an external control system such as an outside agency, Does the contract reflect the details of the incident response procedures?	SR
		1.6	When cyber crisis alert issued more than 'caution' or cyber incident occurs, are there organisations that can be configured to respond if necessary?	SR

Table 5 Domain example (incident response) (continued)

	Domain	*Detail code*	*Question*	*Importance*
Incident response (21)	1. Process and system (7)	1.7	Related to monitoring, response and handling of incident, the cooperative system with external specialists, specialised agencies and professional organisations is established?	SR
	2. Response and recovery (11)	2.1	Are employees aware of cyber incident response procedures?	SR
		2.2	Are establish a DDoS response system and conducts regular training?	SR
		2.3	What information or information security department staff are aware of the actions in case of incident (including cyber attack)?	M
		2.4	What information or information security department staff are well informed of cyber incident response relevant matters?	M
		2.5	When cyber incident occurs, do you manage and maintain related documents such as accident investigation details?(including electronic documents)	SR
		2.6	If indication of incident or incident occurrence is recognised, does reporting completed quickly in accordance with the defined incident report procedures?	SR
		2.7	Is there incident report contains all the necessary information, such as date of accident, accident details?	SR
		2.8	If the incident can severely impact on the organisation, do staffs reported quickly to top management?	SR
		2.9	When incident occurs, there followed a report and a notification procedures in accordance with the relevant laws and regulations?	M
		2.10	When an employee has received a suspicious or unknown sources external email, viewing does the prohibition?	SR
		2.11	When an employee receives a suspicious or unknown sources have external email, should report to the information security officer?	SR
	3. Follow-up control (3)	3.1	After the incident has been terminated, does analyse the causes of the accident and report the results?	SR
		3.2	After cyber incident occurred, did check for accidents that occurred recent one year and establish measures accordingly?	SR
		3.3	Does the incident information and discovered vulnerabilities associated organisations (National Cyber Security Center, etc.) and shared with staff?	SR

Table 6 Modified domain (incident response)

Domain		*Detail code*	*Question*	*Pair set #*	*Importance*
Incident response (21->28)	1. Process and system (7->10)	1.1	Incident response procedures have been established? Response procedure include the following: • Definition and scope of the incident (including the significance and type) • Incident declared procedures and method • Emergency contacting system • Incident occurred, recording and reporting procedure • Incident reporting and notification procedures (authority, user, etc.) • Incident report creation • Incident response and recovery procedure • Construction, responsibility and role of incident recovery organisation • Incident recovery equipment and resourcing • Incident response and recovery training, training scenario • Use of external experts and professional organisations • Required for other security incident prevention, and recovery		M
		1.2	Cyber incident Response System has been established?	*#1*	M
		1.3	The incident has been classified according to the type and significance and reporting system is defined in accordance with that classification?		SR
		1.4	Do introduce and conduct information security management systems for DDoS(Distributed Denial of Service) prevention?	*#2*	SR
		1.5	If you deploy and operate an incident response system via an external control system such as an outside agency, Does the contract reflect the details of the incident response procedures?		SR
		1.6	When cyber crisis alert issued more than ‘Caution’ or cyber incident occurs, are there organisations that can be configured to respond if necessary?	*#3*	SR
		1.7	Related to monitoring, response and handling of incident, the cooperative system with external specialists, specialised agencies and professional organisations is established?		SR

Table 6 Modified domain (incident response) (continued)

Domain		*Detail code*	*Question*	*Pair set #*	*Importance*
Incident response (21->28)	1. Process and system (7->10)	1.8	When incident occurs, is procedure for quick reporting security incidents documented and reporting in accordance with the procedure?	*#1*	M
		1.9	Emergency response team that can respond cyber warning or cyber damage is organised?	*#3*	SR
		1.10	Is the defence set in a DDoS attack?	*#2*	SR
	2. Response and recovery (11->14)	2.1	Are employees aware of cyber incident response procedures?		SR
		2.2	Are establish a DDoS response system and conducts regular training?	*#4*	SR
		2.3	What information or information security department staff are aware of the actions in case of incident (including cyber attack)?		M
		2.4	What information or information security department staff are well informed of cyber incident response relevant matters?		M
		2.5	Does the self cyber incident response training?	*#4*	SR
		2.6	When cyber incident occurs, do you manage and maintain related documents such as accident investigation details?(including electronic documents)	*#5*	SR
		2.7	Business continuity management through simulation training and constantly reviewed and there if there is a change in the organisation's details on this being reflected?	*#4*	SR
		2.8	If indication of incident or incident occurrence is recognised, does reporting completed quickly in accordance with the defined incident report procedures?		SR
		2.9	Is there incident report contains all the necessary information, such as date of accident, accident details?		SR
		2.10	If the incident can severely impact on the organisation, do staffs reported quickly to top management?		SR
		2.11	When incident occurs, there followed a report and a notification procedures in accordance with the relevant laws and regulations?		M
		2.12	What types of security incidents, scope, and impact analysis is to be recorded and managed?	*#5*	SR
		2.13	When an employee has received a suspicious or unknown sources external email, viewing does the prohibition?		SR
		2.14	When an employee receives a suspicious or unknown sources have external email, should report to the information security officer?		SR

Table 6 Modified domain (incident response) (continued)

Domain		*Detail code*	*Question*	*Pair set #*	*Importance*
Incident response (21->28)	3. Follow-up control (3->4)	3.1	After the incident has been terminated, does analyse the causes of the accident and report the results?		SR
		3.2	After cyber incident occurred, did check for accidents that occurred recent one year and establish measures accordingly?	#6	SR
		3.3	Does the incident information and discovered vulnerabilities associated organisations (National Cyber Security Center, etc.) and shared with staff?		SR
		3.4	After a cyber incident did implement recurrence prevention measures?	#6	SR

Table 7 Pair set information (incident response)

Pair set No.	*Verification compliance*
1	The establishment of incident response system (documentation, reporting system)
2	Action to prevent a DDoS
3	Emergency response team configuration (cyber crisis alert more than 'caution')
4	incident response training execution
5	Cyber incident occurs, the relevant document records management
6	Establishing and implementing recurrence prevention measure

5 Proposed process

With the configuration of the domain consistency test is completed and inspected. In the existing risk assessment, there was no way that can be fed back soon for the human error of respondents. Even if the evaluator find a pattern or sign of mistake, modification about error has a structure made in the next survey. Therefore, in the assessment a reduction of accuracy and efficiency occurs. In case of proposed process occurred 'inconsistency' in the consistency test, the domain that contains the item is marked 'suspended' and the part point to pair set is scored zero. The result of domain output score is transmitted to respondent. With lower domain score, respondent shall be re-surveyed. The evaluator should note only fact that respondent have to do re-survey and not notify which part contains 'inconsistency' in consistency test to respondent. For 'coincidence' in consistency test, re-survey is continuing until third re-survey. If the domain of 'inconsistency' after the third re-survey exists, conduct new survey for the entire domain. Flow diagram of re-survey procedure is shown in Figure 3.

Since the survey targeted specialist group, re-survey time was determined by three with reference to the relevant papers. When using the proposed procedure, although was not concrete redlines between evaluators and respondents, may have been a tacit communication that the answer was wrong. In this way, at the level of the independent evaluator is not compromised is one way to improve the efficiency of the assessment. Domain has a low score can be a way to improve the response attitude of the respondents.

Thus, respondents may be more focused on tests to accurately reflect the actual compliance status. Consistency test can prevent the response to disguise the actual compliance because it can detect the examination attitude that 'trying to look good'. Comparison between existing process and proposed process is shown in Table 8.

Figure 3 Re-survey procedure after consistency test

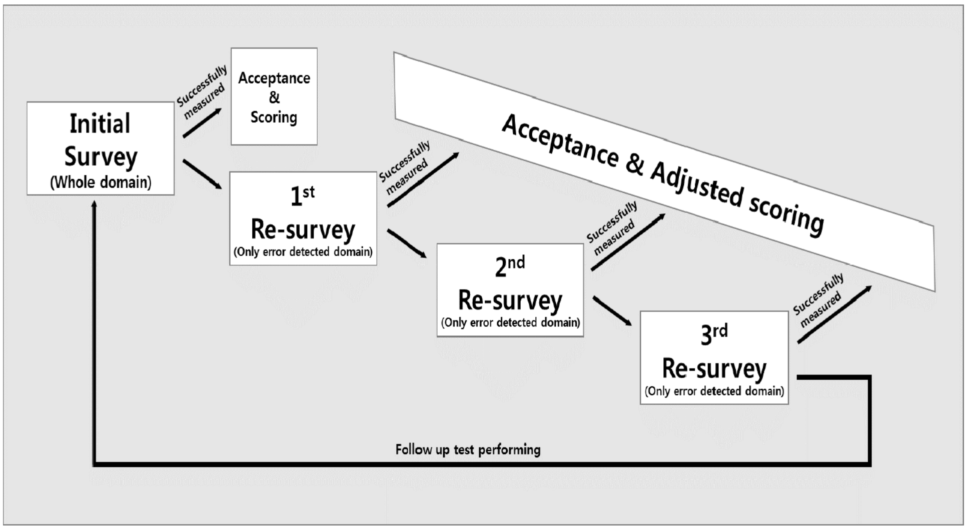


Table 8 Comparison with existing process

	Existing process	*Proposed process*
Survey approach	All at once	Divided into several times (maximum three times)
Human error detection time	After first risk assessment ~ Before next assessment	After each re-survey time
Assessment cost-effectiveness	Low	High (feed effect)

Assessment cost allocable to each time is higher than existing assessment method. That is disadvantage of the proposed process. However, when considering the time and human resources required for the risk assessment, the proposed process can have a high performance in terms of effectiveness.

In addition, by changing the questionnaire to increase the effectiveness of measurement of re-survey steps, it is possible to avoid the duplicate question appeared.

Example of questionnaire is shown in Table 9.

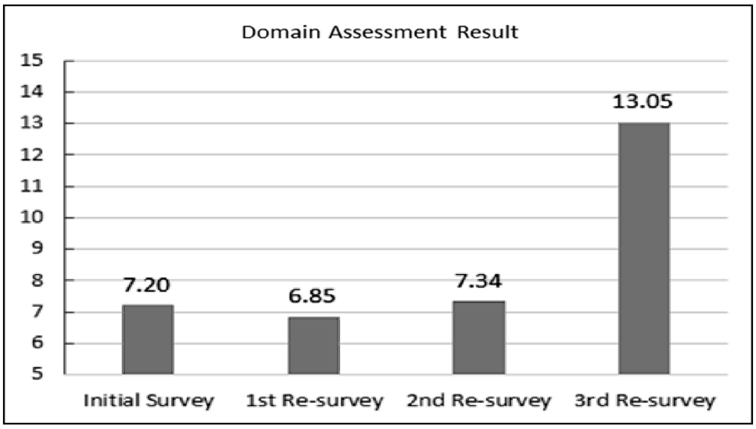
6 Simulation

With the 'Incident Response' domain that contains pair set created in the Methodology section above, this study is carried out in a simulation of a particular virtual energy industry in South Korea. If all of the detail questions that compliance 'No' response, scored ‘0’. And if all of the detail questions that compliance ‘Yes’ response, scored ‘1’. Describe a specific compliance status for focus group. Each question is given weighted values according to their importance, i.e., Mandatory: 1, Strongly Recommended: 0.7, Recommended: 0.5. From three times of re-survey attempts, the average results could be derived. The result is shown in Figure 4.

Table 9 Example of questionnaire changes

	Initial survey		*1st re-survey*		*2nd re-survey*		*3rd re-survey*
Question (follow-up control)	After cyber incident occurred, did check for accidents that occurred recent one year and establish measures accordingly?	⇒	Do utilise incidents of past 1 year to prevention of recurrence?	⇒	Are previous incidents reflect incident response?	⇒	Does staff have check incidents of the past event of an accident?
	After a cyber incident did implement recurrence prevention measures?		Investigate the recent cases after the accident?		Were preventive measures are established based on past practices?		Are refer to past incidents of possible control measures are established?

Figure 4 Trend of domain score (incident response)



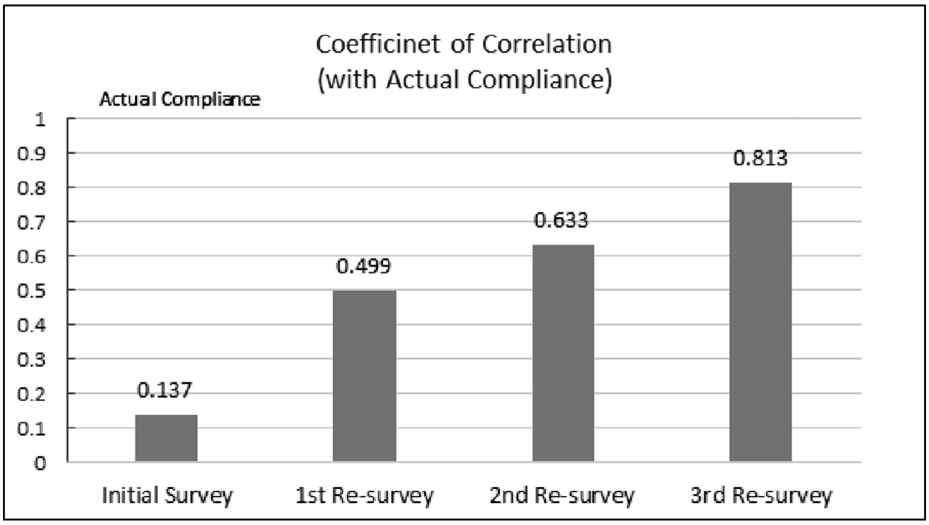
In fact, in compliance with the state of the environment was equivalent to 0.806. Simulation results show while the respondents are relatively low scores on the initial and the first re-survey. However, after the second and third re-survey, results show that getting closer to the actual compliance score. Owing to the ‘suspended’ penalty, there is not seen a significant improvement on first and second re-survey. After third re-survey, result shows a dramatically improvement. To ensure the matching of construction of responses, other than score, initial survey, first re-survey, second re-survey and third re-survey detailed answer was performed bivariate correlation with the actual compliance status. The Pearson correlation coefficient is high, the two surveys are linearly proportional relationship. When the Pearson correlation coefficient is >0.7, generally ‘There is a significant correlation’ is called. Details of correlation trend are shown in Table 10 and trend of correlation coefficient is shown in Figure 5.

Table 10 Correlation trend (incident response)

		Actual compliance	*Initial survey*
Actual compliance	Pearson correlation	1	0.137
	Sig. (2-tailed)		0.488
	N	28	28
Initial survey	Pearson correlation	0.137	1
	Sig. (2-tailed)	0.488	
	N	28	28
		Actual compliance	*First resurvey*
Actual compliance	Pearson correlation	1	0.499**
	Sig. (2-tailed)		0.007
	N	28	28
First resurvey	Pearson correlation	0.499**	1
	Sig. (2-tailed)	0.007	
	N	28	28
		Actual compliance	*Second resurvey*
Actual compliance	Pearson correlation	1	0.633**
	Sig. (2-tailed)		0.000
	N	28	28
Second resurvey	Pearson correlation	0.633**	1
	Sig. (2-tailed)	0.000	
	N	28	28
		Actual compliance	*Third resurvey*
Actual compliance	Pearson Correlation	1	0.813**
	Sig. (2-tailed)		0.000
	N	28	28
Third resurvey	Pearson Correlation	0.813**	1
	Sig. (2-tailed)	0.000	
	N	28	28

This study introduced the questionnaire assessment method applied to consistency test and re-survey process. Proposed process performs consistency test containing a pair set for detecting inconsistency and carelessness and include re-survey up to three times. The proposed process has two purposes. First purpose is giving a penalty to using communication between evaluator and respondents with ‘suspended’ marking. Second purpose achieved through a quick scan attitude correction over the re-survey. In the simulation, the effectiveness of the method was verified by using specific domain. For the application of the consistency test and re-survey process, future researches are needed in various areas not only energy industry but also education, healthcare and defence industry. In addition, it is necessary to design how the re-survey done much in terms of cost-effectiveness and verified.

Figure 5 Correlation coefficient of survey (between actual compliance)



Pearson correlation coefficients from the simulation results of the initial survey are relatively low as 0.137. Through first, second, third re-survey, Pearson correlation coefficients show a continued upward trend. Third re-survey has a significant correlation coefficient of 0.813 was obtained. Through the score and the Pearson correlation analysis of simulation, risk assessment measurement using consistency test with the proposed process is verified in terms of effectiveness and reliability.

7 Conclusion

This study introduced the questionnaire assessment method applied to consistency test and re-survey process. Proposed process performs consistency test containing a pair set for detecting inconsistency and carelessness and include re-survey up to three times. The proposed process has two purposes. First purpose is giving a penalty to using communication between evaluator and respondents with ‘suspended’ marking. Second purpose achieved through a quick scan attitude correction over the re-survey. In the simulation, the effectiveness of the method was verified by using specific domain. When estimating relative to 2014, the economic benefits per a certification are 220 million won. If the re-surveys and simulations performed up to three times as shall be added the cost of ~500 million. The results show that the improvement in the proposed process by 27%. In addition, it can be seen that the benefits of this investment 12 times. For the application of the consistency test and re-survey process, future researches are needed in various areas not only energy industry but also education, healthcare and defence industry. There is also a continued need to research about the effectiveness of the process of the present research in the post-mortem after the certification step.

Bibliography

Greene, R.L. (2009) *The MMPI-2: An Interpretive Manual*, 3rd ed., Allyn & Bacon, USA.

International Organization for Standardization (2013) *ISO 27001:2013: Information Technology – Security Techniques – Information Security Management Systems – Requirements*, ISO, Geneva.

Kang, H.S. (2014) 'An analysis of information security management system and certification standard for information security', *Journal of Security Engineering*, Vol. 11, No. 6, pp.455–468.

Kankanhalli, A., Teo, H.H., Tan, B.C.Y. and Wei, K.K. (2003) 'An integrative study of information systems security effectiveness', *Int. J. Inf. Manage*., Vol. 23, No. 2, pp.139–154.

Kim, J.D. and Park, J.E. (2003) 'A study on TCO-based returend on security investment (ROSI)', *The Korea Society of Digital Policy and Management*, No. 1, pp.251–261.

Ma, W.M. (2010) 'Study on architecture-oriented information security risk assessment model', *Computational Collective Intelligence. Technologies and Applications*, Springer Berlin Heidelberg, pp.218–226.

Nam, S.H. (2006) *An Empirical Study on the Impact of Security Events to the Stock Price in the Analysis Method of Enterprise Security Investment Effect*, Korea University.

Neubauer, T., Ekelhart, A. and Fenz, S. (2008) 'Interactive selection of ISO 27001 controls under multiple objectives', *Proceedings of the Ifip Tc 11 23rd International Information Security Conference*, Milano., Italy, pp.477–492.

Noh, Y.H. (2011) 'A study on measuring the change of the response results in Likert 5-point scale measurement', *Journal of the Korean Society for Information Management*, Vol. 28, No. 3, pp.335–353.

Park, K.T. and Kim, S. (2014b) 'An empirical study on the obstacle factors of ISMS certification using exploratory factor analysis', *Journal of the Korean Institute of Information Security & Cryptology*, Vol. 24, No. 10, pp.951–959.

Park, S. W. and Lee, H.W. (2004b) 'The study on economic aspects of information security industry', *European Applied Business Research Conference*, Article #335.

Park, S.H. and Lee, K.H. (2014a) 'Advanced approach to information security management system model for industrial control system', *The Scientific World Journal*, Vol. 2014, Article ID 348305 [Online], http://dx.doi.org/10.1155/2014/348305 (Accessed 29 December, 2014).

Park, S.W. and Lee, H.W. (2003) 'Korean information security market forecast and analysis', *European Applied Business Research Conference*, Article #449.

Park, S.W. and Lee, H.W. (2004a) 'The study of Korean information security applied market', *The 6th International Conference on Advanced Communication Technology*, pp.512–514.

Park, S.W. and Lee, H.W. (2004c) 'Introduction to information security policy in Korea', *International Business and Economics Research Conference*, Article #297.

Park, S.W., Ko, S.H., Lee, H.W. and Kim, H.J. (2002) 'Development strategy of Korean information security market', *International Business and Economics Research Conference*, Article #275.

Ryu, S.H., Jeong, D.R. and Jung, H.K. (2013) 'Ways to establish public authorities information security governance utilizing E-government information security management system (G-ISMS)', *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 17, No. 4, pp.769–774.

Seo, J.S., Song, M.S. and Lee, K.H. (2014) 'A study on efficiency of ISMS for ICS with compliance', *International Journal of Multimedia and Ubiquitous Engineering*, Vol. 9, No. 5, pp.301–306.

Sun, H.K. (2004) *Impacts of Information Security Policies and Organizations on the Information Security Performance in Korean Enterprises*, Kookmin University.

You, Y.I., Oh, S.K. and Lee, K.H. (2014) 'Advanced security assessment for control effectiveness', *Information Security Applications*, Springer International Publishing, pp.383–393.