Advanced approach to information security management system utilizing maturity models in critical infrastructure

Youngin You[1], Junhyoung Oh[1], Sooheon Kim[2] and Kyungho Lee[1]
[1] Institute of Cyber Security & Privacy (ICSP), Korea University
Anamro 145, Seoul, KOREA
[e-mail: {crenius, ohjun02, kevinlee}@korea.ac.kr]
[2] Data Marketing Korea Research Lab
Teheran Rd. 53 gil 16, Seoul, KOREA
[e-mail: sooheon.kim@datamarketing.co.kr]
*Corresponding author: Kyungho Lee

Received February 27, 2018; revised May 3, 2018; accepted May 15, 2018;
published October 30, 2018

Abstract

As the area covered by the CPS grows wider, agencies such as public institutions and critical infrastructure are collectively measuring and evaluating information security capabilities. Currently, these methods of measuring information security are a concrete method of recommendation in related standards. However, the security controls used in these methods are lacking in connectivity, causing silo effect. In order to solve this problem, there has been an attempt to study the information security management system in terms of maturity. However, to the best of our knowledge, no research has considered the specific definitions of each level that measures organizational security maturity or specific methods and criteria for constructing such levels. This study developed an information security maturity model that can measure and manage the information security capability of critical infrastructure based on information provided by an expert critical infrastructure information protection group. The proposed model is simulated using the thermal power sector in critical infrastructure of the Republic of Korea to confirm the possibility of its application to the field and derive core security processes and goals that constitute infrastructure security maturity. The findings will be useful for future research or practical application of infrastructure ISMSs.

Keywords: Critical infrastructure, Information Security Management System, Maturity model, Security evaluation

This research was supported by the Ministry of Science, ICT and Future Planning, Korea, under the Information Technology Research Center support program (IITP-2017-2015-0-00403) supervised by the IITP (Institute for Information & Communications Technology Promotion).

http://doi.org/10.3837/tiis.2018.10.020 **ISSN : 1976-7277**

1. Introduction

The use of cyber-physical systems (CPSs) is constantly increasing, which means that most organizations are becoming increasingly reliant on information systems [1]. Information security governance is an increasingly critical component of organizational management, and an overall system security structure that covers the attributes of a CPS environment is required [2][3]. Currently, organizations are collectively measuring and evaluating the capability of information security management; however, objectively evaluating a target system is difficult because security-level evaluation systems are not based on the individual characteristics of an organization or the organization's information security activities [4]. In addition, most standards-based information security management systems (ISMSs) have a silos effect because they do not have sufficient consideration of connectivity between security controls [5]. Specifically, in order to secure more than a certain level of security required by ISMSs, each department in the organization prioritizes security control activities that are easy to implement by considering each work efficiency first. However, each security control activity has correlation with each other and should be implemented sequentially considering this. For example, according to the results of analyzing the correlation between security controls for 15 power generation organizations in Korea, security controls with high correlation to other security controls such as Access Control, Maintenance and Contingency Planning can be confirmed [6]. This means that when implementing the control for Access Control, both Audit/Accountability and Personal Security should be considered at the same time for effectiveness. In addition, there are security control activities such as division of duties that should be preceded in order to implement account management and least privilege. The authoritative guideline, such as NIST SP 800 series and ISA / IEC 62443, which presents these security control activities, presents the security control items in a plan view and should be designed and used according to the target infrastructure field. National infrastructures that use industrial control systems with CPS environments also face the above problems. Therefore, this study proposes an information security maturity concept that can effectively evaluate and manage the level of information security for CPS environments in critical infrastructure. This concept was initially employed in the software engineering field [7], and its effectiveness and efficiency have already been verified [8]. So, this study introduces the maturity concept to information security. There are, of course, studies to apply maturity concepts to information security. Previous studies have considered a maturity model for information security; however, to the best of our knowledge, such studies have only presented abstract concepts and have not investigated practical applications [9]. ISA/IEC-62443, i.e., the standard for network and system security for industrial-process measurement and control, which is applicable to infrastructure cyber environments, recommends adoption of the maturity concept to assess an organization's information security management capacity [10]. However, the content of these guidelines is not enough to implement in practical. Therefore, we propose an advanced information security maturity assessment method for critical infrastructure, which is a concrete concept for the introduction of the above maturity concept into the field of information security. This proposed concept targets the thermal power generation field in Korea. Specifically, the specific maturity concept for the field is defined, and the methods and criteria for constructing each maturity tier are proposed. In addition, based on the proposed information security maturity concept, this study derives security activities for each maturity tier required for an infrastructure environment and simulates it relative to the Korean energy infrastructure. Through the simulation, this study confirms the applicability of the proposed maturity concept to cybersecurity by applying it to an actual service field. The overall procedure of the proposed assessment method is shown in **Fig. 1**.

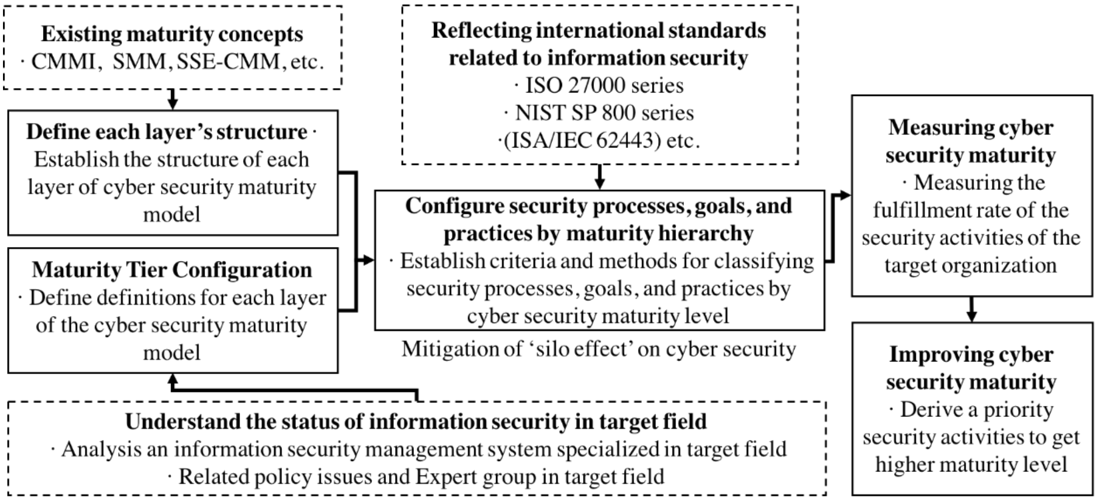
Existing maturity concepts
· CMMI, SMM, SSE-CMM, etc.
Reflecting international standards related to information security
· ISO 27000 series
· NIST SP 800 series
·(ISA/IEC 62443) etc.
Define each layer's structure · Establish the structure of each layer of cyber security maturity model
Maturity Tier Configuration
· Define definitions for each layer of the cyber security maturity model
Configure security processes, goals, and practices by maturity hierarchy
· Establish criteria and methods for classifying security processes, goals, and practices by cyber security maturity level
Mitigation of 'silo effect' on cyber security
Measuring cyber security maturity
· Measuring the fulfillment rate of the security activities of the target organization
Improving cyber security maturity
· Derive a priority security activities to get higher maturity level
Understand the status of information security in target field
· Analysis an information security management system specialized in target field
· Related policy issues and Expert group in target field

Fig. 1. Procedure of Advanced information security maturity assessment

The remainder of this paper is organized as follows. Section 2 discusses studies related to maturity concepts on information security. Section 3 describes the motivation for this study.

Section 4 defines each maturity tier, describes the hierarchical structure of each tier, and discusses the methods and criteria that comprise each tier. The concepts described in Section 4 include information derived from focus groups conducted by a university professor from the Korea Infrastructure Protection Society, a web application server engineer with more than 10 years of experience, an executive from the Korea Air Force Vulnerability Analysis Team, and a project manager from the Infrastructure Management System Development Project. Implementation and simulation of the proposed assessment methods are described in Section 5. The simulation is conducted using the Korean energy infrastructure to derive and propose practical information security activities included in each information security maturity layer. The conclusion, limitations, and implication of this study are presented in Section 6.

2. Related Work

This section reviews previous research into cyber security maturity concepts and models. There are various types of ISMSs that focus on organizational information security objectives; among them, this study focuses on a maturity model that measures the security level of an organization based on defined levels. Thus, studies that deal with the concept of precise maturity, which predefines the concepts of each level, are reviewed. And this section reviews studies that consider the overall concept of maturity and those that focus on the application of maturity concept in a particular field.

Lessing's study was based on the hypothesis that existing information security governance models are similar to information security maturity models (ISMMs). Governance models include all relevant aspects that can affect information security [11]. In other words, governance models include the elements that an organization's information security should consider for effective management. Governance models also describe best practices that can be implemented to reduce costs. The maturity concept in lessing's study comprises five stages [12]. It also explains relationship between risk and effort based on maturity concepts. The maturity concept of the five tiers defined here is somewhat abstract and simple, so we try to define and supplement the concept more specifically.

Security is important in all stages of a project, including planning, designing, and selecting architecture that can be implemented and deployed effectively and efficiently. This is only possible if security requirements are tied to business objectives. Devi (2011) stated that information security management should be based on organization management, organizational culture, system architecture, and service management. The proposed ISMM is based on the above four elements and represents a simple example of an evaluation method. The proposed ISMM is a qualitative method; however, a quantitative method is suggested as a future undertaking. Therefore, we propose a quantitative evaluation method based on the concept formation through qualitative methods.

Karabacak et al. (2016) proposed a maturity model to measure the level of readiness for national infrastructure security. They stated that existing studies on ISMSs are overly reliant on best practices[9]. Therefore, their paper was based on a Delphi [13] questionnaire for experts. Their study identified the root causes of problems with national infrastructure cyber security, such as "cyber security of critical infrastructure is not perceived by national security authorities as a vital component of national security." Based on this, 40 maturity criteria were weighted using the Delphi technique. Each weighted item was evaluated numerically, and the score was calculated based on the arithmetic mean. This was simulated in Turkey; however, as the authors indicated, there are significant differences in the environment and characteristics of each country. Therefore, results based on expert group interviews in one country are not necessarily applicable to other countries.

Yulianto et al. (2016) pointed out that many organizations are now focusing on technology improvements rather than reviewing and improving current processes. Thus, the successful implementation of the Payment Card Industry Data Security Standard (PCI-DSS) was considered to be dependent on an organization's overall information security capabilities rather than on the latest technologies. They proposed a maturity model consisting of four levels: none, initial, basic, and capable [14]. The ISMM for PCI-DSS (ISMM-PCI) is essentially based on best practices. Specifically, Yulianto et al. included the ISO/IEC 27001: 2013 control items based on the PCI-DSS requirements. These items were used to measure the information security management maturity level of the organization. The ISMM-PCI maturity measure is convenient; however, the maturation tier defined by the four levels is inclusive. In addition, the mapping or classification criteria of the items used for measurement are not specific. In order to be able to propose the maturity concept applicable to the field, it would be better if the specification of the criteria were a little more specific.

Various researches have studied the measurement of the information security maturity of target areas. However, to the best of our knowledge, studies to date are not enough to describe specific levels of measurement of organizational maturity or specific methods and criteria to construct them. Therefore, this paper propose the definition, criteria, and structure of information security maturity assessment to complement the research on information security maturity that has been going so far.

3. Motivation

To manage the inherent risks associated with infrastructure control systems, the organization must identify the minimum security criteria required for current system operations and provide an indicator to effectively understand the current level of security [14][15]. In regard this, in addition to the studies mentioned in Section 2, there are more than 50 studies on infrastructure information security management indexed to ACM Digital Library, IEEE Explore and Web of Science since 2000 [16]. However, most papers focus on the identification of vulnerabilities and threats to the industrial control systems targeted in each paper, and to quantify the risks based on them. Therefore, a measurement method is required to efficiently determine gaps between the current and required information security levels based on security activities. However, without considering the organic nature of security controls, it is difficult for information protection to penetrate the entire organization. Even in terms of security management, piecemeal security controls are causing disruption of intra-organizational communication. These problems can be solved by a maturity model that considers and reflects the relationship between security controls. A maturity model can be used to measure and reduce the gap between theory and practice [17]. In addition, maturity models can be applied to measure the capability of a specific area in an organization for effective management. Such models primarily measure the qualities of processes/structures, objects/technology, and people/culture. Typically, maturity models such as the capability maturity model, open-source maturity model, and the modeling maturity levels classification system are used in the software development field [18]. Thus, the effectiveness and efficiency of such models have been confirmed. Maturity concepts, such as capability maturity model integration (CMMI), used in the software development field may not be appropriate for the information security field. However, it is possible in terms of 'a common concepts of control'. That is, software development involves continuous control and information security also involves continuous control relative to unknown attacks. Therefore, this study intends to introduce the concept of maturity that can reflect the characteristics of security control as information security management system based on security control activities. Maturity as it relates to information security has been studied previously; however, to the best of our knowledge, no study has suggested how to define and construct maturity levels specifically for information security (Section 2). In addition, it has not been confirmed that the status of information security can be well observed using the concept of maturity. Therefore, this study proposes a practical method to measure maturity as it relates to information security in critical infrastructure. The proposed concept was developed based on information obtained from a group of experts involved in infrastructure information protection (Section 1). Previous approaches to establishing overall maturity concepts used a top–down approach, similar to that proposed by Becker et al. [17]. This study also presents the security activities of each proposed maturity concept and simulates them based on the Korean infrastructure to demonstrate practical application to information security.

4. Advanced Information Security Maturity Assessment methods

Advanced information security maturity assessment (AISMA) methods define each level of infrastructure security maturity, including the sub-criteria used to construct each level. AISMA methods measure and index the maturity of a target organization and present a roadmap to achieve information security. To overcome the limitations of previous conceptual studies, this study proposes concrete definitions for each level and detailed criteria and methods to construct them. The framework is based on CMMI defined for software engineering [12]. To construct an advanced information security maturity measurement framework suitable for infrastructure, FGIs were conducted with infrastructure security experts, including a web application server engineer with more than 10 years of experience, an executive from the Korea Air Force Vulnerability Analysis Team, and a project manager of the Infrastructure Management System Establishment Project [19]. Specifically, each element required for securing the security of the industrial control system and each phase for implementing it are discussed, and perspectives suitable for constructing additional criteria to building each maturity tier are derived. This was based on meeting the following three requirements. The first requirement must comply with existing maturity frames, and the second must cover the scope of existing information protection management system standards. The last should include clear criteria for constructing and assessing information security maturity. And it is based on a distributed control system, one of the industrial control systems with 50 servers and PCs, 50 pieces of network devices and 40 process control facilities in the power generation field. The structure of the derived AISMA methods is as follows. There are five tiers of maturity, with each tier having its own definition and characteristics. And detailed criteria were established for each maturity tier. The maturity model derived in this study is based on the thermal power generation sector, which is part of a country's critical infrastructure. An outline of advanced information security maturity assessment methods is shown in Fig. 2.

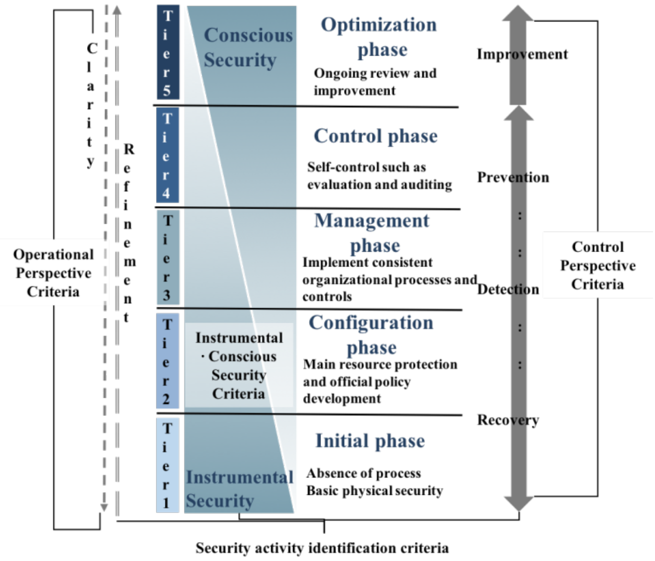
Clarity
Refinement
Tier 5
Tier 4
Tier 3
Tier 2
Tier 1
Conscious Security
Optimization phase
Ongoing review and improvement
Control phase
Self-control such as evaluation and auditing
Management phase
Implement consistent organizational processes and controls
Configuration phase
Main resource protection and official policy development
Initial phase
Absence of process
Basic physical security
Instrumental · Conscious Security Criteria
Instrumental Security
Improvement
Prevention
Detection
Recovery
Operational Perspective Criteria
Control Perspective Criteria
Security activity identification criteria

Fig. 2. Outline of Advanced information security maturity assessment method

4.1 Maturity tier definitions

Each maturity level of the AISMA methods is based on the main concept of ISA/IEC-62443 and can be applied to other information security-related criteria and maturity concepts. ISA/IEC-62443 is used because the scope of the criteria and guides for industrial control systems is the widest [20][21]. Unlike other criteria and guides, this covers the concepts of risk assessment/level evaluation/management, asset identification and classification, threat/vulnerability assessment, and countermeasures[10]. The AISMA methods consist of five tiers. Each phase provides the strength of the security controls that the organization currently performs and the future development level. To this end, we have embodied each layer based on physical and environmental security, protection of explicitly critical IT infrastructure resources, consistent protection procedures and controls throughout the organization, organizational self-control, continuous review and optimization. Each phase is described in detail below.

A. Intial phase

The first tier is where basic control is performed without a formal policy or procedure. This tier performs basic manpower control, such as unauthorized physical access control to the organization's ICT equipment and information assets[22]. From an information security perspective, this tier involves a relatively basic concept; thus, the control items associated with this tier generally have readily acceptable characteristics.

B. Configuration phase

The second tier is the configuration phase. As information security is deemed important in an organization, protecting network infrastructure resources begins in this tier through various means, such as fraud detection systems, firewalls, encryption, and educating employees about security awareness [23]. The management targets in the configuration phase include various resources, such as hardware constituting the application system and commercial software, and the basic network infrastructure for both internal and external communication.

C. Management phase

The third tier is the management phase. In this tier, information security policies and procedures are established and managed for the entire organization. In addition, policies and procedures for security-conscious management are established and executed in this tier [24]. This protects critical infrastructure resources, application systems, and data from damage and unauthorized access through various methods such as authentication and authorization control. In the management tier, all application-level functions are managed and administered between applications and their user interfaces.

D. Control phase

The fourth tier is the control phase, in which self-organization control becomes possible, self-audit and responsibility policies and procedures are established, and risk analysis and management are performed. This tier includes business continuity planning and organizational self-assessment of information security. It focuses primarily on conscious security, conducting security awareness training for all employees, and observing employee behavior [25].

E. Optimization phase

The fifth tier is the optimization phase, which is implemented to continually review and improve information security processes by considering security measures from different perspectives. Note that reaching the fifth tier does not mean that an organization has implemented a system that guarantees perfect security. However, it does mean that such a system has been designed with a very high level of information security, which allows quick detection and recovery from incidents and establishes continuous monitoring and improvement processes.

AISMA methods encompass the main ISMM concepts and the scope of information security criteria, as shown in **Table 1**. And AISMA preserve the unique concept of maturity that originated in CMMI [16]. The information security management maturity model (ISM3) is an information security maturity concept established through its own consortium [26]. ISM3, ISMM, and Gartner have proposed representative concepts of information security maturity, and NIST and ISA/IEC-62443 are the broadest infrastructure information protection standards. Therefore, they are considered the basis of the proposed concept [27][28].

Specific security control activities for the above maturity hierarchy concepts are provided in section 5.

Table 1. Coverage of Advanced information security maturity assessment method

Tier	**CMMI**	**Other Security Maturity Concepts**					**AISMA**
		ISM3	ISMM	Gartner	NIST	ISA/IEC 62443	
1	Process absence / unpredictability	Physical Security	-	No information security program or documentation	Policy Placement	Physical and environmental security	Physical access control
2	Documentation, planning, execution, observation, control, and application of processes	Records of information security processes	Define some roles and responsibilities related to security section	Develop official policy for critical areas / Designate security team	Use policies and procedures (define IT security responsibilities and expected behavior)	Staff training and security awareness	Conduct critical infrastructure resource protection and security awareness training
3	Application of process standards, procedures, and tools at the organization level	Use process results to improve individual processes	Approve common policies and processes across the organization	Introduction of strategic security program	Implement consistent IT security procedures and controls	Element: Security policies and procedures	Establish policies and procedures for protecting applications and application systems and managing security consciousness
4	Process management using statistical and quantitative techniques	-	-	-	Testing, corrective actions for vulnerabilities, mitigation of risk	Conformance	Self-control (self-audit and testing, vulnerability testing, etc.)
5	Continual improvement and management of processes	Improve information security	Optimization of processes and procedures	Continuous process improvement	Implement appropriate security levels for all policies and procedures	Review, improve, and maintain the CSMS	Continuous review and improvement

4.2 Structure of each maturity tier

Completion of each tier of the AISMA methods is an indicator of how well an organization is implementing appropriate levels of information security. Each tier comprises one or more security processes that must be performed to achieve that level. If the performance of the security processes of each tier is above a certain level, the security maturity of the given tier is achieved.

Each security process has several goals that must be achieved. Here, the goal is to determine the extent to which security processes are executed within an organization, e.g., emergency blocking and least privilege. However, the concept of these goals is abstract; therefore, it must be linked to practices that are described in detail. Practices are specific security activities that must be performed to meet specific objectives. An overview of the security processes, objectives, and practices is given in **Table 2** [29].

Table 2. Concepts of information security process, goals and practice

Category	Description
Security Processes	- Activities to be performed to achieve the security level of the layer are placed at levels 1 to 5
Goals	- Goals to be achieved in the security process area - Criteria for determining the degree to which each security process is performed within the organization
Practices	- Specific security activities to meet the objective that constitute each security process area

Security practices consist of security processes and items involved in deriving the goals and security activities of each area of the infrastructure. Additional criteria for precisely configuring each maturity tier with security processes, goals, and practices are described in Section 4.3. Security practices comprise items involved in deriving security processes and goals, as well as security activities performed in each area of the infrastructure. The basic unit for understanding the security activity rate of each maturity tier is the security goal. In addition, the security goal is the minimum unit of decision-making for improving the security level of an organization.

4.3 Additional criteria for configuration each tier

To measure the information security maturity of an organization using a hierarchical definition, it is necessary to implement the abovementioned processes, goals, and practices. Security processes, goals, and practices are established in terms of infrastructure and security-related criteria (ISO 27001/27002, NIST 800-53/82, ISA 62443, etc.), and the definition of each tier (initial, configuration, management, control, and optimization) can be placed in the maturity level after establishment. Basically, each security process, goal, and practice is based on hierarchical definitions and related criteria. However, when deploying practices to hierarchical processes and goals for better classification in each maturity tier, it refers to the control and operational perspective and conscious and instrumental security criteria. In order to derive these criteria, it was discussed based on the propensity of the security control itself, the perspective on the operation of security control activities, and the security target of the security controls.

A. Control and operational perspective criteria

The control and operational perspective criteria refer to the concept of the dimensional structure maturity model. Among these, the control viewpoint criteria are added to improvement procedures for prevention, detection, and restoration, which are the three primary information security procedures. Existing information security controls are classified according to various criteria such as behavior, security objective, and function. It is divided into preventive control, detective control, and restorative control by behavior, and it is divided into integrity control, confidentiality control, and availability control by security objective. And by function, it is divided into administrative control, technical control, and operational control. In order to achieve security control at the highest level, it is necessary to continuously improve the security level. NIST SP 800-53, ISO / IEC 27001, ISO / IEC 15408, etc. The current security control related standards are also updated to include improvements. Therefore, in this study, improvement control is added based on the control classification by behavior as **Table 3**.

So, control viewpoints comprise recovery, detection, prevention, and improvement. Maturity levels 1 to 4 are related to recovery, detection, and prevention. Improvements are referenced in the deployment of practices to achieve the goals of the maturity tier five security process.

Table 3. Control Perspective criteria for Security Maturity Configuration

Category	**Description**
Improvement	Concepts of continuous monitoring, evaluation, and follow-up of the information security process
Prevention	Concepts applicable to all tiers, including policies, procedures, controls, and processes to protect information from unauthorized modification or exposure
Detection	Concepts to detect anomalous behavior in a system at an early tier
Restoration	The concept that the detection process must precede to make sense, the procedure for timely response to accidents and abnormality detection

Implementation and operation of security controls, it can generally be based on a structure of the target system configuration. In case of the critical infrastructure subject to this paper, industrial control system can be categorized as Human Machine Interface, Controller, Sensor & Actuator, Maintenance according to NIST SP 800-82. Although security controls can be categorized and operated on the basis of this, it is difficult to consider the maturity level of security activities. Therefore, this study established the operational perspective criteria of the following concept as **Table 4**. The operational perspective considers the level of technology management, including the degree to which each process is exposed to both attackers and insiders, and the depth and cost of the knowledge required. It is based on two indexes, i.e., complexity and visibility, by referencing the dimensional structure maturity model, and is introduced by redefining the concepts of clarity and refinement.

Table 4. Operational Perspective criteria for Security Maturity

Category	**Description**
Clarity	- Extent to which security practices are exposed to insiders - Degree of clarity increases as maturity level goes down (the higher the clarity, the more vulnerable it is to attack)
Refinement	- Level of depth, cost, technology, and management of knowledge required for security practices - The higher the refinement index, the higher the level of knowledge, cost, and skills required to implement and manage security practices

B. Conscious and instrumental security criteria

In order to manage information security effectively, security objectives that each security activity is aiming for should be considered. For example, whether security activities target physical space or cyberspace. If the security activity falls into cyberspace, it is important to consider which layers, such as the operating system and software, are targeted. There are well-known OSI 7 layer and Cyber terrain concepts that can support this. The OSI 7 layer is a network-based concept, and Cyber terrain is a threat-centered concept of defense. Although both concepts can indicate the location of security activities, the proposed maturity concept should be able to include the security objectives and targets required in the entire organization. Therefore, in this study, conscious and instrumental security criteria which can include all of them were established and used. Conscious and instrumental security criteria are concepts that classify the elements to achieve information security and involve executing practices to achieve the goals of the security process defined in each tier.

Instrumental security involves technology that safeguards information from forgery, alteration, and leakage, and protects assets from various physical threats, such as theft, destruction, and fire. Instrumental security can be achieved by constructing various physical and information security systems, and a system that links, measures, and analyzes such systems should be established. This concept includes vaccines, intrusion detection systems, intrusion prevention systems, and server access control, as well as the encryption of CCTV, access control, and motion sensors. In addition, as the instruments security concept is advanced, it implies active security, which is fused with the conscious security concept. Here, highly sophisticated implementation is required.

The conscious security criteria represent the knowledge and attitudes of an organization's members relative to the security of the physical environment and information assets. In other words, having conscious security criteria means that members understand and respond to the potential risks of information security, such as intentional or accidental deception, damage, and theft of information assets. Typical ways to achieve conscious security include security awareness training relative to trade secrets, personal information security, and access control policies. Conscious security increases as the level of security maturity increases, while the degree of clarity becomes lower and that of refinement increases. If conscious security is relatively low, security awareness education should be implemented throughout the organization. On the contrary to this, as the level increases, security processes, such as policies and procedures for security conscious management, auditing, and responsibility, will be established systematically. A high level of conscious security provides various advantages, such as enabling members to use security functions appropriately, allowing employees to report potential security issues, and understanding the overall importance of security.

5. Simulation : Thermal Power Generation in Korea

The validity of the method of managing information security begins with the applicability of the method. The purpose of this simulation is to show that the method is not "accurate" but rather practical [30]. Therefore, we show that adopting such a method is reasonable in managing infrastructure information security.

A simulation was performed to confirm that the proposed maturity concept is applicable to information security. Through this simulation, by identifying causal relationships in existing security controls, the proposed maturity concept can more organically assess the status of information security. The advanced information security maturity assessment method described in Section 4 was simulated using the procedure shown in **Fig. 1** (Section 1). The implemented assessment method was simulated for power generation facilities among Korea’s critical infrastructure facilities. Specifically, this was done in conjunction with the research project for the improvement of infrastructure information security system, five thermal power plants equipped with an industrial control system were measured. Information security maturity was measured based on the security control activities carried out at each power plant.

5.1 Outline of AISMA derived for simulation

A total of 185 information security control activities were derived to measure maturity. It is mainly based on ISA/IEC-62443, which covers the broadest concept, and reflects ISO/IEC 27001/27002 and NIST SP 800-53/82 [31][32][33]. The 185 security practices were classified into 81 security objectives and 17 security processes according to the detailed criteria (Section 4.3), such as control and operation viewpoints, and were mapped to each maturity level. **Table 5** summarizes the details derived according to the maturity level criteria (Section 4) used to assess the information security maturity of the target facilities. We constructed a checklist based on the 185 security control activities derived and conducted the measurements. Practitioners of five thermal power plants, which were the targets of the project to establish infrastructure information security management system, participated in this. Two facilities were measured through on-site visits and three were performed online. Specifically, responses to the implementation of each security control activity consist of 'Yes', 'No', 'Partial', and 'N / A’. A 'Yes' response indicates compliance with applicable security control activities and that it has relevant evidence and documentation of compliance. The 'No' response corresponds to the case where the organization being evaluated does not meet the criteria and there are no relevant grounds and documents. The 'Partial' response means that the level of compliance of the security control activity is insufficient, or the relevant grounds and documents are partially maintained.

Table 5. Derived security activities for Critical Infrastructure

Maturity level	Security Processes	Goals (n): number of practices
Optimization phase	Audit and accountability	Auditable events (1), Response to audit processing failure (1), Reduces unnecessary audits and generates reports (1)
	Security assessment and authorization	Policies and procedures for security assessment and certification (2), Security assessment (3), Continuous monitoring (3)
	Configuration management	Control over configuration changes (1), Restrict access to configuration changes (1)
	Business continuity planning	Testing and implementing business continuity planning (1)
	Planning	Planning for system security (1)
	Risk assessment	Vulnerability scan (3)
	System and information integration	Actions against system defects (1)
Control phase	Access control	Separation of duties (4), System usage notice (2), Access control for mobile devices (2)
	Audit and accountability	Audit and responsibility policies and procedures (2), Auditable events (2), Audit incidents (1)
	Security assessment and authorization	Security assessment (1)
	Configuration management	Security impact analysis (1)
	Business continuity planning	Policies and procedures for business continuity planning (2), Testing and implementing business continuity planning (2), Control system recovery and reconfiguration (1)

	Incident response	Incident response training (1), Incident response testing and practice (1), Incident handling (1), Incident response plan (1)
	Physical and environmental protection	Physical access monitoring (1)
	Planning	Behavioral rules (1), Personal information impact assessment (1)
	Privacy	Transfer of personnel (1), Personal sanctions (1)
	Risk assessment	Risk management (1), Vulnerability scan (3)
	Acquisition of systems and services	Purchase (1), Security engineering principles (1), Supply chain protection (1)
	System and information integration	Actions against system defects (3)
	Awareness and education	Security training (1)
Management phase	Access control	Access control policies and procedures (2), Control system account management (10), Least privilege (1), Parallel session control (1), Session lock (3), Remote access (3), Wireless access (2), Access control for mobile devices (3)
	Audit and accountability	Response to audit processing failure (1)
	Configuration management	Restrict access to configuration changes (1)
	Business continuity planning	Alternative processing location (3)
	Identification and authentication	Identification and authentication policies and procedures (2), User identification and authentication (institutional users) (1), Device verification and authentication (1), ID management (1)
	Incident response	Incident response policies and procedures (2)
	Maintenance	System maintenance policies and procedures (2), Remote maintenance (3), Maintenance personnel (1)
	Storage media protection	Storage media protection policies and procedures (2), Marking storage media (1)
	Physical and environmental protection	Physical and environmental protection policies and procedures (2)
	Acquisition of systems and services	Software installed by the user (1)
	Communication and system protection	Application classification (1), Separation of security functions (1), Public access protection (1), Co-computing device (1), Mobile code (2), VOIP (2)
	System and information integration	Prevent malware (5), Anti-spam (2)
	Awareness and education	Security awareness and education policies and procedures (2), Security training (1)
Configuration phase	Access control	Login attempt failed (2), System usage notice (2), Remote access (3), Wireless access (3), Access control for mobile devices (3)
	Audit and accountability	Auditable events (2), Audit incidents (3)
	Configuration management	Restrict access to configuration changes (1)
	Identification and authentication	Cryptographic module authentication (1)
	Maintenance	Remote maintenance (3)
	Storage media protection	Storage media access (1), Marking storage media (1)
	Communication and system protection	Information from a shared resource (1), Protection against denial of service (1), System boundary protection (4), Transport integrity (1), Transfer confidentiality (1), Terminate network connection (1), Trust path (1), Cryptographic key establishment and operation (1), Using passwords (1), Session authentication (1)
	Awareness and education	Security awareness and education policies and procedures (1)
Initial phase	Storage media protection	Keep the storage media (4), move storage media (2)
	Physical and environmental protection	Physical access rights (3), Physical access monitoring (2), Outsider control (1), Emergency block (1), Emergency light (1), Fire

		prevention (1), Temperature and humidity control (1), Flood damage prevention (1), Component location (1)

The 'N / A' response is selectable if the security control activity is not correlated with the industrial control system business process being measured. Each is given 1 point for Yes, 0 points for No, and 0.5 points for Partial, and N / A (Not Applicable) is excluded from the score calculation. Since security control activities have already been deployed at each mature level, no separate weighting was taken into account in the score calculation.

5.2 Simulation Result

In the simulation, the process fulfillment rate of each maturity tier, the security maturity level of each facility, and the level of implementation of individual processes and targets were confirmed. The simulation derived the priority security process and goals for each facility and finalized security practices that require implementation and supplementation to achieve.

The results of the assessments of five facilities based on the AISMA established in section 5.1 are shown in **Table 6**. The answers to derive results and scores were organized into four categories according to the description in section 5.1 for each tier. Result means security activities corresponding to Yes (1) / Partial (0.5) / No (0) / NA and Score indicates average values based on this.

Table 6. Assessment result by derived security activities

Maturity Tier	Category	'A' Facility	'B' Facility	'C' Facility	'D' Facility	'E' Facility
Tier 1	Score	1.000	1.000	0.840	0.625	0.545
Tier 2	Score	0.962	0.929	0.946	0.571	0.308
Tier 3	Score	0.983	0.980	0.790	0.447	0.127
Tier 4	Score	1.000	1.000	0.783	0.464	0.100
Tier 5	Score	1.000	1.000	0.711	0.211	0.000
Excluding all facilities' score calculation with common N / A		Remote access, Wireless accss, Access control for mobile devices, Remote maintenance				

The security controls themselves may not be applied to the target facilities according to the size of the facility, equipment's aging condition, the operation policy, etc. to be assessed. These items are classified as N/A. Therefore, although the distributional deviation of the N/A item may occur depending on the facilities to be assessed, it is possible to maintain some degree of assessment equality. In the case of the five facilities that were the subject of this simulation, remote access, wireless access, mobile device access control and remote maintenance were not used originally. Thus, items corresponding to these can be excluded in common from the next assessment. This can be refined as assessments and improvements are repeated.

The overall fulfillment results of the simulation are as follows: Tier 1 81% (initial phase), Tier 2 65% (configuration phase), Tier 3 65% (management phase), Tier 4 63% (control phase), and Tier 5 58% (optimization phase). These results show that the process fulfillment rates decreased as the tiers advanced. In general, the maturity concept adopts 75% to 85% or more of the implementation rate of the activities included in each tier as a reference value for achieving the maturity tier. In this study, if the implementation rate of the information security activities included in a given maturity tier is greater than or equal to 80%, the corresponding maturity level is achieved. This can be adjusted after application 2 or 3 times in the field being assessed. An outline of the measurement results for the five facilities is shown in **Fig. 3**.

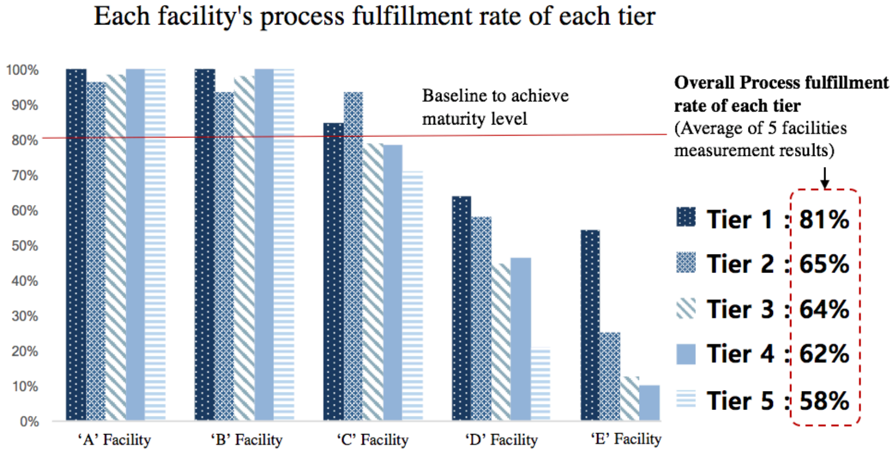

Fig. 3. Summary of the simulation result

Facilities A and B have a security maturity level of 5 because the hierarchical process fulfillment rates for all five tiers are more than 80% for these facilities. In case of facility C, tiers 1 and 2 show 89% and 94% process fulfillment rates, respectively; however, the process fulfillment rates of tiers 3, 4, and 5 are less than 80%, thereby resulting in maturity level 2. For facilities D and E, the process fulfillment rates of all tiers are less than 80%; thus, these facilities have not even achieved security maturity level 1.

For facilities (D, E) that have not reached maturity level 1, the security control belonging to the initial phase should be performed first and maturity level 1 should be achieved. Security activities at maturity level 1 and maturity level 2 are not based on information security policies and procedures. Therefore, in the case of E facilities, level 2 is expected to be achieved faster than other higher levels after achieving maturity level 1 when performing security enhancements. D facilities, since policies and procedures for information security have been partly established and the implementation of their own organizational control has begun, it will be effective to implement tier 2 and tier 3 in parallel after achieving level 1. C facilities are considered to be achievable in the final maturity tier. Details for facility C are shown in **Fig. 4**.

The fulfillment rates of the security process for facility C are 89% in tier 1 (initial phase), 94% in tier 2 (configuration phase), 77% in tier 3 (management phase), 78% in tier 4 (control phase), and 71% in tier 5 (optimization phase); thus, facility C achieved level 2 security maturity. In this case, since the process fulfillment rates of tiers 3, 4, and 5 are all greater than 70%, it is possible to improve the security maturity level to 5 by selecting and executing the priority target according to the implementation status. In other word, sufficient tier 2 security maturity has been accomplished; thus, it is necessary to improve processes belonging to tier 3 rather than those belonging to tiers 1 and 2. From the index of the results for facility C, we can derive the priority items required to achieve tier 3, i.e., mobile code and VOIP, which are goals included in the communication and system protection process.

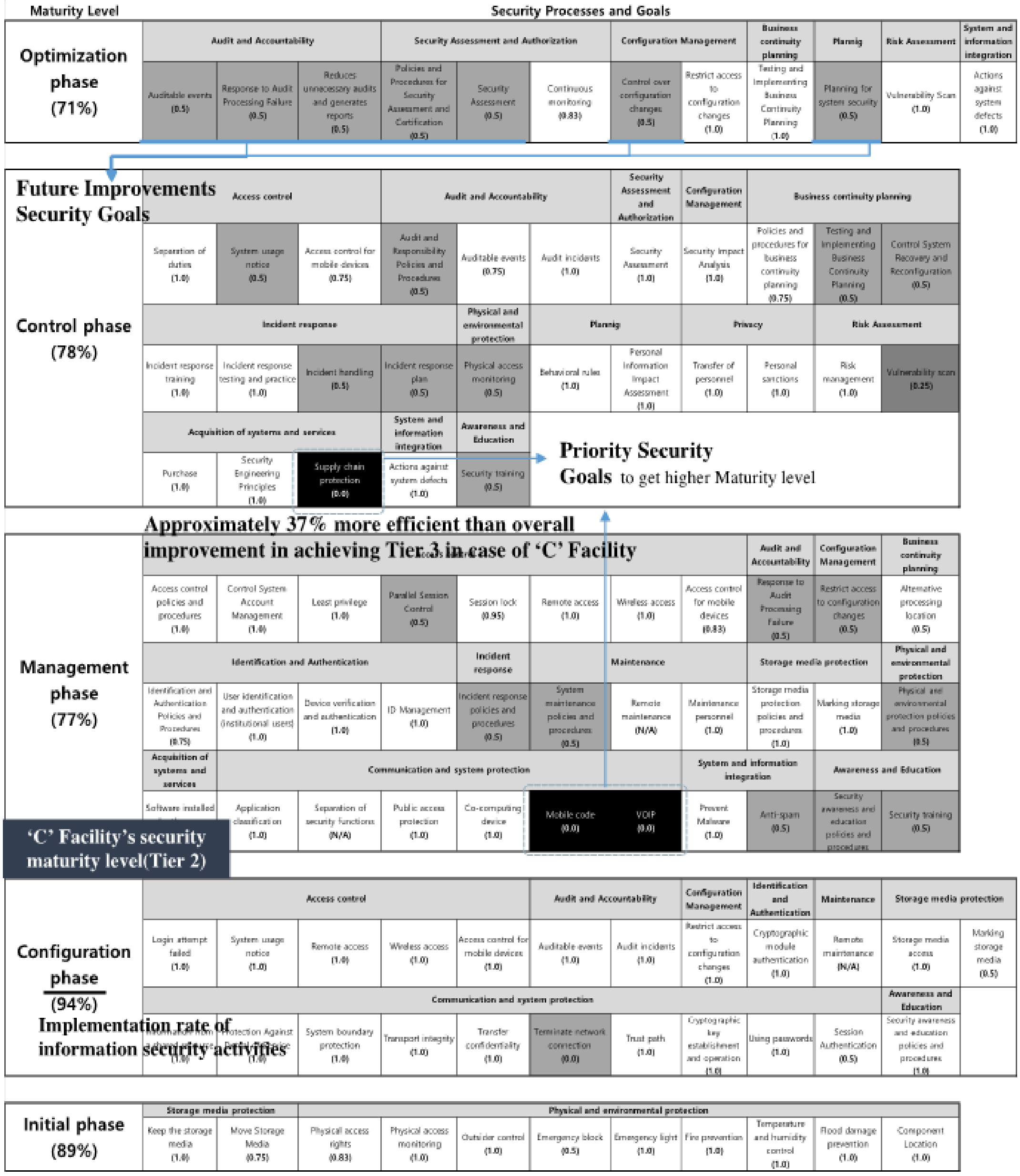
Maturity Level
Security Processes and Goals
Optimization phase (71%)
Audit and Accountability
Security Assessment and Authorization
Configuration Management
Business continuity planning
Plannig
Risk Assessment
System and information integration
Auditable events (0.5)
Response to Audit Processing Failure (0.5)
Reduces unnecessary audits and generates reports (0.5)
Policies and Procedures for Security Assessment and Certification (0.5)
Security Assessment (0.5)
Continuous monitoring (0.83)
Control over configuration changes (0.5)
Restrict access to configuration changes (1.0)
Testing and Implementing Business Continuity Planning (1.0)
Planning for system security (0.5)
Vulnerability Scan (1.0)
Actions against system defects (1.0)
Future Improvements Security Goals
Control phase (78%)
Access control
Audit and Accountability
Security Assessment and Authorization
Configuration Management
Business continuity planning
Separation of duties (1.0)
System usage notice (0.5)
Access control for mobile devices (0.75)
Audit and Responsibility Policies and Procedures (0.5)
Auditable events (0.75)
Audit incidents (1.0)
Security Assessment (1.0)
Security Impact Analysis (1.0)
Policies and procedures for business continuity planning (0.75)
Testing and Implementing Business Continuity Planning (0.5)
Control System Recovery and Reconfiguration (0.5)
Incident response
Physical and environmental protection
Plannig
Privacy
Risk Assessment
Incident response training (1.0)
Incident response testing and practice (1.0)
Incident handling (0.5)
Incident response plan (0.5)
Physical access monitoring (0.5)
Behavioral rules (1.0)
Personal Information Impact Assessment (1.0)
Transfer of personnel (1.0)
Personal sanctions (1.0)
Risk management (1.0)
Vulnerability scan (0.25)
Acquisition of systems and services
System and information integration
Awareness and Education
Purchase (1.0)
Security Engineering Principles (1.0)
Supply chain protection (0.0)
Actions against system defects (1.0)
Security training (0.5)
Priority Security Goals to get higher Maturity level
Approximately 37% more efficient than overall improvement in achieving Tier 3 in case of 'C' Facility
Management phase (77%)
Audit and Accountability
Configuration Management
Business continuity planning
Access control policies and procedures (1.0)
Control System Account Management (1.0)
Least privilege (1.0)
Parallel Session Control (0.5)
Session lock (0.95)
Remote access (1.0)
Wireless access (1.0)
Access control for mobile devices (0.83)
Response to Audit Processing Failure (0.5)
Restrict access to configuration changes (0.5)
Alternative processing location (0.5)
Identification and Authentication
Incident response
Maintenance
Storage media protection
Physical and environmental protection
Identification and Authentication Policies and Procedures (0.75)
User identification and authentication (institutional users) (1.0)
Device verification and authentication (1.0)
ID Management (1.0)
Incident response policies and procedures (0.5)
System maintenance policies and procedures (0.5)
Remote maintenance (N/A)
Maintenance personnel (1.0)
Storage media protection policies and procedures (1.0)
Marking storage media (1.0)
Physical and environmental protection policies and procedures (0.5)
Acquisition of systems and services
Communication and system protection
System and information integration
Awareness and Education
Software installed
Application classification (1.0)
Separation of security functions (N/A)
Public access protection (1.0)
Co-computing device (1.0)
Mobile code (0.0)
VOIP (0.0)
Prevent Malware (1.0)
Anti-spam (0.5)
Security awareness and education policies and procedures
Security training (0.5)
'C' Facility's security maturity level(Tier 2)
Configuration phase (94%)
Access control
Audit and Accountability
Configuration Management
Identification and Authentication
Maintenance
Storage media protection
Login attempt failed (1.0)
System usage notice (1.0)
Remote access (1.0)
Wireless access (1.0)
Access control for mobile devices (1.0)
Auditable events (1.0)
Audit incidents (1.0)
Restrict access to configuration changes (1.0)
Cryptographic module authentication (1.0)
Remote maintenance (N/A)
Storage media access (1.0)
Marking storage media (0.5)
Communication and system protection
Awareness and Education
Information from Protection Against Denial of Service (1.0) (1.0)
System boundary protection (1.0)
Transport integrity (1.0)
Transfer confidentiality (1.0)
Terminate network connection (0.0)
Trust path (1.0)
Cryptographic key establishment and operation (1.0)
Using passwords (1.0)
Session Authentication (0.5)
Security awareness and education policies and procedures (1.0)
Implementation rate of information security activities
Initial phase (89%)
Storage media protection
Physical and environmental protection
Keep the storage media (1.0)
Move Storage Media (0.75)
Physical access rights (0.83)
Physical access monitoring (1.0)
Outsider control (1.0)
Emergency block (0.5)
Emergency light (1.0)
Fire prevention (1.0)
Temperature and humidity control (1.0)
Flood damage prevention (1.0)
Component Location (1.0)

Fig. 4. Result indicator of 'C' facility

By implementing the practices included in the above goal, facility C will acquire security maturity level 3 and security maturity level 4 will be accomplished by implementing the supply-chain protection goal of the system and service acquisition process. In the same manner, security maturity level 5 can be achieved by complementing tier 5's audit and accountability, security assessment and authorization, planning, and configuration management processes. Compare to overall security improvement, the indicators shown in Fig. 4 suggest that facility C only needs to complement 37% of security activities to achieve security maturity level 3. It is also possible to make efficient decisions about improvement activities performed after supplementing security control activities to achieve maturity level 4.

Specifically, in the indicators proposed in this study, security control activities to achieve the same security goal are distributed according to the level defined in each tier. **Table 5** shows the contents of this. Therefore, according to the result obtained after evaluating the target organization, it is possible to complement the items that can be linked with the upper item among the security control activities of each layer, before the other items, for the security goal that needs to be supplemented. For example, in the case of facility C, after completing the priority improvement items for achieving the fourth stage of maturity tier, the security control activities are selectable which should be preceded before performing security control activities such as system usage notice and audit and responsibility.

Note that it is very difficult to implement all recommended security activities. Therefore, effective strategies are needed to meet the level of security required by an organization. The AISMA methods presented in this paper can be a good solution to this issue. And, this will make intuitive decision-making possible and a strong basis for this. This study has also confirmed that the simulation of AISMA methods allows us to evaluate information security from a maturity perspective.

6. Conclusion, limitations and implication

An overall management system that considers both physical and cyber characteristics is required to achieve information security for critical infrastructure. In other words, it is evident that detailed technology is important; however, an ISMS must cover an entire organization [34]. Currently, the information security of the critical infrastructure is checked and diagnosed; however, the existing ISMS does not define a specific maturity level for information security controls. In addition, there are no criteria or methods available to measure the maturity level. And the level of guidance provided by ISO / IEC, 62443, and related studies alone will be difficult to define and accurately measure the maturity level. Because each standard and guideline that provides the security controls used information security management has a different focus and coverage, there is also a need for a way to implement it properly. This study proposed AISMA which can complement the above problems. This was based on the concept of maturity that can effectively perform and measure each security control activity. The proposed method and criteria for configuration each tier and detailed maturity level items have been presented and simulated relative to five energy facilities in the Republic of Korea to demonstrate the applicability of the proposed definitions of each maturity tier, as well as the methods and criteria involved in each tier. In addition, security activities applicable to actual fields required for each layer of infrastructure security maturity have been derived and presented. Because of the sensitivity and criticality of the infrastructure, it was not possible to apply the results derived from the simulation in batches. However, we confirmed the practicability of this information security management method through simulation. Therefore, the proposed concept of information security maturity and the security control activities mapped to the concept are practical.

There were limitations to this study. The source of the data collected for the simulation of this study is limited to the infrastructure of Korea. In other words, the results collected are limited to the characteristics of the Korean thermal power generation such as environmental characteristics, operational policies and organizational culture. Therefore, when data is collected by applying AISMA to various national infrastructures, the content of the proposed method can be tuned more precisely. Another important limitation is the fact that it is very difficult to gain the authority to survey and collect data for each organization due to the closed nature of the critical infrastructure. Therefore, in this study, the primary results were derived based on the collected data, but the feedback to these results could not be confirmed. If on-site feedback is possible, more accurate validation of the proposed method will be possible.

Existing security activities in the information security field were predominantly preventive. However, current trends in information security field's security activities are shifting from traditional prevention to sustainable security emphasized by international standards such as ISO / IEC 27001 and NIST SP 800-53. In this context, the results of this study show that there is an organization that is far below the level of security maturity, which has the final goal of continuous review and improvement of the organization itself. In other words, despite the fact that they belong to the same generation field in the same industry field, there is a big gap between organizations in the maturity of the security perspective. Therefore, in order to respond to the core concept required for information security, it is considered that the index for sustainable security such as AISMA suggested in this study is required.

Lastly, the proposed criteria for constructing maturity model can be useful for establishing maturity model in other fields. And, it is expected that the results demonstrated in this paper will advance similar future research in fields other than infrastructure.

References

[1] Q. Shafi, “Cyber Physical Systems Security: A Brief Survey,” in *Proc. of 2012 12th Int. Conf. Comput. Sci. Its Appl.*, pp. 146–150, 2012. Article (CrossRef Link)

[2] S. Amin, G. A. Schwartz, and A. Hussain, “In Quest of Benchmarking Security Risks to Cyber-Physical Systems,” *IEEE Network*, vol. 27, no. 1, pp. 19–24, February, 2013. Article (CrossRef Link)

[3] R. Bojanc and B. Jerman-Blažič, “A Quantitative Model for Information-Security Risk Management,” *Eng. Manag. J.*, vol. 25, no. 2, pp. 25–37, 2013. Article (CrossRef Link)

[4] W. Knowles, J. M. Such, A. Gouglidis, G. Misra, and A. Rashid, “Assurance Techniques for Industrial Control Systems (ICS),” in *Proc. of First ACM Work. Cyber-Physical Syst.* pp. 101-112, 2015. Article (CrossRef Link)

[5] T. C. C. Tan, A. B. Ruighaver, and A. Ahmad, “Information Security Governance : When Compliance Becomes More Important than Security,” in *Proc. of IFIP*, pp. 55–67, 2010. Article (CrossRef Link)

[6] Y. You, I. Cho, and K. Lee, “An advanced approach to security measurement system,” *J. Supercomput*, vol. 72, no. 9, pp. 3443–3454, 2016. Article (CrossRef Link)

[7] K. L. Thomson and R. von Solms, “Towards an Information Security Competence Maturity Model,” *Comput. Fraud Secur.*, vol. 2006, no. 5, pp. 11–15, 2006. Article (CrossRef Link)

[8] T. De Bruin, R. Freeze, U. Kaulkarni, and M. Rosemann, “Understanding the Main Phases of Developing a Maturity Assessment Model,” in *Proc. of Australas. Conf. Inf. Syst.*, pp. 8–19, November 29 - December 2, 2005. Article (CrossRef Link)

[9] B. Karabacak, S. O. Yildirim, and N. Baykal, “A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness,” *Int. J. Crit. Infrastruct. Prot.*, vol. 15, pp. 47–59, 2016. Article (CrossRef Link)

[10] ISA99 committee, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*, ISA, January, 2009. Article (CrossRef Link)

[11] M. M. Lessing, “Best practices show the way to Information Security Maturity,” in *Proc. of 6th Natl. Conf. Process Establ. Assess. Improv. Inf. Technol.*, pp. 1–9, September 17-19, 2008. Article (CrossRef Link)

[12] CMMI Team, *CMMI ® for Development*, Version 1 . 2, Software Engineering Institute, Pittsburgh, August, 2006. Article (CrossRef Link)

[13] H. Linstone, M. Turoff, *The Delphi method: Techniques and applications*. Addison-Wesley, 1975. Article (CrossRef Link)

[14] S. Yulianto, C. Lim, and B. Soewito, "Information security maturity model: A best practice driven approach to PCI DSS compliance," in *Proc. of 2016 IEEE Reg. 10 Symp. TENSYMP 2016*, pp. 65–70, May 9-10, 2016. Article (CrossRef Link)

[15] G. a Francia, D. Thornton, and J. Dawson, "Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems," in *Proc. of Int. Conf. on Security and Management. pp.1-7*, July 16-19, 2012. Article (CrossRef Link)

[16] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones and H. Soulsby, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, 2016. Article (CrossRef Link)

[17] J. Becker, R. Knackstedt, and J. Pöppelbuß, "Developing Maturity Models for IT Management," *Bus. Inf. Syst. Eng.*, vol. 1, no. 3, pp. 213–222, 2009. Article (CrossRef Link)

[18] J. D. Herbsleb, D. R. Goldensen, D. Zubrow, W. Hayes, and M. Paulk, "Software quality and the Capability Maturity Model," *Commun. ACM*, vol. 40, no. 6, pp. 30–40, 1997. Article (CrossRef Link)

[19] T. Takemura and A. Komatsu, "Who Sometimes Violates the Rule of the Organizations?: Empirical Study on Information Security Behaviors and Awareness," *WEIS*, pp. 1–21, 2012. Article (CrossRef Link)

[20] ISA99 committee, "Security for Industrial Automation and Control Systems Part 1 : Terminology, Concepts, and Models," *ISA*, October, 2007. Article (CrossRef Link)

[21] ISA99 committee, "Security for industrial automation and control systems. Part 3-3: System security requirements and security levels," *ISA*, Agust, 2013. Article (CrossRef Link)

[22]G. Dimić, N. D. Sidiropoulos, and R. Zhang, "Medium access control-physical cross-layer design," *IEEE Signal Process. Mag.*, vol. 21, no. 5, pp. 40–50, 2004. Article (CrossRef Link)

[23] E. Amankwa, M. Loock, and E. Kritzinger, "A conceptual analysis of information security education, information security training and information security awareness definitions," in *Proc. of 9th Int. Conf. Internet Technol. Secur. Trans.*, pp. 248–252, December 8-10, 2014. Article (CrossRef Link)

[24] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, 2012. Article (CrossRef Link)

[25] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006. Article (CrossRef Link)

[26] ISM3, *ISM3 Handbook*, ISM3 Consortium, 2007. Article (CrossRef Link)

[27] M. F. Saleh, "Information Security Maturity Model," *Int. J. Comput. Sci. Secur*, vol. 5, no. 3, pp. 316–337, 2011. Article (CrossRef Link)

[28] G. Karokola and Y. Louise, "Discussing E-Government Maturity Models for the Developing World-Security View," in *Proc. of SSA* 2009, pp. 81–98, August, 2009. Article (CrossRef Link)

[29] T. Yamada, "A politically feasible social security reform with a two-tier structure," *J. Jpn. Int. Econ*, vol. 25, no. 3, pp. 199–224, 2011. Article (CrossRef Link)

[30] D. L. Moody, "The Method Evaluation Model : A Theoretical Model for Validating Information Systems Design Methods," in *Proc. of ECIS 2003*, no. 79, 2003. Article (CrossRef Link)

[31] ISO/IEC JTC, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Requirements," *2nd Edition, ISO/IEC* 2013. Article (CrossRef Link)

[32] NIST SP 800 JTF, "Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations," *Revision 4, NIST*, 2014. Article (CrossRef Link)

[33] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security," *Revision 2, NIST*, 2015. Article (CrossRef Link)

[34] A. Segev, J. Porra, and M. Roldan, "Internet Security AND THE CASE OF BANK OF AMERICA," *Commun. ACM*, vol. 41, no. 10, pp. 81–87, 1998. Article (CrossRef Link)

Youngin You received M.S degree from Korea University. He is now a Ph.D student at the school of information security, Korea University. He is also a member of risk management laboratory in Korea University. His current research interests include Cloud security, Machine learning and Information security management.

Junhyoung Oh received B.S degree from Korea University. He is currently studying as an Unified Master's and Doctor's Course Students at Korea University. He is also a member of risk management laboratory in Korea University. His research interests include Usable security, Security Evaluation, Privacy in IoT.

Sooheon Kim received his B.S. in International Studies and Business from Korea University in 2017. His research interests include Natural Language processing, cyber security, and machine learning.

Kyungho Lee received his Ph.D degree from Korea University. He is now a professor in the school of information security at Korea University, and has been leading the risk management laboratory in Korea University since 2012. He was a former CISO at NAVER Corporation, and now he is serving as a president of Office of Information Technology & Service Center in Korea University.