IRA-3MSS: Integrated Risk Assessment Method for Three Management System Standards in the Field of Information Technology Service

Noriaki Matsumura[1,a)] Takahiro Hasegawa[2]

Received: November 16, 2023, Accepted: March 15, 2024

Abstract: Three Management System Standards (MSS) published by the International Organization for Standardization (ISO) are applicable to organizations providing IT services: the MSS of Information Security, Service, and Business Continuity (3MSS). Operating 3MSS without integrating processes, including Risk Assessments (RA), may result in duplication of processes and inconsistency in assessment results. Although the ISO provides examples for integrating MSS requirements, it does not provide specifics on how to integrate RA, which are the core elements of MSS. Studies related to the integration of MSS have not yet revealed any methods for integrating RA. Here, we devise and present a method for integrating RA in 3MSS, called the Integrated Risk Assessment Method for Three Management System Standards (IRA-3MSS). The Business Impact Analysis (BIA), which is required by the Business Continuity Management System (BCMS) shows priorities of IT services to be followed. The IRA-3MSS incorporates those priorities as parameters into the integrated RA method for the Information Security Management System (ISMS), and the Service Management System (SMS). The case study results showed that the duplication of RA processes in 3MSS could be avoided using IRA-3MSS. Because IRA-3MSS also integrates the calculation of risk levels for assets and IT services through an established formula, inconsistency in assessment results did not occur. These results demonstrate the effectiveness of IRA-3MSS and provide a novel perspective for studies related to MSS integration.

Keywords: integrated risk assessment, ISMS, SMS, BCMS, BIA, relations

1. Introduction

Information technology (IT) has become a fundamental technology and is inherent in our society. Computer networks cover the world, and various IT services are provided. However, issues such as security incidents that threaten the stable provision of IT services are increasing. Therefore, IT services must be provided on the basis of appropriate risk management.

Both Technical and human efforts are needed to address issues related to the provision of IT services. One measure of the human efforts comes from the perspective of organizational management. Management System Standards (MSS) published by the International Organization for Standardization (ISO) include Information Security Management System (ISMS) [1], Service Management System (SMS) [2], and Business Continuity Management System (BCMS) [3].

ISMS is an MSS aimed at security management; Organizations manage controls needed to protect the confidentiality, integrity, and availability of assets including information from threats and vulnerabilities according to their information security policy. SMS is for effective management of services; Organizations need to agree on the Service Level Agreement (SLA) with customers, manage service quality, and report the status of service levels. SMS focuses on customer needs for IT services. BCMS aims to minimize negative impacts on services in preparation for business continuity risks. These MSS are relevant to organizations that provide IT services. Obtaining certification and operating these MSS will contribute to the stable provision of IT services through appropriate management.

Risk Assessments (RA) are the central components of ISMS, SMS, and BCMS (hereinafter referred to as 3MSS). In practice, conducting RA for each MSS individually may result in duplication of processes and inconsistency in assessment results. The ISO has published documents such as a handbook and guidance on the integration of MSS. Although the ISO provides examples for integrating the requirements of multiple MSS, it does not provide methods for integrating RA. Studies related to the integration of MSS have not revealed any methods for integrating

[1] Shinshu University, Matsumoto, Nagano 390–8621, Japan
[2] Shizuoka University, Hamamatsu, Shizuoka 432–8561, Japan
[a)] matsumura@shinshu-u.ac.jp

RA. Hence, the method for integrating RA in 3MSS is not yet clear. The challenge remains in developing effective, scientifically based methods to address duplication of processes and inconsistency in assessment results.

The authors have developed and reported on a method for integrating RA in ISMS and SMS [4], [5]. We hypothesized that by inputting the results of the Business Impact Analysis (BIA) required by BCMS into this method as parameters, RA in 3MSS would be integrated. In this study, we devise and propose a method for integrating RA in 3MSS, thereby avoiding the issues of process duplication and inconsistency in assessment results that occur when conducting RA individually. Our method is referred to as the Integrated Risk Assessment Method for Three Management System Standards (IRA-3MSS). The validity of IRA-3MSS is demonstrated in terms of meeting requirements, and its effectiveness is explained using values obtained from the operational records of ISMS and SMS.

The contributions of this study to the integration of RA are as follows:

– To devise a novel method for integrating RA in 3MSS. The results are then output as numerical values.
– To provide a scientific rationale for the integration method of RA in 3MSS.
– To present an effective method for operating RA in 3MSS.

Section 2 describes related studies on the integration of MSS; Section 3 describes IRA-3MSS, which includes BIA results as parameters of the RA integration method in ISMS and SMS; Section 4 shows the results of applying IRA-3MSS using values obtained from the operational records of ISMS and SMS; and Section 5 analyzes the results and discusses the validity and effectiveness of IRA-3MSS. The results are summarized in Section 6.

2. Related Studies

The survey results of documents and studies related to the integration of RA in 3MSS are summarized to clarify the position of this study.

The ISO published "The Integrated Use of Management System Standards (IUMSS)" [6] in relation to the integration of MSS. The IUMSS shows a process for unifying the requirements of multiple MSS and provides an example of a bakery integrating its quality, environmental, and food safety management systems. Regarding the integration of ISMS and SMS, "ISO/IEC 27013 Information Security, Cybersecurity and Privacy Protection - Guidance for integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1" has been published [7]. Here, common risk management, including RA, is indicated as an approach that should be adopted in ISMS and SMS to avoid duplication of processes. However, these ISO documents did not devise methods for integrating RA in 3MSS.

Boehmer examined the applicability of the Discrete Event System (DES) theory to 3MSS, explaining that 3MSS can be expressed using DES theory and that control loops can be considered equivalent to the behaviors of Management Systems (MS) [8]. The loop equations expressing 3MSS were analyzed in combination with the coupling parameters between MS, and it was concluded that there should be a strong coupling between ISMS and SMS, whereas a weak coupling is ideal between ISMS and BCMS. Boehmer pointed out that 3MSS can be coupled through risk analysis. However, there was no indication of how to integrate RA in 3MSS.

Białas proposed the Integrated Security Platform (ISP), a model that describes the processes of ISP and 3MSS in Unified Modeling Language (UML) and integrates 3MSS as subsystems of ISP [9]. The focus was on introducing concepts such as expressing the relations between processes in 3MSS and the relations between ISP and subsystems in UML. The integration of RA was not mentioned in this paper.

Kawaguchi reported the integration of RA in multiple MSS [10]. This study started with the same awareness of issues as the authors, such as duplication of RA processes and inconsistency in RA results in the operation of multiple MSS. The commonality rate among RA requirements in multiple MSS was analyzed using text mining and 0-1 integer planning, and ISMS and BCMS were found to have a satisfactory commonality rate. His study analyzed and evaluated the commonality among RA requirements in multiple MSS, which was useful but did not present a method for RA integration. In this respect, it differs from our study.

Domingues et al. reported the survey results of existing studies related to the integration of MSS [11]. Existing studies have indicated the motivations for integration, the disadvantages and advantages of integration, the strategies and models adopted, and the level of integration achieved. However, the survey results did not indicate integration methods for RA in 3MSS.

Other studies have indicated that risk management is fundamental to MSS [12], [13].

As far as the authors have been able to ascertain from documents and studies related to RA integration in 3MSS, although documents and studies related to the integration of 3MSS have been published, no documents and studies on RA integration methods were available. Therefore, in this study, we propose a method for integrating RA in 3MSS based on scientific rationale. Boehmer pointed out that 3MSS can be combined through risk analysis. Based on this knowledge, we hypothesize that RA in 3MSS can be integrated by inputting the results of the BIA re-

quired by BCMS as a parameter in the method of integrating RA in ISMS and SMS [4], [5] devised by the authors. IRA-3MSS is pioneering in the field of 3MSS integration, which proposes a novel method for integrating RA and contributes to the integration of 3MSS.

3. Method

3.1 Assumptions

The proposed method assumes the following:

– The proposed method targets organizations that provide IT services.
– Assets within the scope of ISMS shall provide IT services.
– When conducting RA for assets within the scope of ISMS, incorporate the perspective of RA in SMS and BCMS intended for IT services related to assets.
– These three parameters of the proposed method are regularly reviewed during the operational process of MSS in each organization to improve its accuracy:
  (1)Strength of the relations between assets and IT services
  (2)Values of risk criteria in RA
  (3)Priority of each IT service

3.2 IRA-3MSS

IRA-3MSS integrates RA in 3MSS in the following steps. IRA-3MSS was developed on the basis of our previous studies [4], [5].

Step 1: Define the Relations.

Identify assets and IT services within the scope of 3MSS and define the relations between them. An asset is anything that has value for the organization. Business processes, information, hardware, software, personnel, and organizational structures can also be assets.

To explain the proposed method, let assets be a_i (i = 1, ⋯, n), IT services be s_j (j = 1, ⋯, m), and risks be r_{ik} (i = 1, ⋯, n; k = 1, ⋯, ℓ), where n is the number of assets, m is the number of IT services, and ℓ is the number of risks related to asset a_i. Assume that an organization owns a set of assets A and provides IT services S within the scope. Let A and S be

$$A = \{a_1,\ a_2,\ \ldots,\ a_n\}, \tag{1}$$

$$S = \{s_1,\ s_2,\ \ldots,\ s_m\}. \tag{2}$$

Let us define the relations between sets A and S. Set L denotes the relations between sets A and S. Set L is shown in **Fig. 1**, and can be expressed as follows:

$$L = \left\{ \begin{array}{l} (a_1, s_1), (a_1, s_2), (a_2, s_2) \ldots, \\ (a_i, s_j), \ldots, (a_n, s_m) \end{array} \right\}. \tag{3}$$

Step 2: Conduct BIA.

BCMS requires organizations to conduct BIA and RA. Organizations must use BIA to prioritize business continuity. Business continuity refers to an organization's ability to continue providing products or services at a predefined acceptable level after an incident. In this study, business refers to IT services, and business continuity refers to an organization's ability to continue providing IT services. The details of BIA are left to ISO documents and other manuals, but in general, BIA stipulates the following:

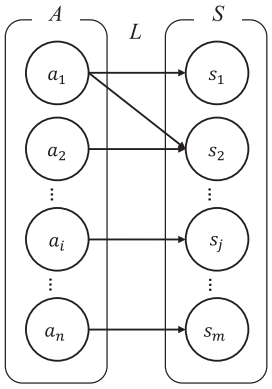

Fig. 1 Relation L between sets A and S.

– Prioritized business (IT services in this study)
– Maximum Tolerable Period of Disruption (MTPD)
– Recovery Time Objective (RTO)
– Identified resources needed for the prioritized business (IT Services)

In this study, it is assumed that each IT service is analyzed using multiple items by conducting BIA, and the priority β_j (j = 1, ..., m) of IT service s_j is expressed numerically.

Step 3: Conduct RA.

Conduct RA for assets within the scope of 3MSS, incorporating the perspective of RA in SMS and BCMS intended for IT services related to assets. In other words, RA for assets within the scope of ISMS shall include the perspectives of service availability (SMS) and service continuity after an incident (BCMS). By conducting RA, the risk level of risk r_{ik} is determined numerically. Let the set of risks r_{ik} identified for the set of assets A be R, and let the relations between sets R and A be denoted by set L'. This is illustrated in **Fig. 2**. Here, the following equation express L' in Fig. 2:

$$L' = \left\{ \begin{array}{l} (r_{1k}, a_1), (r_{2k}, a_2), (r_{i1}, a_i), (r_{i2}, a_i), \\ \ldots, (r_{ik}, a_i), \ldots, (r_{i\ell}, a_i), \ldots, (r_{nk}, a_n) \end{array} \right\}. \tag{4}$$

The composition of relations L' and L, $L' \circ L$ is then obtained. The composition of relations $L' \circ L$ in Fig. 2 is denoted as follows:

$$L' \circ L = \left\{ \begin{array}{l} (r_{1k}, s_1), (r_{1k}, s_2), (r_{2k}, s_2), \\ \ldots, (r_{ik}, s_j), \ldots, (r_{nk}, s_m) \end{array} \right\}. \tag{5}$$

Therefore, risks r_{ik} are determined to be the risks of IT services s_j related to assets a_i.

In a real society, IT services s_j are related to multiple risks.

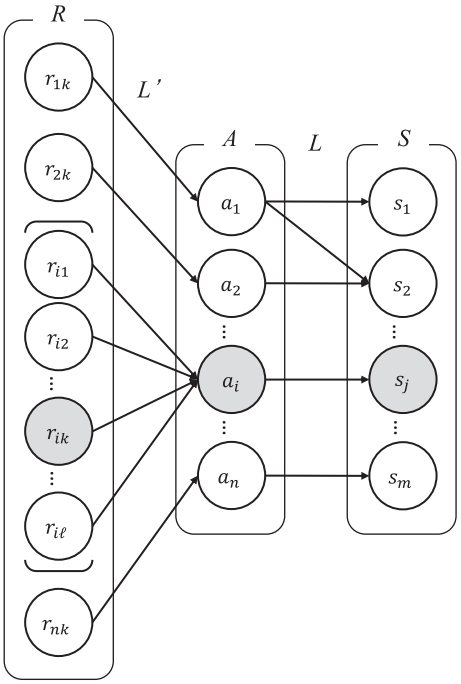

Fig. 2 Set *R* of risks identified for set *A*.

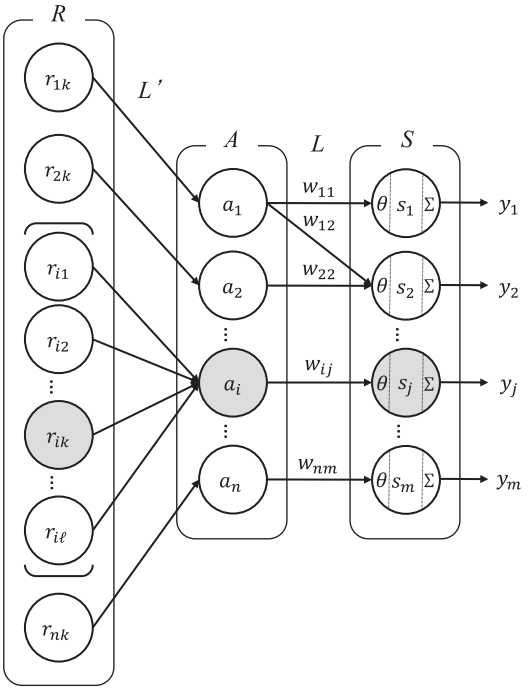

Fig. 3 Risk calculation for IT services s_j in the integrated risk assessment.

Let y_j be the entire risk of IT services s_j, which is the sum of the risks r_{ik} related to IT services s_j. In addition, the authors considered the following two points when calculating y_j:

(1)Strength of the relations between assets and IT services

(2)Values of risk criteria in RA

The method used by the authors is shown in **Fig. 3**. Let (1) Strength of the relations between assets and IT services be w_{ij}, and (2) Values of risk criteria in RA be θ.

To calculate the entire risk y_j of IT service s_j, it is first necessary to calculate each risk related to IT service s_j. Let x_{jh} ($j = 1, ..., m$; $h = 1, ..., p$) be each risk related to s_j, where m is the number of IT services and p is the number of risks related to IT service s_j. By conducting RA, the risk level of risks r_{ik} related to assets a_i is determined numerically. Because there may be variations in the strength of the relations between assets a_i and IT services s_j, multiply r_{ik} by w_{ij} to obtain x_{jh}. The equation for x_{jh} is

$$x_{jh} = w_{ij} r_{ik}. \tag{6}$$

The RA specified in the ISO standards compares and evaluates the risk levels using pre-established risk criteria. Therefore, in our integration method, only x_{jh} that exceeds the risk criteria is summed to obtain the entire risk y_j of IT service s_j. The following equations express this procedure

$$y_j = \sum_{h=1}^{p} x_{jh} C_h, \tag{7}$$

$$C_h = \begin{cases} 0, & x_{jh} \le \theta \\ 1, & x_{jh} > \theta, \end{cases} \tag{8}$$

where C_h represents the result of comparing x_{jh} and θ, and when

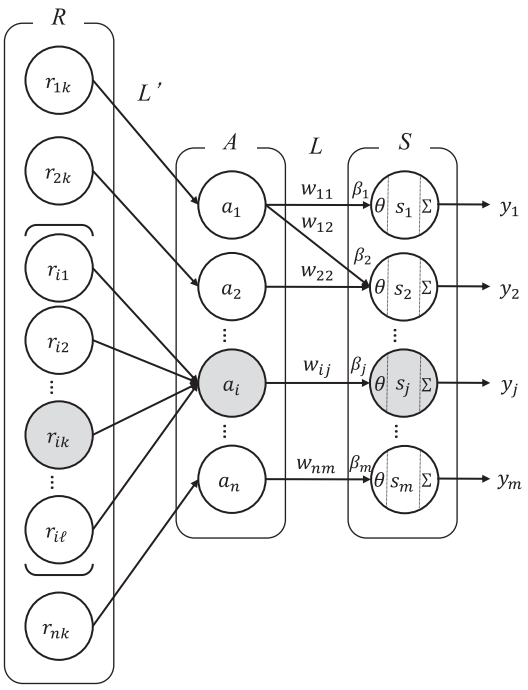

Fig. 4 Risk calculation for IT services s_j in the integrated risk assessment with business impact.

C_h is 1, it indicates that x_{jh} exceeds the risk criterion. The IT service s_j with the highest value of y_j should be treated with the highest priority, and the order of priority is determined by the descending order of y_j. If $y_j = 0$, it can be determined that the risk is tolerable and that no risk treatment is necessary.

Add the priority β_j of each IT service s_j obtained in Step 2 to this RA integration method. Consequently, the priority of IT ser-

vice s_j, which is determined from the business continuity perspective, is also integrated into the RA. This procedure is expressed in **Fig. 4**, Eqs. (9) and (10).

$$y_j = \sum_{h=1}^{p} \beta_j x_{jh} C_h, \tag{9}$$

$$C_h = \begin{cases} 0, & \beta_j x_{jh} \leq \theta \\ 1, & \beta_j x_{jh} > \theta. \end{cases} \tag{10}$$

4. Results

IRA-3MSS was applied to the operational records of our case study which has reported the integration method of RA in ISMS and SMS [5]. The results of applying IRA-3MSS to two IT services, "Mail" and "Global IP address", are shown in this section. In our previous case study, (1) Strength of the relations w_{ij} between assets a_i and IT services s_j and (2) Value θ of risk criteria in RA were set as follows:

(1)Strength of the relations between assets and IT services

1) Normal relation w_{ij}=1
2) Strong relation w_{ij}=1.2

(2)Values of risk criteria in RA

1) Risk regarding Confidentiality θ=24
2) Risk regarding Integrity θ=24
3) Risk regarding Availability θ=16

The strength of the relations w_{ij} between assets a_i and IT services s_j was set to 1 for a "Normal relation" and 1.2 for a "Strong relation," where the SLA of the related IT service cannot be satisfied if there is a problem with an asset. The strength of the relations w_{ij} between assets a_i and IT services s_j depends on the organizational context and was defined in two levels by the MSS administrator for the sake of simplicity and reproductivity from a practical point of view. Reproductivity is intended as a constraint to ensure that there are no significant differences in risk assessment even if the risk assessment is performed by a different person, and the strength of the relation is defined as "Normal" or "All those evaluated to be greater than normal". Ultimately, it is up to the discretion of the MSS administrator to decide how much weight to place on "All those evaluated to be greater than normal". In this paper, we have adopted 1.2, and determined that this value does not conflict with "All those evaluated to be greater than normal". If the MSS administrator decides that this value is not optimal during the PDCA (Plan-Do-Check-Act) cycle of MSS, it is possible to change the weight and reevaluate or simulate the risk of the organization. The proposed method works effectively by treating weights as important risk control parameters that are equal to risk criteria of the organization.

The value θ of risk criteria in RA was set to 24 for "risk regarding confidentiality and/or integrity" and 16 when "availability is at risk". The risk criteria (θ) should be referred to the external and internal context of the organization as well. The risk criteria (θ) in previous case study were based on the MSS integration manual of the university, which was the target organization of the adapted case study. Availability was emphasized in particular because of the public nature of the university and its obligations to society through continuity of research and education. Consequently, the availability criterion was set 30% higher than confidentiality and integrity.

Tables 1 and **Table 2** show the assets a_i related to IT services s_j, the strength of the relations w_{ij} between them, and the number of risks r_{ik} related to asset a_i. For security reasons, the details of the assets and risks are not described, instead, they are written as "Asset 1", "Risk 1", etc. Table 1 shows the assets related to the IT service "Mail," the strength of the relations w_{ij} between them, and the number of risks related to the assets. In Table 1, the nine grouped assets are related to the Mail service. The table indicates the value of w_{ij} and the number of risks related to each asset. Similarly, Table 2 shows information about the assets and risks related to the "Global IP address" service.

Here, Asset 1 and 9 in Table 2 represent the same assets as Asset 1 and 9 in Table 1. This indicates the overlap of assets comprising Mail and Global IP address service. IRA-3MSS conducts RA for assets. The results of RA are then multiplied by the Strength of the relations w_{ij} between assets and IT services and the priority β_j of each IT service obtained by BIA. Therefore, even if an asset is related to multiple IT services, the results of RA for IT services will not affect each other because the parameters w_{ij} and β_j can be varied depending on the context of organi-

Table 1 Assets and risks related to Mail service.

	w_{ij}	Number of Risks
Asset 1	1	4
Asset 2	1	3
Asset 3	1	3
Asset 4	1.2	4
Asset 5	1.2	3
Asset 6	1	3
Asset 7	1.2	3
Asset 8	1.2	2
Asset 9	1	5

Table 2 Assets and risks related to Global IP address service.

	w_{ij}	Number of Risks
Asset 10	1.2	4
Asset 1	1.2	4
Asset 11	1	3
Asset 9	1	5

zations in this method.

Priority β_j of each IT service s_j in IRA-3MSS was assigned a value between 1 and 2 based on the total evaluation score of IT service s_j in BIA.

BCMS requirements include the following:

8.2.2 Business impact analysis

f) use this analysis to identify prioritized activities;

It is required to use BIA to identify the prioritized activities (IT services in this study). However, the requirements do not describe a method for calculating priority. Neither does ISO/IEC 31010:2019, which describes risk assessment techniques that include BIA, prescribe such a method [14]. Therefore, in this case, the authors decided to use following calculation method for the sake of simplicity from a practical point of view.

(3)Priority β_j of each IT service s_j

1) Set the base value of each IT service s_j as 1.
2) With the total weights as 1, calculate the weight of each IT service s_j according to the BIA evaluation score.
3) Add the weight in 2) to the base value of 1 for each IT service s_j and make the result the priority β_j of each IT service s_j.

Priority β_j was obtained using the following equation:

$$\beta_j = 1 + \frac{impact_j}{\sum_1^m impact_j}, \tag{11}$$

where $impact_j$ represents the total evaluation score of each IT service s_j in the BIA. **Table 3** shows the results of calculating the priority β_j of "Mail" and "Global IP address" using Eq. (11). I to V represent the analysis items of business impact and are analyzed on a five-level scale from 1 to 5, and priority β_j is determined.

Here, it is important to note that the result of Eq. (11) affects the result of Eqs. (9) and (10). This is because β_j is an input parameter to Eqs. (9) and (10). Thus, if necessary, adjustments with risk criteria θ are required. Generally, as organizations operate MSS, the parameters, β_j and θ, become more reliable or modified to appropriate values.

The procedure for calculating risk levels to IT services utilizing IRA-3MSS is presented. **Fig. 5** shows the results of applying IRA-3MSS to Asset 1 of Mail service. As shown in Table 1, four risks are related to Asset 1. These risk levels are 32 for Risk1, 4 for Risk2, and 3 for Risk3 and 4, as shown in **Table A·1** in Appendix A.

Table 3 Calculation results of priority β_j for IT services.

IT Service	Impact Analysis I	II	III	IV	V	β_j
Mail	5	5	5	3	4	1.55
Global IP address	3	3	5	3	4	1.45

To calculate the entire risk of IT service, the risk levels of each risk x_{jh} related to IT services are needed to calculate using Eq. (6). Multiply the risk levels of Risk 1 to 4 by the strength of the relations w_{ij} between Asset 1 and Mail service. In addition, multiply priority β_j determined by Eq. (11). Then, the risk levels of each risk are calculated as follows (Table A·1 in Appendix A):

– Risk 1: 32*1*1.55 = 49.6
– Risk 2: 4*1*1.55 = 6.2
– Risk 3: 3*1*1.55 = 4.65
– Risk 4: 3*1*1.55 = 4.65

Compare these values with the risk criteria θ. As mentioned above, the risk criterion θ is 24 for risks regarding confidentiality and integrity and 16 for risks regarding availability. Risk 1 is a risk regarding availability, and exceeds the risk criterion θ. Hence, add the risk level to the entire risk y_j of Mail service. The risks other than Risk 1 did not exceed the criteria θ. This procedure is expressed in Fig. 4, Eqs. (9) and (10) in section 3. In Fig. 5, the entire risk y_j for Mail service is denoted as y_{mail}, and Global IP address service as y_{gip}.

The same procedure is followed for all other risks. Tables A·1 to A·13 in Appendix A show the results of applying IRA-3MSS to the case study in our study [5] and calculating the risk levels of all risks for Mail and Global IP address services. Risks with a highlighted result column indicate that they exceed risk criterion θ. In the table, "CIA" represents the risk attribute, where C rep-

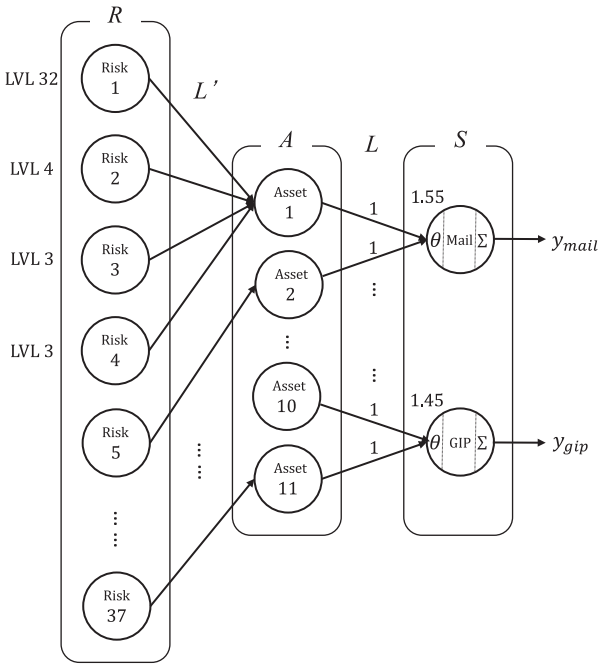

Fig. 5 Risk calculations for Asset1 of the Mail service utilizing IRA-3MSS.

resents the risk regarding confidentiality, I represents the risk regarding integrity, and A represents the risk regarding availability. From the results in Tables A·1 to A·13 in Appendix A, and eliminating those which do not exceed the risk criterion, as indicated in Eqs. (9) and (10), the entire risks y_j of the IT service Mail and Global IP address are determined as follows:

(4)The entire risk y_j of IT services s_j.

1) Mail y_j=166.16
2) Global IP address y_j=100.92

5. Discussion

The validity of the IRA-3MSS is demonstrated from the perspective of meeting the 3MSS requirements. In addition, the effectiveness of IRA-3MSS for the issues described in Section 1 is discussed.

5.1 Meeting the Requirements

RA comprises three processes: risk identification, risk analysis, and risk evaluation. The requirements for RA in 3MSS are as follows:

ISMS（ISO/IEC 27001:2022）：

6.1.2 Information security risk assessment

c) identifies the information security risks:
  1) apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and
  2) identify the risk owners;
d) analyses the information security risks:
  1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;
  2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2 c) 1); and
  3) determine the levels of risk;
e) evaluates the information security risks:
  1) compare the results of risk analysis with the risk criteria established in 6.1.2 a); and
  2) prioritize the analyzed risks for risk treatment.

SMS（ISO/IEC 20000-1:2018）：

6.1 Actions to address risks and opportunities

6.1.2 The organization shall determine and document:

a) risks related to:
  1) the organization;
  2) not meeting the service requirements;
  3) the involvement of other parties in the service lifecycle;
b) the impact on customers of risks and opportunities for the SMS and the services;
c) risk acceptance criteria;
d) approach to be taken for the management of risks.

6.1.3 The organization shall plan:

a) actions to address these risks and opportunities and their priorities;
b) how to:
  1) integrate and implement the actions into its SMS processes;
  2) evaluate the effectiveness of these actions.

BCMS（ISO 22301:2019）：

8.2.3 Risk assessment

The organization shall:

a) identify the risks of disruption to the organization's prioritized activities and to their required resources;
b) analyze and evaluate the identified risks;
c) determine which risks require treatment.

As mentioned in Section 3, IRA-3MSS conducts RA on assets within the scope of ISMS. An asset is anything that has value for the organization. Business processes, information, hardware, software, personnel, and organizational structures can also be assets. The form of information does not matter; it may be paper or electronic. Resources used to hold and handle information, such as data cables, can also be assets. IRA-3MSS conducts RA on these assets within the scope of ISMS. Thus, RA for information and information-related assets is conducted and can be concluded to meet ISMS requirements.

In IRA-3MSS, the relations between assets and IT services are defined in Step 1 before conducting RA in Step 3. Therefore, when conducting RA for assets, IT services related to assets are already clear. Asset is anything that has value for the organization and can include other parties and SLA. In addition, because IRA-3MSS includes the perspective of service availability (SMS) in RA for assets, it can be concluded that IRA-3MSS meets the SMS requirements. Note that the guidance for the integrated implementation of ISMS and SMS states that the risk classification shown in SMS requirement 6.1.2 a) can also be used as a classification of information security risks when implementing ISMS [7].

In IRA-3MSS, the relations between assets and IT services are defined in Step 1, and the BIA is conducted in Step 2 from the perspective of business continuity. In other words, the organization's prioritized activities (IT services in this study) and their required resources (assets in this study) are clear, and RA is conducted for them. Furthermore, because the RA for assets includes the perspective of service continuity after an incident (BCMS), IRA-3MSS meets the requirements of BCMS. Here, the perspective of service continuity (BCMS) includes the risk of restoring interrupted IT services. For example, if the cause of interruption of IT services is a cyber-attack, measures such as

blocking access to the IT services or preserving evidence would have priority even over restoration, to prevent the spread of damage caused by the attack. The same is true in case where cyber-attack is persistently conducted until the objective is achieved. In BCMS, the BIA is conducted to determine the prioritized activities (IT services in this study), the maximum tolerable period of disruption (MTPD), the recovery time objective (RTO), and required resources for the prioritized activities (assets in this study). Next, RA identifies, analyses, and evaluates the risks that hinder the recovery goals of the IT services not only from the preventive and detective perspective, but also from the corrective perspective. IRA-3MSS assumes that this perspective is also incorporated. Therefore, IRA-3MSS also covers risk of restoring interrupted IT services.

5.2 Evaluation of Effectiveness

The effectiveness of IRA-3MSS in addressing the issues described in Section 1 is evaluated.

When RA is conducted individually without integrating 3MSS, there are possibilities for duplication of processes and inconsistency in assessment results. Here, we discuss whether these issues can be avoided by applying IRA-3MSS.

First, we consider the duplication of processes.

When RA is conducted individually without integrating 3MSS, duplication of processes occurs. ISO 31000 defines RA as the entire process of risk identification, analysis, and evaluation. The process diagram for conducting RA individually without integrating 3MSS is shown in **Fig. 6**, and the processes are duplicated.

ISMS requires RA for information and information-related assets, whereas SMS requires RA for IT services. BCMS requires RA for the organization's priority business activities (IT services in this study) and the resources required for those activities. Therefore, duplications occur in the processes of risk identification, analysis, and evaluation of assets or IT services.

In IRA-3MSS, assets and IT services within the scope of 3MSS are identified, and the relations between them are defined in Step 1. Then, in step 3, RA is conducted for assets within the scope of 3MSS, incorporating the perspective of RA in SMS and BCMS intended for IT services related to assets. Consequently, the RA process is completed once without duplication. A process diagram of RA in the case of 3MSS integration is shown in **Fig. 7**.

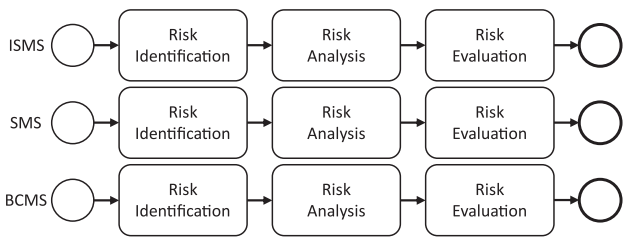

Fig. 6 Process diagram for individual risk assessment.

By avoiding the duplication of processes, IRA-3MSS can also be expected to reduce the number of documents related to RA. In other words, IRA-3MSS can consolidate RA-related documents that were created and managed in each MSS into one, whereas each MSS has strong documentation requirements. This contributes to the integration of the 3MSS.

Here, we consider whether duplication of processes could be avoided because of applying IRA-3MSS in our case study. Section 4 presented the results of applying IRA-3MSS to ISMS and SMS operational records in the case study [5]. **Fig. 8** shows the area covered by 3MSS. ISMS is an MS that balances the confidentiality, integrity, and availability of information and information-related assets. It is common for ISMS to focus on confidentiality, availability, or integrity according to the information security policies of organizations. SMS emphasizes the availability of IT services. However, this does not mean that confidentiality or integrity are not considered. BCMS focuses only on availability from the perspective of business continuity. In our case study, perspective of service availability (SMS) was emphasized because RA was integrated by applying SMS as well as ISMS. Therefore, as mentioned in Section 4, the risk criterion θ was set at 16 for availability, which is a 30% reinforcement value, whereas confidentiality and integrity were set at 24. Appendix A of the ISMS describes a control for business continuity. Since this control was applied in the case study, RA has already been implemented from the perspective of business continuity. Therefore, in the case study presented in Section 4, no new risks were identified because of the application of IRA-3MSS, and there was no increase in the workload for RA process. The actual RA process was shown in Fig. 7; there was no duplication in the RA process. Hence, it can be concluded that the application of

Fig. 7 Process diagram for the integrated risk assessment.

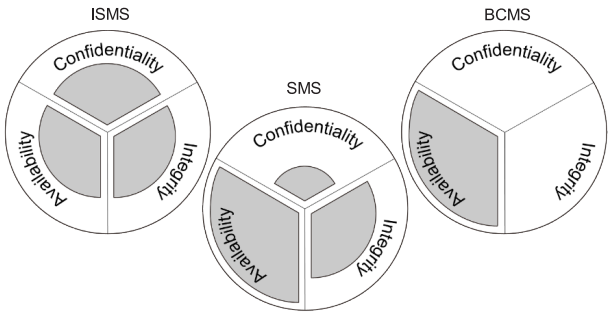

Fig. 8 3MSS coverage area [17].

IRA-3MSS is effective in avoiding the duplication of RA.

It is important to note that workload may increase in some cases because RA depends on the internal and external conditions of the organization. However, even if new risks are identified as a result of applying IRA-3MSS, this means an increase in the number of risks detected and the associated workload, not a duplication of processes, because there is no need to conduct the RA process more than once.

Documents published by the ISO support the development of integrated methods such as IRA-3MSS, which avoid duplication of processes. To begin with, ISO published "Appendix 2 Harmonized structure for MSS with guidance for use" in Annex SL of "ISO/IEC Directives, Part 1 - Procedures for the technical work - Consolidated ISO Supplement - Procedures specific to ISO" [15], and continued efforts to standardize the core elements of MSS and improve consistency among MSS by defining common structures and terminology. The 3MSS that are subjects of this study are all based on Annex SL. In addition, 3MSS refer to ISO 31000, Risk management-Guidelines [16], and incorporate common RA processes described in ISO 31000. Furthermore, as mentioned in Section 2, common risk management, including RA, is one of the approaches to be adopted in ISMS and SMS to avoid the duplication of processes in Ref. [7]. Therefore, even though there are differences in RA perspectives, efforts to integrate and avoid the duplication of RA processes in ISMS, SMS, and BCMS are indicated in the ISO policy, which supports the validity of the IRA-3MSS.

Next, we discuss inconsistency in the assessment results.

When RA is conducted individually without integrating 3MSS, there may be inconsistencies in the assessment results. Therefore, it is important to confirm that there are no logical inconsistencies in the assessment results. For example, a logical inconsistency is when an IT service is provided using assets that are assessed as having high risks in the RA of ISMS, but the risk assessment result of the IT service is low in the RA of SMS. As RA is one of the highly logical requirements in MSS, there are opportunities for this kind of inconsistency to be pointed out during an audit by a certification body.

In IRA-3MSS, assets and IT services within the scope of 3MSS are identified, and the relations between them are defined in Step 1. In Step 3, conduct RA for assets within the scope of 3MSS and incorporate the perspective of RA in SMS and BCMS intended for IT services related to assets. Subsequently, the entire risk of IT services was calculated using Eqs. (9) and (10), summing the risk levels identified in RA for assets that exceed the risk criteria, so that there is no room for logical inconsistency, as shown in the example. Therefore, it can be concluded that IRA-3MSS is effective in addressing the issue of inconsistency in assessment results.

6. Conclusion

The purpose of this study was to develop an integrated method for RA in 3MSS, thereby avoiding the issues of process duplication and inconsistency in assessment results that occur when conducting RA individually in 3MSS.

First, the validity of the proposed method IRA-3MSS from the perspective of meeting requirements was demonstrated by describing the RA requirements in ISMS, SMS, and BCMS, and explaining that IRA-3MSS meets the requirements of each MS. Next, we showed that duplication of RA processes in 3MSS could be avoided by using IRA-3MSS. In addition, IRA-3MSS calculated the entire risk of IT services utilizing Eqs. (9) and (10), indicating that inconsistency in assessment results could not occur, and the effectiveness of IRA-3MSS was demonstrated.

In this paper, the validity and effectiveness of the IRA-3MSS were discussed on the basis of records of RA for assets and IT services obtained from an organization that has ISMS and SMS certifications [5]. This paper also focused on the integration of RA in 3MSS. Thus, the parameters, w_{ij}, θ, and β_j of the proposed method in this paper were set to simple values and calculation methods from a practical point of view. The remaining challenges include the verification of IRA-3MSS in organizations that have obtained all 3MSS certifications and the search for appropriate values for the parameters. The parameters of the proposed method can be varied depending on the external and internal context of organizations to improve their accuracy. By accumulating data gathered from RA in 3MSS, appropriate values and calculation methods for the parameters could be derived.

References

[1] ISO/IEC 27001: 2022: Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO (2022).

[2] ISO/IEC 20000-1: 2018: Information technology — Service management — Part 1: Service management system requirements, ISO (2018).

[3] ISO 22301: 2019: Security and resilience — Business continuity management systems — Requirements, ISO (2019).

[4] Matsumura, N., Hasegawa, T.: Integration of the risk assessment for an information security management system and that for an IT service management system using composition of relations, *IPSJ* (*Inf. Process. Soc. Japan*) *J.*, Vol.60, No.1, pp.250–259 (2019) (in Japanese).

[5] Matsumura, N., Nishigaki, M., and Hasegawa, T.: Risk Evaluation Model for Information Technology Services in Integrated Risk Assessment. In: Várkonyi-Kóczy, A. (eds) Engineering for Sustainable Future, INTER-ACADEMIA 2019, Lecture Notes in Networks and Systems, Vol.101, pp 318–325, Springer, Cham (2020).

[6] ISO HANDBOOK: The Integrated Use of Management System

Standards (IUMSS), ISO (2018).
[7] ISO/IEC 27013: 2021: Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1, ISO (2021).
[8] Boehmer, W.: Toward a target and coupling function of three different Information Security Management Systems, *Concurrency Computat.: Pract. Exper.*, Vol.24, No.15, pp.1708–1725 (2012).
[9] Białas A.: Development of an Integrated, Risk-Based Platform for Information and E-Services Security. In: Górski J. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2006. Lecture Notes in Computer Science, Vol 4166, Springer, Berlin, Heidelberg (2006).
[10] Kawaguchi, H.: Development of a Multi-purpose Risk Assessment System for Multiple Management System Standards, *J Jpn Ind Manage Assoc*, Vol.64, No.4E, pp.628–637 (2014).
[11] Domingues, P., Sampaio, P. and Arezes, P.: Integrated management systems assessment: a maturity model proposal, *J. Clean. Prod.*, Vol.124, pp.164–174 (2016).
[12] Kozłowski, M.: Integrated airport safety audit, *LogForum*, Vol.13, No.1, pp.39–49 (2017).
[13] BIAŁAS, A.: Information security and business continuity issues and solutions with OSCAD -case studies in public administration, *Theoretical and Applied Informatics*, Vol.25, No.3–4, pp.183–200 (2013).
[14] ISO/IEC 31010: 2019 Risk management – Risk assessment techniques, ISO (2019).
[15] ISO/IEC Directives, Part 1 — Procedures for the technical work — Consolidated ISO Supplement — Procedures specific to ISO, available from 〈https://www.iso.org/sites/directives/current/consolidated/index.html〉 (accessed 2023-09-28).
[16] ISO 31000: 2018: Risk management — Guidelines, ISO (2018).
[17] Hasegawa, T., Matsumura, N., Nagata, M.: Implementation and Effectiveness of ISO Management System in University Information Infrastructure, *Communications of the Operations Research Society of Japan*, Vol.64, No.9, pp.524–533 (2019) (in Japanese).

Appendix

Appendix A: Calculation of the risk levels of all risks for Mail and Global IP address services.

IT Service: Mail

Table A·1 Results of risk level calculations for asset 1.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 1	A	16	32	1	1.55	49.6
Risk 2	A	16	4	1	1.55	6.2
Risk 3	C	24	3	1	1.55	4.65
Risk 4	I	24	3	1	1.55	4.65

Table A·2 Results of risk level calculations for asset 2.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 5	C	24	12	1	1.55	18.6
Risk 6	I	24	8	1	1.55	12.4
Risk 7	A	16	4	1	1.55	6.2

Table A·3 Results of risk level calculations for asset 3.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 8	I	24	12	1	1.55	18.6
Risk 9	C	24	6	1	1.55	9.3
Risk 10	A	16	3	1	1.55	4.65

Table A·4 Results of risk level calculations for asset 4.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 11	I	24	12	1.2	1.55	22.32
Risk 12	I	24	12	1.2	1.55	22.32
Risk 13	C	24	4	1.2	1.55	7.44
Risk 14	A	16	4	1.2	1.55	7.44

Table A·5 Results of risk level calculations for asset 5.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 15	C	24	16	1.2	1.55	29.76
Risk 16	A	16	8	1.2	1.55	14.88
Risk 17	I	24	4	1.2	1.55	7.44

Table A·6 Results of risk level calculations for asset 6.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 18	C	24	16	1	1.55	24.8
Risk 19	A	16	12	1	1.55	18.6
Risk 20	I	24	4	1	1.55	6.2

Table A·7 Results of risk level calculations for asset 7.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 21	C	24	4	1.2	1.55	7.44
Risk 22	A	16	2	1.2	1.55	3.72
Risk 23	I	24	2	1.2	1.55	3.72

Table A·8 Results of risk level calculations for asset 8.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 24	I	24	3	1.2	1.55	5.58
Risk 25	A	16	2	1.2	1.55	3.72

Table A·9 Results of risk level calculations for asset 9.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 26	C	24	16	1	1.55	24.8
Risk 27	A	16	12	1	1.55	18.6
Risk 28	A	16	8	1	1.55	12.4
Risk 29	I	24	8	1	1.55	12.4
Risk 30	I	24	4	1	1.55	6.2

T Service: Global IP address

Table A·10 Results of risk level calculations for asset 10.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 31	A	16	16	1.2	1.45	27.84
Risk 32	A	16	4	1.2	1.45	6.96
Risk 33	C	24	2	1.2	1.45	3.48
Risk 34	I	24	2	1.2	1.45	3.48

Table A·11 Results of risk level calculations for asset 1.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 1	A	16	32	1.2	1.45	55.68
Risk 2	A	16	4	1.2	1.45	6.96
Risk 3	C	24	3	1.2	1.45	5.22
Risk 4	I	24	3	1.2	1.45	5.22

Table A·12 Results of risk level calculations for asset 11.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 35	A	16	3	1	1.45	4.35
Risk 36	I	24	2	1	1.45	2.9
Risk 37	C	24	1	1	1.45	1.45

Table A·13 Results of risk level calculations for asset 9.

	CIA	θ	r_{ik}	w_{ij}	β_j	Result
Risk 26	C	24	16	1	1.45	23.2
Risk 27	A	16	12	1	1.45	17.4
Risk 28	A	16	8	1	1.45	11.6
Risk 29	I	24	8	1	1.45	11.6
Risk 30	I	24	4	1	1.45	5.8

Note. In Tables A·1 to A·13, risks with a highlighted result column indicate that they exceed risk criterion θ.

Noriaki Matsumura has a Ph.D. in Informatics from Shizuoka University (2020), and a Master of Political Science from Tokai University (2003). He is a Senior Assistant Professor at Shinshu University. His research interests include information infrastructure, information security, risk management, and social network analysis. He is a member of the IEICE and IPSJ.

Takahiro Hasegawa received his M.S. and Ph.D. in Information Engineering from Kyushu Institute of Technology in 1994 and 1997, respectively. He is a Professor and Director of the Center for Information Infrastructure at Shizuoka University. His research interests include information infrastructure, information security, and management systems. He is a member of the JSDSS, SSJ, and IPSJ.