J. Inf. Technol. Appl. Manag. 23(3): 61~69, September 2016
http://dx.doi.org/10.21219/jitam.2016.23.3.061

ISSN 1598-6284 (Print)
ISSN 2508-1209 (Online)

A Continuous Evaluation Processes for Information Security Management

Myeonggil Choi*

Abstract

Growing information threats have threatened organization to lose information security controls in these days. Many organizations have accepted the various information security management systems does mention necessity of a continuous evaluation process for the executions of information security management in a theoretical aspect. This study suggests a continuous evaluation process for information security management reflecting the real execution of managers and employees in organizations.

Keywords : Continuous Monitoring Processes, Information Security Management System, Monitoring Tool, Information Security Evaluation

Received : 2016. 06. 22.　　Final Acceptance : 2016. 07. 22.

* School of Business, Chung-Ang University, 84 Heuksuk-Ro, Dongjak-Gu, Seoul, 06974 South Korea, e-mail : mgchoi@cau.ac.kr

1. Introduction

Increasing information threats from external and internal organizations have jeopardized organization into loss of information controls in these days. To protect organization from these threats, many organizations have accepted the various information security management systems such as ISO27000, IT Baseline, and FISMA [Gilbert and Gips, 2000; Choi, 2016]. These management approaches provide a theoretical ground for information security management, but does mention necessity of a continuous evaluation process for the executions of information security management in a theoretical aspect [Jo et al., 2016]. The absence of a continuous evaluation process results in separation of security management from the practices in information security. To overcome the shortcomings, this study suggests a continuous evaluation process for information security management reflecting the real execution of managers and employees in organizations. The proposed processes consist of architecture, contents and criteria for the continuous management systems. The suggested processes provide a real-time monitoring to the external threats such as the suspicious activities of external sources and the internal threats including behaviors of information security managers and employees, thus protecting the assets of information systems securely.

2. The Analysis of Information Security Evaluation System

Information security managements have been suggested and implemented in practice fields. Most of them are used in the private sectors but are focused in the government agency or institutes. The representative systems for information security systems are explained below;

2.1 CyberScope

The federal government of U.S. provides Cyberscope, an automated support systems tool support for FISMA. Cyberscope automatically collects the status information of security and simplifies the evaluation processes. The CyberScope reporting FISMA have been distributed to government institutions by OMB (Office of Management and Budget) in 2009. The system establishes two-factor certification for efficiently collecting data and reports the results of the status of information security by on-line access. The language of Cyberscope is XML like that of SCAP (Security Content Automation Protocol).

The CyberScope automatically collects compliance data FISMA. CyberScope can automatically change business data to meta data such as CVE (Common Vulnerabilities and Exposures), CCE (Common Configuration Enumeration), CPE (Common Platform Enumeration) based on SCAP. It can generates a report which can be used to assess information security evaluation [NIST SP 800-64, 2008].

FISMA adopts three-tiered approach. for reporting information security of institutions. First, it provides data directly from security management tools. Second, it provides benchmarking of information security with governments each level of securities. Third, it surveys the institution-specific conditions.

2.2 CAESARS (Continuous Asset Evaluation, Situational Awareness, and Risk Scoring)

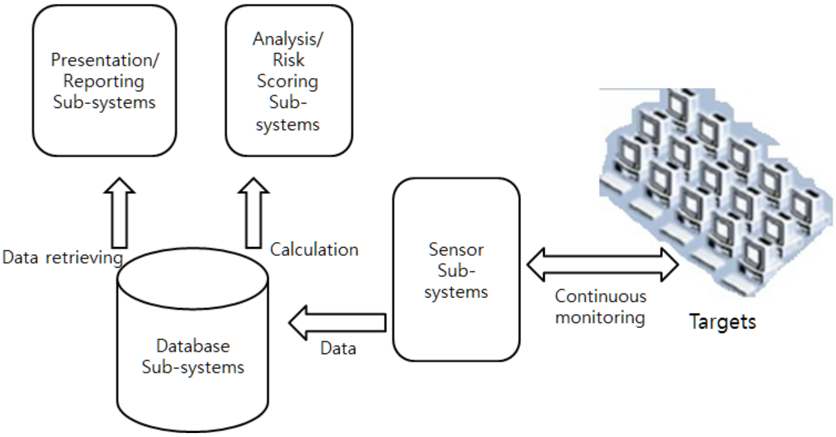
The architecture of CAESARS can be also utilized in continuous monitoring information security. DHS (Department of Homeland Security) provides a kind of self-assessment, CAESARS (Continuous Asset Evaluation, Situational Awareness and Risk Scoring) [Department of Homeland Security, 2010]. CAESARS has been developed to provide an integrated framework of information security risk assessment for Department of State, DoT (Department of Treasury), DoJ (Department of Justice). CAESARS ties systems, which evaluate the risk as score systems, into a single architecture. For providing the information of the current security status and helping users in decision making, CAESARS provides information of security based on the score of the risk assessment.

We review the operational concept of reference architecture of CAESARS. CAESARS provides the continuous monitoring through combination of system development life cycle and RMF (Risk Management Framework). NIST SP 800-64 Rev.2 suggests system development life cycle as initiation, development/acquisition, implementation/evaluation, operation and maintenance [NIST SP 800-64, 2008]. RMF presented in NIST SP 800-37 presented risk management life cycle as classification of information, selection of information controls, implementation of security controls, and evaluation of security controls [NIST SP 800-37, 2010].

CAESASRS conceptually consists of four subsystems, which are sensor subsystems, database/repository subsystems, analysis/risk scoring subsystems, and presentation and reporting subsystems in <Figure 1>.

We can extract the concept of continuous security monitoring from the architecture of CAESARS. We can provide the status of information security in organization through threat information, effective security controls based on the automated data collection tools, and prioritize the information security risk.

The relationship between Cyberscope and CAESARS is as followings; First, OMB demands



<Figure 1> The Conceptual Architecture of CAESARS

the specific information which are broader than that CAESARS can collect. Second, CAESARS can achieve the goals of OMB through directly checking the vulnerabilities of the systems, services, hardware, softwares. Third, CAESAERS and Cyberscope can support the goals of OMB through surveying all of information assets in the institutions.

3. A Proposed Continuous Evaluation Processes for Information Security Management

The current evaluation of information security management establishes procedures to evaluate evaluating items and assess overall information status of an organization by evaluation team in Korea government [Choi, 2016; Shaw and Harrald, 2004]. The current assessment, therefore, demand considerable time and human resources for pre-preparation procedures for evaluating items. To improve the status of current information security evaluation, the continuous information security evaluation processes should be strengthened.

US DHS (Department of Homeland Security)'s CAESARS FE (Framework Extension) may be helpful to construct a framework for continuous monitoring evaluation of governmental institutions. CAESARS may be a framework to analyze the risk assessment score commonly, CAESARS FE implies the details performing CAESARS for organizations substantially.

We suggest continuous evaluation process for informations security management. The process framework is composed of four phases based on CAESARS and CAESARS FE. The proposed process has the following advantages. First, it can be substantially performed for self-evaluation by the evaluated organization. Second, it can configure the 4 steps of the process. The suggested continuous evaluation process is shown in <Table 1>.

<Table 1> The proposed continuous evaluation process

Phases	Required performing tasks	Subject	Required output
Development of continuous self-evaluation process	• Construction of the evaluation process for institutional self-evaluation • Construction of the overview of the process, objectives, procedures, definitions, modeling, work flow	Assessor (assessment body, institution)	Institutional self-evaluation process
Designing continuous self-evaluation process	• Designing and appling the continuous evaluation process to organization • Assigning the department/staff to take charge of continuous self-evaluation • Top security administrator performs management tasks	Appraisee (Subjects (institution) of evaluation)	Institutional specific self-evaluation framework
Design and establishment of continuous evaluation technical architecture	• Construct the data collection strategy for self-evaluation • Construct the item of continuous self-evaluation and strategy • Construct the system of self-evaluation	Assessor (assessment body, institution)	Classification criteria of institutional self-evaluation target item
		Appraisee (Subjects (institution) of evaluation)	Institutional self-evaluation's execution result
Presentation and reporting of self-evaluation architecture's detailed report	• Submit the report of self-evaluation results	Appraisee (Subjects (institution) of evaluation)	Institutional self-evaluation's result report

3.1 Step 1 : Development Phase of Continuous Self-Evaluation Process

Organizations can establish continuous self-evaluation process. The process consists the overview of the framework, objectives, procedures, definitions, modeling, and business work flow at the development phase. The overall design level of the process and the resources required for each of the design level are shown in <Table 2>.

<Table 2> Design of Institutional Self-Evaluation Reinforcement Framework

The overall design level	Reference resources for design
Definition of framework properties	NIST SP 800-37
EA	NSA architecture model
Subsystem modeling	DHS CAESARS
Technical modeling	CAESARS FE research
Composition of work flow	CAESARS FE research

3.2 Step 2 : Designing Continuous Self-Evaluation Process

Organizations design and establish continuous self-evaluation process considering the features of institutions based on the developed continuous self-evaluation process. Continuous self-evaluation process should include continuous monitoring to warn dangerous situation. The continuous self-evaluation process should be designed to contain the continuous monitoring and analysis for situational awareness and decision-making [Shaw and Harrald, 2004].

Management should consider the following features in designing the process step.

- Vulnerability management
- Patch management
- Event management
- Incident management
- Malware detection
- Asset management
- Configuration management
- Network management
- License Management
- Information management
- Software assurance
- Digital policy management
- Advanced persistent threat

Organizations should consider the following factors in order to establish the continuous self-evaluation process. First, organizations should place the expertises or specialized departments for the self-evaluation. Second, the organizations perform the continuous self-evaluation at strategic level of the institution's information security. Third, the organizations refer to use use the security standards such as ISO27000 etc al.

3.3 Step 3 : Design and Establishment of Continuous Self-Evaluation Technical Architecture

The continuous self-evaluation process can not replace or change the existing evaluation system, but establish the architecture to process data collected by continuous monitoring at all times.

The construction of data collection system is needed for the continuous self-evaluation process. The specific evaluation body is not assumed for data collection system for the automated evaluation data.

The continuous self-evaluation data collection system, which is the alternative method to replace the CAESARS sensor subsystem, collects evidential data submitted the existing evaluation.

The self-evaluation item classification system is constructed. Each detailed evaluation scores can be divided into 3 levels as following-High, Moderate, Low from the perspective of confidentiality, integrity and availability. or other classification methods. The more important information/information system institutions have, the more 'high' weighed values they get. Therefore, it can be recognized that the size of organization is greater. The continuous self-evaluation system collects data classified by the following features in <Table 3>.

〈Table 3〉 Collected Technical Security Functions

Technical security functions	
Compliance	Test for IT planning and execution, Training program
Identification of system risk	Prevention of malicious program accident
Operation of security policy	Development of security DNS
Identification of security control	Encryption algorithm for personal identification assurance
Network security system	Biometric data for personal identification assurance
Detailed system configuration	PDA forensic
User data security policy	IT products guideline for check-list users and developers
Application of system development life cycle's security policy	Security configuration check-list for IT products
Portable communication equipment security	Budget appropriation and control process for IT security
Central server security	Security considerations in system development life cycles
Personal information security (Privacy)	Electronic authentication guideline
Wireless communication security	Computer security accident management
Physical access control system security	Security categorization for information and information system
Information security testing · assurance	Security considerations for IP system purchase
External device security for remote access	Key management
VPN security	Performance measuring guide for information security
Storage device of cryptography technology for end-user	Gateway protocol security
Key encryption function	TLS selection and use
Use of Hash algorithm	CVE scheme use
Random hash for digital signature	Awareness of Information technology security and composition of training program
Image encryption	IEEE 802.11 wireless network security guideline
Mobile forensic	security for Internal information system connection
RFID system security	Broadband communication security
IEEE 802.11i wireless security network	Electronic mail security guideline
Security web service	Public web server security
intrusion detection and protection system	Firewall policy
Computer security log management	Patch, vulnerability management program
Random bit generator	Risk management of information system
Assurance of digital signature application	PBX vulnerability analysis
Media permanent deletion	Development of information security training requirement
Incident response by forensic technology	Communication network security guideline

3.4 Step 4 : Presentation and Report of the Continuous Self-Evaluation Process Report

The subjects of evaluation should make a report of self-evaluation results and submit to the assessor (assessment body, rating agency). The report should include component list of self-evaluation process, self-evaluation team and member, evaluation item performed self-evaluation, evaluation result. Assessor (assessment body) should determine the size of assessment through a submitted self-evaluation report. The evaluation of the reports are known by exiting evaluations, FISMA, ISO, and related instances. Information security management assessment can be divided into 4 levels-excellent, good, average (normal), insufficiency (poor)- on an absolute grading scale. The insufficiency rating organizations must be submitted for the future plans.

FISMA divide into 3 levels -green, yellow, red-by standard of information security score C, I, A. Organizations must meet the minimum requirements to get the green level that is the highest level. The green level is the case that successfully meet all of the criteria, the yellow level is achieved when the intermediate level or above on all criteria, and the red level is the case that have even just one serious flaw. ISO27000 is not indicated rating, but pass-through authentication, maintenance of authentication, and so on.

4. Conclusion

The proposed continuous evaluation can remedy the shortcomings of the various processes of information security management. Most of the information security systems focus on the activity of information security. They just consider the activities of information security as broken workflows. The suggested process assumes that each activity of information security closely connected and influence each another. The suggested process continuously monitors the status of information and reports the status information automatically. The suggested processes can improve the information security process turning into continuos activities.

References

[1] Choi, M. and Park, E., “The Influences of Enterprise Management Strategy on Information Security Effectiveness”, *International Journal of Applied Engineering Research*, Vol. 11, No. 15, 2016, pp. 8686-8694.

[2] Choi, M., “An Evaluation Methodology of Information Systems in Business Contingency Planning”, *Journal of Information Technology Application and Management*, Vol. 23, No. 1, 2016, pp. 119-128.

[3] Choi, M., “Leadership of Information Security Manager on the Effectiveness of Information Systems Security for Secure Sustainable Computing”, *Substantiality*, Vol. 8, No. 7, 2016, pp. 1-21.

[4] Department of Homeland Security, Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS), 2010.

[5] Gilbert, G. A. and Gips, M. A., “SUPPLY-SIDE CONTINGENCY PLANNING Contingency Planners Often Forget to Consider

Key Elements of the Supply Chain", *Security Management*, Vol. 44, No. 3, 2000, pp. 70-75.

[6] Jo, S., Lee, Y., and Choi, M., "A Study on Factors Influencing Telecommunications Fraud : In the Case of Voice Phishing", *Journal of Information Technology Service*, Vol. 15, No. 2, 2016, pp. 35-49.

[7] NIST SP 800-37, Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems : A System Life Cycle Approach, 2010.

[8] NIST SP 800-64, Rev. 2, Security Considerations in the System Development Life Cycle, 2008.

[9] NIST SP 800-64, Revision 2, Security Considerations in the System Development Life Cycle, 2008.

[10] Shaw, G. L. and Harrald, J. R., "Identification of the Core Competencies Required of Executive Level Business Crisis and Continuity Managers", *Journal of Homeland Security and Emergency Management*, Vol. 1, No. 1, 2004.

■ Author Profile

Myeoggil Choi

Professor M. Choi has served in Dept.of Business Administration in Chung-Ang Univ. and received his Ph.D from KAIST. Before joining his current institution, he had worked Inje University, ETRI (Electronic and Telecommunication Research Institution) and ADD (Agency for Defense Development) as senior researcher. He has been interested in information security. He has worked in research institutions and has published numerous papers in the international journals. He has also researched and worked in entrepreneurship.