Proposal and Evaluation of Method for Establishing Consensus on Combination of Measures Based on Cybersecurity Framework

Shota Fukushima and Ryoichi Sasaki
Tokyo Denki University
Tokyo Denki University, 5 Senjuasahicho, Adachi-ku, Tokyo 120-8551, JAPAN
16fmi27@ms.dendai.ac.jp and sasaki@im.dendai.ac.jp

ABSTRACT

Due to the development of our information society in recent years, the number of companies depending on IT systems has increased. However, it has been noticed that executives have not implemented sufficient information security measures, primarily due to the lack of consensus regarding information security between executives and IT administrators in enterprises. Numerous approaches to solving this problem have been formulated and applied. The Cybersecurity Framework developed by the US NIST is one approach. However, the Cybersecurity Framework does not have a function that can be used to enumerate and select an appropriate combination of rectifying measures based on mutual understanding between executives and administrators. Herein, by applying the Cybersecurity Framework and use cases of the framework provided by Intel Corporation, we propose a method that can enumerate measures and obtain an optimal combination of measures that could lead to mutual agreement between executives and administrators. In addition, we have developed a system called Risk Communicator for Tier (RC4T) to support the abovementioned function along with a method for its use. By applying this framework and RC4T to a small example, we were able to select a combination of measures suitable for obtaining mutual consensus between executives and administrators.

KEYWORDS

Cybersecurity Framework
Information security management
Information security governance
Risk management
Consensus building

1. INTRODUCTION

In recent years, incidents related to information security have been increasing. However, the awareness of companies involved in information security is insufficient [1]. One cause is the poor understanding of information security among executives such as chief information officers (CIOs), chief executive officers (CEOs) and information technology (IT) administrators (such as security managers) [1].

If understanding is poor, executives will not be reasonably aware of the organization’s information security state, and will be less likely to fund information security measures. As a result, the level of company-wide information security could be reduced because adequate information security measures for the entire organization are unlikely to be implemented.

Acknowledging that some executives have minimal technical knowledge, various methods that treat information security as a risk have been proposed [2]. One of these methods is the Cybersecurity Framework (CSF) proposed by the US National Institute of Standards and Technology (NIST) [3]. The CSF is a framework for information security management in which the current and target states of information security management are compared in order to express, comprehend, and manage risks associated with information security.

In general, it is assumed that executives are able to understand the current state of information security in an organization by comparing the current and target states. Therefore, CSF is intended to facilitate mutual understanding between executives and administrators. In addition, the usefulness of the CSF is expected to be confirmed by experimental results obtained by applying the CSF to actual issues, as was done by Intel Corporation [4]. However, it is still necessary to enumerate and select measures to fulfill the overall targets of an organization.

Because the CSF compares the current and target states, it is impossible to enumerate and select specific measures that will ensure the target is reached. By considering use cases for Intel Corporation, as well as other cases related to the CSF, we found a number of CSF implementation guidelines. However, those guidelines do not include a method for enumerating and selecting measures.

Accordingly, herein we propose a method for obtaining the optimal combination of measures that will lead to mutual understanding between executives and administrators. In addition, we report on the development a system named Risk Communicator for Tier (RC4T) that is designed to support the method. By applying this framework and RC4T to a small example, we were able to select the most appropriate combination of measures for obtaining mutual consensus between executives and administrators.

This paper describes the concise procedures used to formulate the problem for obtaining the optimal combination of measures as well as the content shown in our conference paper [5].

2. CSF OVERVIEW

The CSF is a framework that summarizes the risk management principles for the purpose of improving the cybersecurity of critical infrastructures. In addition, the CSF can be used to confirm in the gap between the current and target states, as well as the gap in the level of understanding between executives and administrators in a risk-based approach.

The CSF, which can be customized to fit needs of each organization, is composed of the following three elements:

(1) Framework core (hereinafter referred to as “core”)
(2) Framework implementation tiers (hereinafter referred to as “tiers”)
(3) Framework profile (hereinafter referred to as “profile”)

For more information about each element, refer to [3].

3. CSF USE CASE BY INTEL CORP.

Intel Corporation carried out a pilot project to verify the usefulness of the CSF.

3.1 Pilot Project Groups

The following three groups were formed in the pilot project:

(1) Core group
The core group, which consists of eight to 10 engineers with knowledge of advanced information security, has the authority to select and edit categories and to set targets. In this paper, the core group includes the chief information security officer (CISO).

(2) Individual security subject matter experts (SMEs)
The SMEs have the authority to evaluate the risks in their specialized area. In this paper, the SMEs are administrators.

(3) Stakeholders and decision makers
Stakeholders and decision makers have the authority to evaluate a target, review the evaluation result, and set the acceptable risk. In this paper, executives (except for the CISO) are the stakeholders and decision makers.

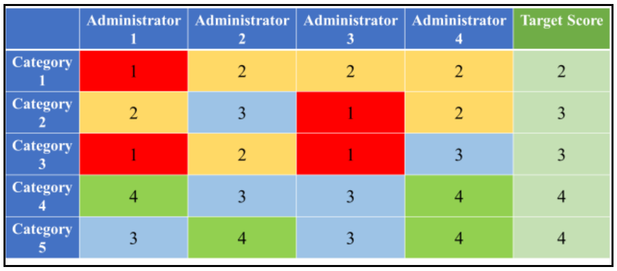
3.2 Pilot Project Policy

In the pilot project, subcategories were excluded for simplification and categories were enriched instead. In addition, specific definitions were set for each tier and listed in a table. Those definitions were then used as an index for evaluation by tier (Table 1).

Table 1. Tier definition examples (created according to [4])

Tier 1	Tier 2	Tier 3	Tier 4
The staff has a limited or nonexistent training pipeline.	The staff has a training pipeline.	Employees should receive regular cybersecurity-related training and briefings.	Employees receive regular cybersecurity-related training and briefings on relevant and emerging security topics.
Business decisions and prioritization are not factored into risk and threat assessments.	Risk-informed, management-approved processes and procedures are defined and implemented, and the staff has adequate resources to perform its cybersecurity duties.	Consistent risk management practices are formally approved and expressed as policy, and there is an organization-wide approach to manage cybersecurity risk.	The organization actively adapts to a changing cybersecurity landscape, evolving and sophisticated threats, predictive indicators, and lessons learned from previous events in a timely manner.

Moreover, an administrator evaluated the value of each tier to perform a risk assessment of each category. By comparing the current and the target states, a heat map was created by emphasizing the lower value of the tier with the color red (Fig. 1). The resulting heat map would be used as a profile in the pilot project.



	Administrator 1	Administrator 2	Administrator 3	Administrator 4	Target Score
Category 1	1	2	2	2	2
Category 2	2	3	1	2	3
Category 3	1	2	1	3	3
Category 4	4	3	3	4	4
Category 5	3	4	3	4	4

Figure 1. Heat map example (created according to [4])

3.3 Pilot Project Progress

The pilot project continued for seven months and followed the flow from (1) to (4) below by introducing the definitions of tiers and the heat map.

(1) The CISO sets the tier target for each category.
(2) The administrators evaluate the current state.
(3) The CISO and the administrators analyze the evaluation results.
(4) The CISO and the administrators communicate with executives using the analysis results.

4. RELATED WORK

Another example of a CSF application was reported at the University of Chicago [6]. They conducted a comparative study of current states and targets by inputting values of 0 to 4 derived from the International Organization for Standardization (ISO) 15504 standard in each category.

Related research conducted to obtain a consensus of measures with executives led to the development of a system called the Multiple Risk Communicator (MRC) [7]. This system outputs the optimal combination of measures by inputting the quantitative effect of each measure and the constraints as a cost and an objective function, respectively. With MRC, we can obtain the optimal combination of measures under the constraints set by the executives. Therefore, we find that the MRC is effective for building consensus to select measures.

5. PROPOSED METHOD TO ENUMERATE AND SELECT MEASURES

Since the CSF compares only the current and target states, a method that can be used to enumerate and select measures for evolving the current state to the target state is required.

While applications and discussions related to the CSF have been studied, we could not find any research that consider measures needed to approximate the current and target states.

In the MRC, building an information security consensus with the executives has been difficult due to an environment of insufficient mutual understanding between executives and administrators, primarily because MRC produced consensus requires executives who have sufficient knowledge of information security and sufficient time to deal with matters related to it [8].

5.1 RC4T Overview

The RC4T system, which was developed in Java 8, was designed to obtain the optimal combination of measures that leads to a mutual understanding between executives and administrators [9]. The program contains a total of about 2800 steps and prepares “inputting the current state tool” and “understanding the current state tool” steps.

“Inputting current state tool” is used to input the tier definition of the current state given by the administrator, while “Understanding the current state tool” is used by executives to gain an understanding of the current state based on the “inputting current state tool” data. In addition, administrators can evaluate measures by using this tool and watching the effect of the measures.

Furthermore, in this paper, we report on the development of an “optimizing combination of measures function” in “understanding the current state tool”. This function can be used to provide information references needed to select measures. The method for optimizing the combination of measures is described on Section 6.

5.2 Process for Using CSF between Executives and Administrators

Our proposed processes for using the CSF are shown in Fig. 2 [5]. The processes were proposed in order to enumerate measures and help select the optimal measure combinations required for obtaining mutual understanding between executives and administrators. The following steps show the descriptions of (1) to (8) in Fig. 2:

(1) The CISO is included in the core group input categories and tier definition in the RC4T for agreement with executives.

(2) Administrators input the current state of his/her related area into each category in the RC4T.

(3) The RC4T shows the current state to executives and the CISO in profile form.

(4) The executives and the CISO gain an understanding of the current state by examining the profile. In addition, they set the target of the tier in each category and show the total acceptable cost for measures.

(5) The CISO and administrators gain an understanding of the range of necessary measures by using the information received from the RC4T.

(6) The CISO and administrators then hold a meeting to enumerate and input the measures, their cost, and their effect into the RC4T, as shown in Fig. 3.

(7) The RC4T computes and shows the optimal combination of measures necessary to minimize the gap between the target and current states for executives and the CISO at an acceptable cost, as in the MRC. It is possible to provide the RC4T with a function to set measures that should always be adopted in the computation because executives might wish to select specific

measures to be adopted. The method used for optimizing the combination of measures is described in Section 6.

(8) If executives and the CISO are satisfied with the total cost and the state for carrying out measures, the combination of measures will be adopted and carried out. If the executives and the CISO are not satisfied, the process returns to Steps (5) and (6) in order to come up with a new acceptable cost and choose other categories to close the gap. In this way, executives can renew the risk communication cycle.

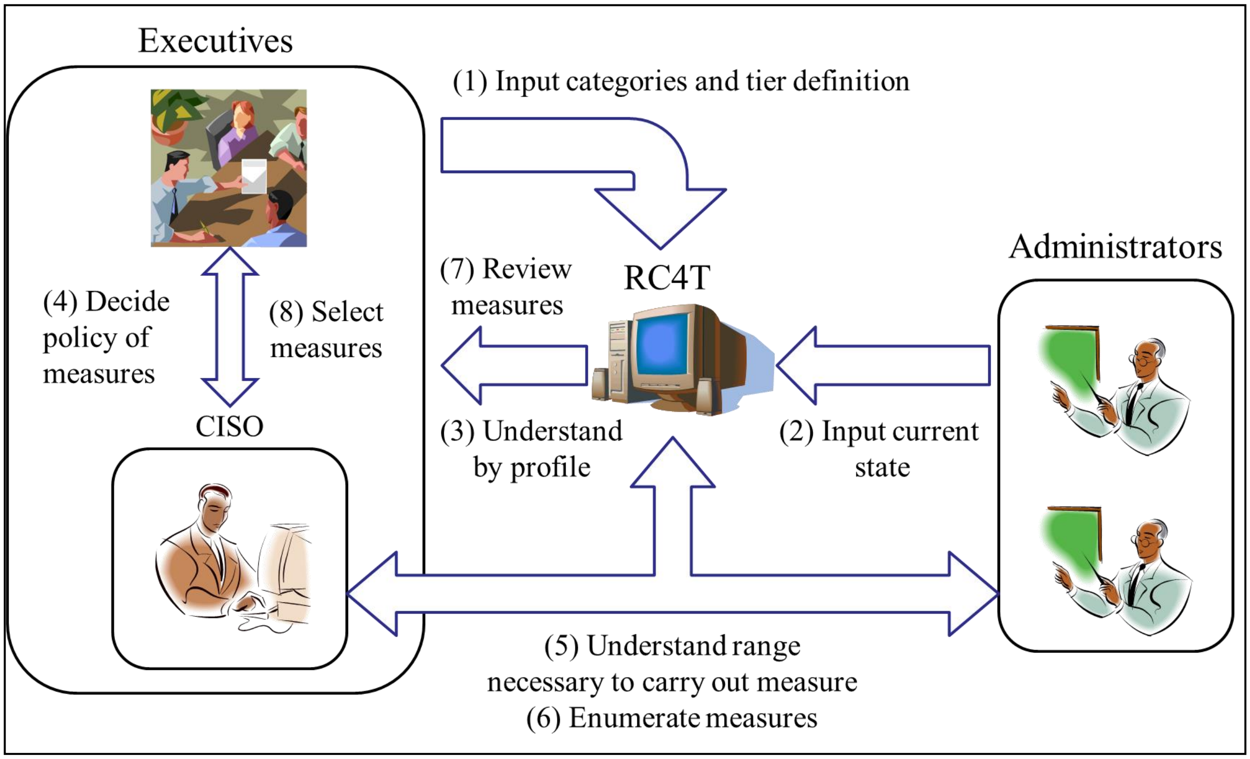

Executives
(1) Input categories and tier definition
Administrators
(7) Review measures
RC4T
(4) Decide policy of measures
(8) Select measures
CISO
(3) Understand by profile
(2) Input current state
(5) Understand range necessary to carry out measure
(6) Enumerate measures

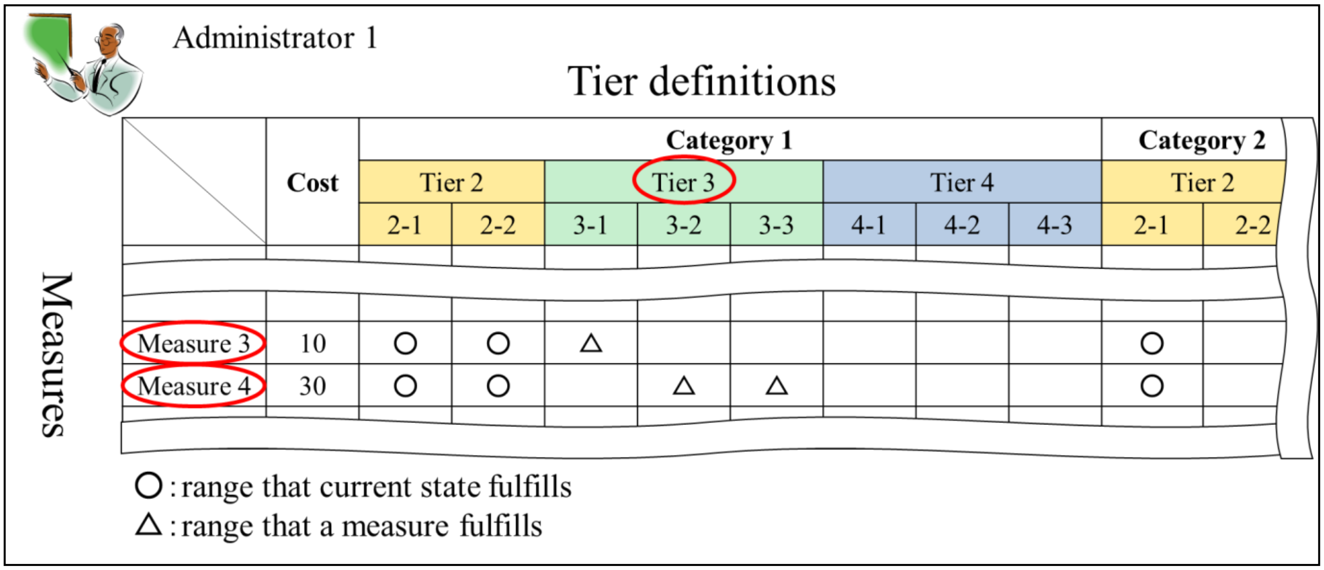
Figure 2. Process of using CSF for executives, the CISO and administrators

5.2 Method for Enumerating Measures

As previously explained, Tier 1 is a state that does not fit into any other tier. We also explained that each tier could only be fulfilled when all definitions of each preceding tier are satisfied. In addition, we set identification (ID) definitions for each tier (e.g., 2-1, 3-2). Given these definitions, we now propose a method to find the effects of measures as the "target administrators of measures," the "target categories of measures," and the "definition of tiers solved by measures" [9].

In the table of tier definitions and measures shown in Fig. 3, "○" is the range that the current state fulfills, and "△" is the range that a measure fulfills. We assume the effect of "Measure 3" is "Tier definition 3-1" of "Category 1" of "Administrator 1" and that the effect of "Measure 4" is "Tier definition 3-2, 3-3" of "Category 1" of "Administrator 1".

Then, "Category 1" of "Administrator 1" is raised to Tier 3 by fulfilling all the definitions of Tier 3 while carrying out "Measure 3" and "Measure 4". Consequently, we can optimize the combination of measures for minimizing the gap between the current and target states under the cost constraints.



	Cost	Category 1								Category 2	
		Tier 2		Tier 3			Tier 4			Tier 2	
		2-1	2-2	3-1	3-2	3-3	4-1	4-2	4-3	2-1	2-2
Measure 3	10	○	○	△						○	
Measure 4	30	○	○		△	△				○	

○ : range that current state fulfills
△ : range that a measure fulfills

Figure 3. Table of tier definitions and measures for Administrator 1

6. FORMULATION AND METHOD FOR OBTAINING OPTIMAL COMBINATION OF MEASURES

In this section, we provide a concise description of the procedure used to formulate the problem for obtaining the optimal combination of measures, which was not described in our conference paper [5]. This function, which is used in (7) and (8) in Fig. 2, takes advantage of the MRC knowhow described in Section 4.

6.1 Formulation for Obtaining Optimal Combination of Measures

Here, the “Optimizing combination of measures function” is intended for outputting the optimal combination of measures at the most acceptable cost in order to minimize the gap between the target and current states. In this paper, we show the objective function and constraints in the optimization problem in order to clarify the method.
The following function shows the objective function:

$$\min \sum_{a=1}^{Ja} \sum_{c=1}^{Jc} (T[c] - T'[a,c]) \qquad (1)$$

a: The a-th administrator.
Ja: The total number of administrators.
c: The c-th category.
Jc: Total number of categories.
T[c]: Target (tier) for the c-th category.
T’[a, c]: Tier of the a-th administrator and the c-th category after carrying out measures. (If this value exceeds T[c], it is set to T[c]).

The following formula is formulated for T’[a, c]:

$$T'[a,c] = \min(T[c], R[a,c]) \qquad (2)$$

R[a, c]: Tier of the a-th administrator and the c-th category after carrying out measures.

The following formula is formulated for R[a, c]:

$$R[a,c] = \sum_{t=2}^{4} R'[a,c,t] + 1 \qquad (3)$$

t: The t-th tier.
R’[a, c, t]: If the a-th administrator fulfills all definitions for the t-th and lower tiers in the c-th category after carrying out measures, this value is 1. In other cases, this value is 0.

The following formula is formulated for R’[a, c, t]:

$$R'[a,c,t] = \prod_{t'=2}^{t} R''[a,c,t'] \qquad (4)$$

t’: The t’-th tier.

R''[a, c, t']: If the a-th administrator fulfills all definitions for the t'-th tier in the c-th category after carrying out measures, this value is 1. In other cases, this value is 0.

The following formula is formulated for R''[a, c, t'].

$$R''[a,c,t'] = \prod_{d=1}^{Jd[t']} R'''[a,c,t',d] \qquad (5)$$

d: The d-th tier definition.
Jd[t']: The total number of definitions in the t'-th tier.
R'''[a, c, t', d]: If the a-th administrator fulfills the d-th definition for the t'-th tier in the c-th category after carrying out measures, this value is 1. In other cases, this value is 0.

The following formula is formulated for R'''[a, c, t', d].

$$R'''[a,c,t',d] = \begin{cases} 1 \; if \; L[a,c,t',d] \geq 1 \\ 0 \; if \; L[a,c,t',d] = 0 \end{cases} \qquad (6)$$

$$L[a,c,t',d] = CS[a,c,t',d] + M[a,c,t',d] \qquad (7)$$

CS[a, c, t', d]: If the a-th administrator fulfills the d-th definition for the t'-th tier in the c-th category in the current state, this value is 1. In other cases, this value is 0.
M[a, c, t',d]: If the selected measures can fulfill the d-th definition for the t'-th tier in the c-th category and the a-th administrator, this value is 1. In other cases, this value is 0.

In addition, the following formula is formulated for M[a, c, t', d].

$$M[a,c,t',d] = \begin{cases} 1 \; if \; M'[a,c,t',d] \geq 1 \\ 0 \; if \; M'[a,c,t',d] = 0 \end{cases} \qquad (8)$$

$$M'[a,c,t',d] = \sum_{m=1}^{Jm} (E[a,c,t',d,m] \times x[m]) \qquad (9)$$

m: The m-th measure.
Jm: The total number of measures.
E[a, c, t', d, m]: If the m-th measure can fulfill the d-th definition for the t'-th tier in the c-th category and a-th administrator, this value is 1. In other cases, this value is 0.
x[m]: if the m-th measure is selected, this value is 1. In other cases, this value is 0.

The following function shows the constraints.

$$\sum_{m=1}^{Jm} C[m] \times x[m] \leq Ct \qquad (10)$$

C[m]: The cost of the m-th measure.
Ct: The acceptable total cost.

6.2 Method for Obtaining Optimal Combination of Measures

To obtain the optimal combination of measures, RC4T uses a brute force approach. Here, the optimal combination of measures is the solution that minimizes the objective function expressed by Eq. (1) under constraints such as those in Eqs. (9) and (10), and selected from all combination of measures.

7. TRIAL APPLICATION

7.1 Trial Application Result

By using the processes shown in Fig. 2, we explained how executives could enumerate measures and obtain satisfactory measure combinations. A trial application was carried out in our laboratory in order to confirm this result.

In our trial, different work tasks necessary to maintain laboratory operations were assigned to the students. The leader of each task is called an administrator. Since, in our university, laboratory members are changed every year, it is also necessary to replace administrators yearly. However, replacement is not often successful due to the communication gap, so we decided to improve the administrator replacement system.

In this trial application, the lead author of this paper acted as the CISO, and the second author, who is a professor at the laboratory, acted as the executive.

Table 2 shows the administrators who participated in this trial application.

Table 2. Trial application administrators

Administrator ID	Administrator's name	Work
PLA	Planning administrator	Planning events and managing their costs.
PUB	Public relations administrator	Managing laboratory web pages.
CYB	Groupware administrator	Managing laboratory groupware.

The trial application was conducted as follows:

(a) The CISO decided the categories and tier definitions as shown in (1) of Fig. 2, and sets the tier target in each category. Tables 3 and 4 show the categories and the tier definitions that were finally decided upon.

Table 3. Trial application categories

Functions	Category ID	Category	Evaluation of executive	Target
Identify	ID.AM	Asset management	2	3
	ID.BE	Business environment	2	3
	ID.RA	Risk assessment	2	2
Protect	PR.AC	Access control	3	3
	PR.AT	Awareness / Training	3	4
	PR.DS	Data security	3	3
Respond	RS.IM	Improvement	2	3

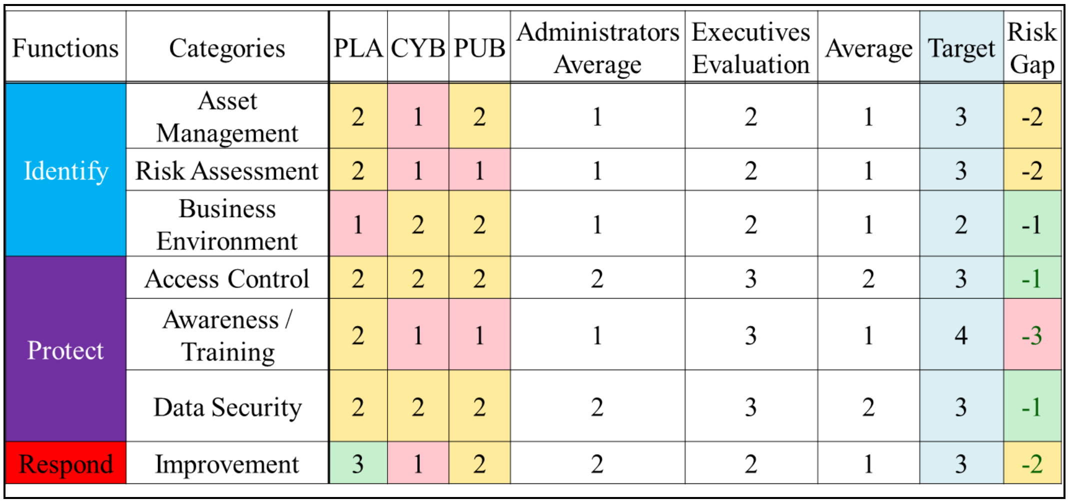
Table 4. Trial application tier definitions

Tier	Definition ID	Explanation of definition
2	2-1	We identified information about this category that should be given to the replacement student.
	2-2	We understand the risk and damage when this category is impaired.
3	3-1	Transition for this category was carried out smoothly and documented accurately.
	3-2	We have the knowledge, skills and assets needed to fulfill the responsibilities of this category.
	3-3	We defined policy to manage the risks of this category.
4	4-1	Our current organization can improve the replacement subject.
	4-2	We were self-motivated to learn and respond to this category.
	4-3	The risk management for this category is our laboratory policy.

The categories and tier definitions were then input into the RC4T by the CISO.

(b) The CISO then asked administrators to set the subjective tier value for the evaluations of each category, as shown in (2) of Fig. 2. Then, the tier definitions that are fulfilled in current state were input into the RC4T by the administrators. After this, RC4T calculated the tier value based on the inputted tier definitions.

(c) The inputted result was shown to the CISO and executives by using the RC4T, as shown in Fig. 1. This process is (3) in Fig. 2.



Functions	Categories	PLA	CYB	PUB	Administrators Average	Executives Evaluation	Average	Target	Risk Gap
Identify	Asset Management	2	1	2	1	2	1	3	-2
	Risk Assessment	2	1	1	1	2	1	3	-2
	Business Environment	1	2	2	1	2	1	2	-1
Protect	Access Control	2	2	2	2	3	2	3	-1
	Awareness / Training	2	1	1	1	3	1	4	-3
	Data Security	2	2	2	2	3	2	3	-1
Respond	Improvement	3	1	2	2	2	1	3	-2

Figure 4. Inputted result

(d) Based on the profile, the executives and the CISO could then gain an understanding of the current state, as shown in Fig. 4 and in (4) of Fig. 2. The executive then ordered the CISO and the administrators to enumerate the measures for the tiers that have gaps between the current and target states. The administrators were also directed to show an acceptable total cost for those measures. Here, the time required to execute the measure was used as the cost and a total time of 10 hours was given as a constraint.

(e) The CISO and the administrators enumerated the measures and estimated the cost and effect of improving the tier as shown in (5), (6), and (7) in Fig. 2. Here, after considering the risk gap between the current and target states, the CISO and the executives determined that the measures of “Awareness / Training,” ”Risk Assessment” and “Asset Management” should be carried out. In addition, the CISO and executives decided that the public relations administrator should carry out “Access Control” measure.

Tables 5 to 8 show details about the current state of “Awareness / Training,” ”Risk Assessment,” “Asset Management” and “Access Control”, where:

○: The range fulfilled by the current state.

×: The range the current state does not fulfill.

●: The range fulfilled by the current state that exceeds the target.

—: The range that the current state does not fulfill that exceeds the target.

Table 5. State of “Awareness / Training” before carrying out measures

	2-1	2-2	3-1	3-2	3-3	4-1	4-2	4-3
PLA	○	○	×	×	×	×	×	×
PUB	×	×	×	×	×	×	×	×
CYB	○	×	×	○	×	×	○	×

Table 6. State of “Risk Assessment” before carrying out measures

	2-1	2-2	3-1	3-2	3-3	4-1	4-2	4-3
PLA	○	○	○	○	×	—	—	—
PUB	×	×	×	×	×	—	—	—
CYB	×	○	×	○	×	—	●	—

Table 7. State of “Asset Management” before carrying out measures

	2-1	2-2	3-1	3-2	3-3	4-1	4-2	4-3
PLA	○	○	○	○	×	—	—	—
PUB	○	○	×	○	×	—	—	—
CYB	○	×	×	○	×	—	●	—

Table 8. State of “Access Control” before carrying out measures

	2-1	2-2	3-1	3-2	3-3	4-1	4-2	4-3
PLA	○	○	○	×	×	—	—	—
PUB	○	○	×	×	×	—	—	—
CYB	○	○	×	○	×	●	—	—

CISO and Administrators enumerated measures after reviewing the details about the current state shown in Tables 5 to 8. Table 9 shows the list of measures.

Table 9. List of measures

Measure ID	Measure name	Administrator ID	Category ID	Tier definition ID	Cost (hour)
M01	Organize information related to the takeover	PUB	PR.AT	2-1	0.5
M02	Short course for awareness of takeover	PUB CYB	PR.AT	2-2 3-1	1
M03	Short course for asset management	CYB	ID.AM	2-2 3-1	1
M04	Include information about risk assessment to information of the takeover.	PUB CYB	ID.RA	2-1 2-2 3-2	1
M05	Takeover information documentation	PLA PUB CYB	PR.AT ID.AM ID.RA	2-1 3-1	3
M06	Improve the takeover process in response to the risk	PLA PUB	PR.AT	3-2	1
M07	Include risk management in policy	PLA PUB CYB	PR.AT ID.AM ID.RA	3-3	0.5
M08	Meeting for dividing administrative account for public relations administrator	PUB	PR.AC	3-1 3-2 3-3	1
M09	Create processes takeover improvements	PLA PUB CYB	PR.AT	4-1	2
M10	Establish a system to perform regular knowledge confirmation	PLA CYB	PR.AT	4-2	2
M11	Make executive layer policies for takeover in the laboratory	PLA PUB CYB	PR.AT	3-3 4-3	3

RC4T computed the optimal combination of measures that minimized the gap between the current and target states under the cost constraint. The calculated result showed that the combination of M02 to M08 was optimal.

The executives who examined the result from the RC4T display ordered the CISO to implement the measures, as shown in (8) of Fig. 2.

7.2 Trial Application Considerations

Since we were able to obtain the combinations of measures that minimized the gap between the current and target states, we consider it proven that the proposed method and RC4T can be useful for easily performing risk communications related to the selection of measures between the executives and the CISO. More specifically, the executives and the administrators can easily obtain a consensus of measures through the CISO via the proposed process shown in Fig. 2.

In addition, in the organization requirement steps, we found that changing the requirements for categories and tier definitions is difficult. Thus, future challenges will include proposing a method that will allow easy changes to the categories and tier definition requirements.

8. CONCLUSIONS

In this paper, we proposed a method for enumerating measures and selecting optimal combination for reaching the target state of a tier. Moreover, we also formulated a method for optimizing the combination of measures, and developed a system called RC4T to support the method, and applied it to a small practical problem.

We found that by using the RC4T system, executives can determine the optimized combination of measures needed to close the gap between the current and target states at an acceptable cost. Accordingly, we confirmed that the proposed processes could assist in producing a consensus between executives and administrators related to measures.

In our future work, we intend to propose a method that will allow easy changes organization requirements to the categories and tier definition.

REFERENCES

1. Ministry of Economy, Trade and Industry, “Guidance for introduction of information security governance (in Japanese),” pp. 1--64 (2009).
2. K. Hayashi, “From the chief security to president security: Japanese-style management and information security (in Japanese),” Information Security Science, no.2, pp. 1--42 (2010).
3. National Institute of Standards and Technology (NIST), “Framework for Improving Critical Infrastructure Cybersecurity version 1.0,” pp. 1--43 (2014).
4. T. Casey, K. Fiftal, K. Landfield, J. Miller, D. Morgan, and B. Willis, “The Cybersecurity Framework in Action: An Intel Use Case,” Intel Corporation, pp. 1--10 (2015).
5. S. Fukushima, R. Sasaki, “,” The Third International Conference on Digital Security and Forensics (DigitalSec2016), pp. 27--34 (2016).
6. University of Chicago – Biological Sciences Division, G2 Inc. “Applying the Cybersecurity Framework at the University of Chicago ‐ An Education Case Study,” University of Chicago, pp. 1--5 (2016).
7. R. Sasaki, Y. Hidaka, T. Moriya, K. Taniyama, H. Yajima, K. Yaegashi, Y. Kawashima and H. Yoshiura, “Development and Applications of Multiple Risk Communicator,” Transactions of Information Processing Society of Japan, vol. 49, no. 9, pp. 3180--3190 (2008).
8. M. Taniyama, Y. Hidaka, M. Arai, S. Kai, H. Igawa, H. Yajima and R. Sasaki, “Application of "multiple risk communicator" to the personal information leakage problem in the enterprise,” Japan society of security management journal, vol. 23, no. 2, pp. 34--51 (2009).
9. S. Fukushima and R. Sasaki, “Proposal of the method for establishing the consensus on the measures based on Cybersecurity-Framework,” DICOMO 2016, pp. 1699--1704 (2016).