Journal of Information Systems Engineering and Management
2025, 10(10s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Assessing Information Security Risks in an Interconnected System using Octave Allegro, NIST Privacy Framework and ISO 27010:2015

Fauzan[1*], Benfano Soewito[2]
[1,2]*Computer Science Department, BINUS Graduate Program, Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia*
*fauzan001@binus.ac.id[*1], bsoewito@binus.edu[2]*
**Corresponding Author: fauzan001@binus.ac.id*

ARTICLE INFO

Received: 08 Nov 2024

Revised: 25 Dec 2024

Accepted: 12 Jan 2025

ABSTRACT

The increasing adoption of information systems (IS) within government organizations necessitates the seamless integration of these systems to improve efficiency and transparency in service delivery. While the operation of interconnected government information systems enhances efficiency, it also introduces unknown risks to information security and privacy. The purpose of this study is to identify and assess the potential risks that may arise from the nature of interconnected systems and to propose measures to mitigate these risks. The study employs the OCTAVE Allegro method to address information security risks based on data gathered from the day-to-day operations of the interconnected systems. A new framework is then developed by integrating two well-established frameworks— the NIST Privacy Framework and ISO/IEC 27010:2015— with the risk assessment findings. This new risk-based information security framework is subsequently used to evaluate the current operations of three IS within the Ministry of Public Works and Housing, based on organizational, technical, and personnel indicators. The results reveal that the average score of the current controls in place is 2.58, which is considered fairly good although the organizational indicator received the lowest score. To address this, specific recommendations are provided for each control in the new framework to close the gap between the ideal and current conditions. These insights are then utilized by the government organization to enhance overall infrastructure security and privacy practices, ultimately contributing to a more resilient and interconnected ecosystem for public services.

Keywords: Information Security, Government, Organizational Privacy, Infrastructure Security, Privacy Framework, ISO/IEC 27010:2015

INTRODUCTION

In recent years, privacy discussions have primarily centered around individual privacy, especially concerning personal data protection. However, academic discourse needs to devote more attention to organizational privacy, which encompasses the confidentiality, integrity, and availability of sensitive institutional information (Rath & Kumar, 2021). The risks associated with organizational privacy have grown more significant as government entities increasingly adopt interconnected systems to facilitate seamless communication and service delivery. These risks are not limited to conventional data intrusions; they include systemic vulnerabilities, unauthorized access, and data misuse, potentially compromising public trust and internal operations. The growing need for interoperability among government systems presents complex challenges in managing information security. By "interoperability", we refer to the capability of two or more organizations or entities to seamlessly exchange necessary information and leverage it for common objectives (Bass, Clements, & Kazman, 2003). This cross-organizational system integration introduces a new class within information systems known as the System-of-Information-Systems (SoIS) (Neto, Cavalcante, El Hachem, & Santos, 2017; Saleh & Abel, 2018). SoIS represents a collaboration between information systems for specific periods of time, improving functionality and offering new possibilities that would be unattainable by any individual system alone. However, this integration also introduces new challenges (Paniagua, Eliasson, & Delsing, 2019), (Ceccarelli, Bondavalli, Froemel, Hoeftberger, & Kopetz, 2016). Unlike typical systems that are generally transactional and capable of sharing data with other systems, SoIS is distinguished by its central management. This management oversees the flow of information, ensuring that systems work together effectively and efficiently. This increased participation of cross-organizational entities raises the risk of potential threats to information security and privacy (Lubbe & Serfontein, 2023), including inconsistent data formats, insecure data exchanges, and uncoordinated security practices across interconnected systems. Furthermore, the exchange of information and collaboration can lead to the emergence of new vulnerabilities that have a significant impact on the entire SoIS (Olivero, Bertolino, Dominguez-Mayo, Matteucci, & Escalona, 2022).

Therefore, this study aims to provide a comprehensive evaluation of the information security risks associated with SoIS in government organizations. This research employs the OCTAVE Allegro method to identify information security risks then utilizes well-established frameworks like the NIST Privacy Framework 1.0 and ISO/IEC 27010:2015 to manage those risks. This research was carried out in one of the organizational units in the Ministry of Public Works and Public Housing of Indonesia (Kemen PUPR), which coordinates the implementation of an interconnected system/SoIS for construction and development services in Indonesia. The organization is the Directorate General of Construction Development (DJBK), and the SoIS referred in this research is the licensing procedure which consists of 3 systems which belongs to DJBK and several other systems from other organizations. This research fills a critical gap in the literature by offering a nuanced understanding of how government organizations can balance the need for interoperability with robust information security and privacy measures. The findings contribute to advancing secure digital transformation initiatives, ensuring that interconnected systems within the public sector remain resilient against emerging threats while maintaining the integrity of organizational privacy.

Literature Review

Information security encompasses the measures used to protect information assets, ensuring that it remains confidential, unaltered, and readily available during its storage, process, and the transmission (Whitman & Mattord, 2021). An information security risk assessment is an essential component of an information security audit (Kuzminykh, Ghita, Sokolov, & Bakhshi, 2021). Many established information security risk assessment methods have already been created to be used by government or private companies (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). Some approaches are specifically tailored to achieve certification objectives, while others are exclusively developed to address the needs of information security-critical systems. Some approaches may require the expertise of an analyst and a large team, while others can be accomplished with just a few skilled people (Ionita, 2013). OCTAVE Allegro methodology belongs to the latter category, making it suitable for our research. The result of this risk assessment methods is subsequently utilized to establish the security requirements, encompassing both functional and nonfunctional requirements that must be satisfied to reach the required level of security (Ionita, 2013).

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Allegro establishes a thorough review process by consolidating the information assets, risks, and vulnerabilities the company may initiate to comprehend which information is susceptible to risk and minimize the overall vulnerability of its information assets.

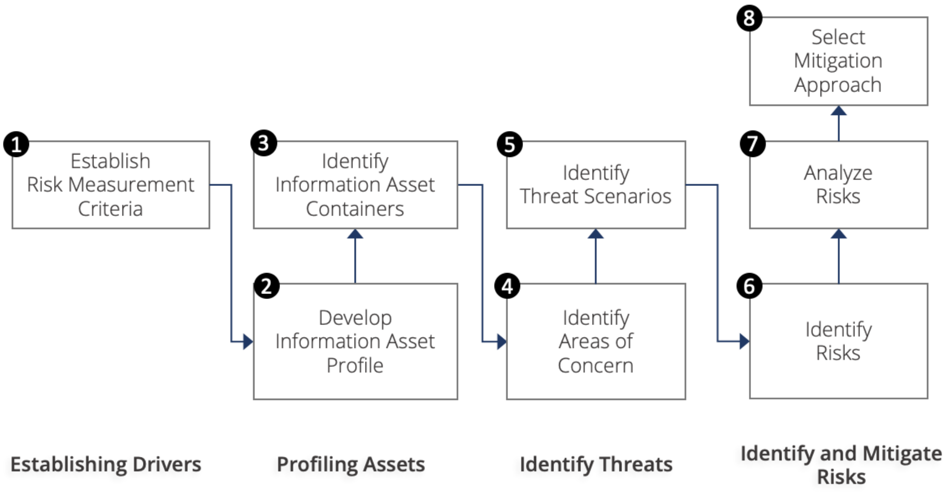

8 Select Mitigation Approach
1 Establish Risk Measurement Criteria
3 Identify Information Asset Containers
5 Identify Threat Scenarios
7 Analyze Risks
2 Develop Information Asset Profile
4 Identify Areas of Concern
6 Identify Risks
Establishing Drivers
Profiling Assets
Identify Threats
Identify and Mitigate Risks

Fig. 1. OCTAVE Allegro Process (Caralli, Stevens, Young, & Wilson, 2007)

The OCTAVE Allegro (OA) methodology has eight sequential steps, as can be seen in Fig. 1, which are divided into four distinct phases:

- During first phase, the organization establishes risk measurement criteria that match its objectives.
- In second phase profiles critical information assets. This profiling method determines asset parameters, security needs, and places where the asset is stored, moved, or processed.
- In the third phase, threats to information assets are identified within their specific storage, movement, or processing environment.
- The last phase identifies, analyses, and develops information asset risk reduction measures.

As a methodology that is focused on information assets as essential properties, OA included a threat tree, as illustrated in, that can be used to maximize how we look at threats when handling information assets.

The National Institute of Standards and Technology (NIST) Privacy Framework (PF) is a voluntary instrument created to assist organizations in identifying and managing privacy risk (National Institute of Standards and Technology, 2020). While initially intended for individual privacy, many of the controls offered in NIST PF also correspond to the organizational level regarding interactions with external parties. This characteristic makes it well-suited for our study. The core component of NIST PF encompasses activities and outcomes in five primary functions, namely **Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P.**

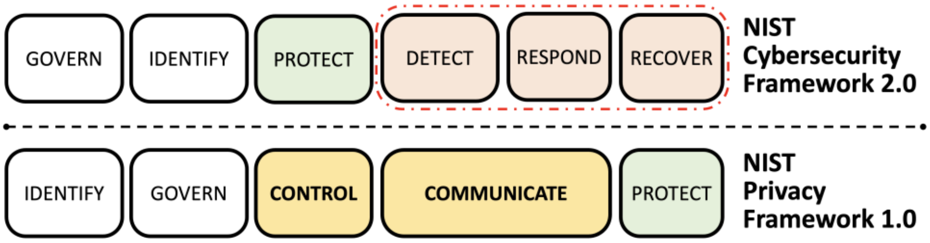


Fig. 2. Differences between NIST CSF and PF

These core functions differ from those outlined in the NIST Cybersecurity Framework (CSF), as shown in Fig. 2. While the NIST CSF's Detect, Respond, and Recover functions are well-suited for managing a single information system, they cannot be fully implemented in managing a System-of-Information-Systems (SoIS), which consists of multiple interconnected systems, due to conflicting authority between these systems. The NIST Privacy Framework (PF) addresses this issue by introducing the "Control" and "Communicate" functions. Since NIST has developed.

guidelines in NIST 800-53 Rev 5, which are already mapped to both the NIST CSF and NIST PF, these guidelines can be used to select appropriate recommendations for each risk.

ISO/IEC 27000 family is a globally recognized standard that outlines the necessary controls for managing information security systems. ISO/IEC 27010:2015 (International Organization for Standardization, 2015) is an addition to the ISO27000 family, which addresses the need to secure exchanges of sensitive information between public and private organizations within the same industry or between sectors where the information cannot be made publicly available other than the member of the pre-defined community. There are 4 additionals measures dan 14 changed description from ISO 27002:2013 which been identified in clauses 5 to 18 of ISO 27010:2015.

When assessing the risks to their information security, several organizations and academics are already utilizing OA. To aid in risk-based decision-making, for instance, Ki-Aries et al. (Ki-Aries, Faily, Dogan, & Williams, 2022), created the OASoSIS (OA for SoS with CAIRIS) framework, which expands the usage of OA methodologies to the SoS environment. After the necessary procedures were carried out, the CAIRIS model was used to visualize risks and highlight crucial information. The research has proven highly promising in terms of visualizing the results, discovering emergent behavior, and detecting flaws in the interconnection environment of the systems involved. However, the scope of research is purposedly limited, without including all the systems and information systems involved. The implementation could be more significant if this study included other organizations with different business processes. Irsheid et al. (Irsheid, Murad, AlNajdawi, & Qusef, 2022) compared applicability, adaptability, and involvement in finding the best risk management strategy for cloud-hosted systems. Thus, researchers recommend OA with certain adjustments for cloud-based methods. OA excels at adapting to changing cloud threats. The researchers found that OA is better at handling complex operational difficulties in cloud systems with several enterprises. OA prioritizes risk detection and analysis for vital information assets, especially in cloud situations where information is often the main focus. This prioritization lets companies concentrate and secure their most valuable assets. The comparison is extensive, and the results are relevant to what this research needs, especially when information is the primary asset and several businesses are involved in the interconnectivity business process. However, it limited by its difficulty applying it to real-world cross-government circumstances involving several regulations. To fill this gap, this study will be more concern on regulatory issues and the recommendations for the said issues.

METHOD

Fig. 3 illustrates the steps of this research method. The initial stage involves a literature review and problem identification, establishing the context based on the organization's need for information security controls to manage multiple interconnected information systems while defining the scope of the research. This stage includes a review of prior studies on interoperability, system-of-information-systems (SoIS), the ISO 27000 family, privacy frameworks, and information security risks. Data collection is conducted through business observations, interviews, and questionnaires to capture the organization's perspectives on the subject. Subsequently, relevant clauses from the NIST Privacy Framework and ISO 27010:2015 are selected and integrated in accordance with the findings from the data collection phase. A risk assessment is then conducted using the OCTAVE Allegro (OA) method based on the gathered data. We also make sure the weighting of the risks incorporate the nature of SoIS, therefore interoperability analysis are also added in this phase as mentioned in the study by (Ki-Aries et al., 2022).

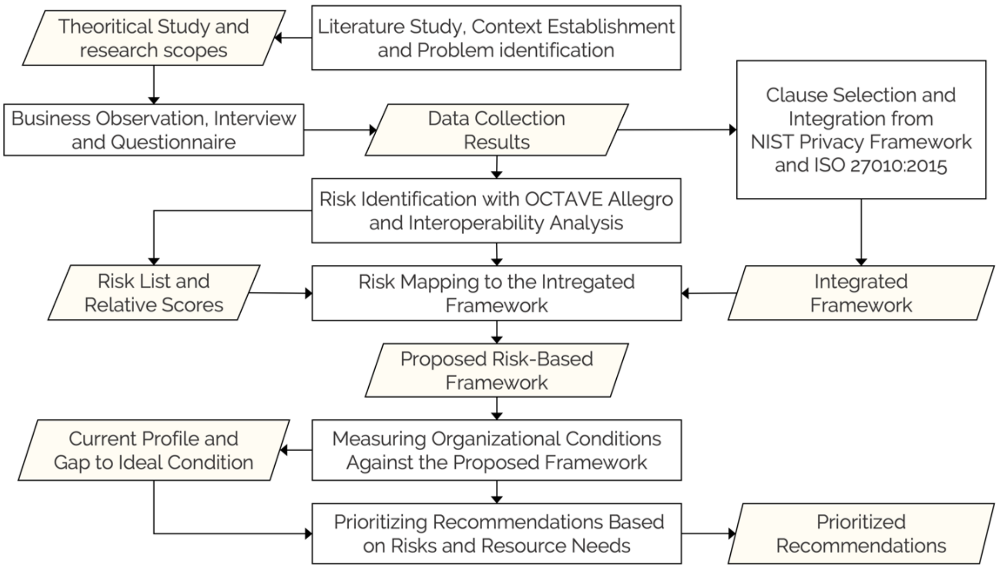

Theoritical Study and research scopes
Literature Study, Context Establishment and Problem identification
Business Observation, Interview and Questionnaire
Data Collection Results
Clause Selection and Integration from NIST Privacy Framework and ISO 27010:2015
Risk Identification with OCTAVE Allegro and Interoperability Analysis
Risk List and Relative Scores
Risk Mapping to the Intregated Framework
Integrated Framework
Proposed Risk-Based Framework
Current Profile and Gap to Ideal Condition
Measuring Organizational Conditions Against the Proposed Framework
Prioritizing Recommendations Based on Risks and Resource Needs
Prioritized Recommendations

Fig. 3. Research Methodology

Then, we utilize the risk findings and the integrated framework to develop a new risk-based framework for evaluating the organization's current controls. Finally, using all the data gathered from the data collection phase, we assess the gap between the organization's current state and the ideal condition using three indicators: organizational, technical, and personnel. Organizational (O) indicators examine policy and regulatory availability, leadership support and expertise, and organization-wide processes. Technological (T) indicators examine infrastructure, budget, and monitoring systems. Personnel (P) indicators evaluate technical staff availability, understanding, and competency. The gap from these three indicators illustrates how many resources the organizations need to achieve the target profile. Based on the results of this evaluation, we provide recommendations to enhance the organization's cyber resilience posture.

RESULTS AND DISCUSSION

Defining Risk Measurement Criteria

At this stage, an evaluation of the impact and selection of priority impact areas is conducted. Within the OA, the selection of impact areas can be done by utilising the provided template or by independently creating user-defined impact areas. As stated in Table 1, two impact areas are taken from the OA template, while the other two are determined by using information gathered during the data collecting phase.

Table 1 - Impact Areas and Descriptions

Impact Areas	Descriptions	Priority
Reputation and Stakeholder Trust	The organization's image or reputation and stakeholder trust may be compromised.	**3**
Legal/Regulatory Compliance	The organization may be subject to legal consequences and violations of regulations.	**2**
Budget	Changes to the organization's work plan and additional budget requirements	**1**
Operational	Daily operational issues affecting service delivery and business processes	**4**

The priority is assigned to the areas based on the impact on the organization. The reason for establishing the greatest priority value on "*Operational*" area is because it has a direct impact on the service delivery and business process. If operations become disrupted, the consequences will be significant enough to also affects other areas. The "*Budget*" is considered a low priority due to its relatively minor influence or the ease of managing any potential impact.

Then, a relative risk score was given to each impact area. The relative scores can be categorized as High, Moderate, Low, or Minimal, as explained in the preceding chapter. The example of circumstances under which this area was affected is then recorded as in Table 2. Each relative score represents a scenario that could occur and its potential impact on the corresponding area which is reputation and stakeholder trust.

Table 2 - Example of Relative Score on Reputation and Stakeholder Trust

Minimal	Low	Moderate	High
REPUTATION			
Negligible effect on the organization's reputation	Not many users have felt the damage yet, therefore reputation can be restored with little effort	Repairing the organization's reputation requires moderate effort	Organization's reputation severely damaged, requires significant effort to restore
STAKEHOLDERS CONFIDENCE (from e-government usage)			
Negligible effect on the stakeholders confidence	Reduced stakeholder confidence by 5%	Reduced stakeholder confidence from 6-10%	Reduced stakeholder confidence more than 10%
PUBLIC SATISFACTION			
Negligible effect on the on public satisfaction	Public satisfaction is slightly reduced with 1-9 complaints received	Public satisfaction suffers with 10-15 incoming complaints	Public satisfaction collapsed with 16-30 incoming complaints

Defining Risk Measurement Criteria

The following step involves creating an information asset profile for each information asset that is deemed essential for the functioning of SoiS. In this step the asset's ownership and the access requirements for users to access the information asset, seen from a confidentiality, integrity, and availability perspective are also documented. To begin, we establish the criteria for information assets that are deemed critical to SoIS. The following criteria that have been established:

1. Assets store a process-specific data that is not publicly available
2. Assets are utilized to ensure the functionality and functioning of the SoIS
3. Restoring damaged or lost of information assets requires downtime

By the criteria established earlier, the three most important information assets that have been discovered are Contractors and Personnel Reference Data, Contractors' Work Experience Data, and Contractors' Machinery Ownership Data. Table 3 provides an example of how information profiling is conducted on the "Contractors and Personnel Reference Data". The same approach will also be applied to the remaining information assets.

Table 3 - Example of Profiling the Information Asset

Contractors and Personnel Reference Data	
Rationale	The main data used as initial validation of the application to process Certification Applications by the Contractors. This data is important as it is the main requirement of the said application by from Contractors
Owner	Manager and IT Team of SIKI subsystem
SECURITY REQUIREMENTS	
Confidentiality	Only authorized accounts can view and change all information: subsystem administrator, contractor /personnel user account, API Perizinan, and API LSBU can take action according to the agreed-upon endpoint and payload
Integrity	Actions on this information are restricted to users who possess credentials or services that include tokens. The information must correspond to the user in question
Availability	This data must always be available so that user's applications on the licensing portal can proceed. The process in the licensing portal by contractors and personnel are available outside of working hours, so this data must be available 24 hours a day, 7 days a week
Availability is the most important security requirement	

Information Asset Container Identification

Every information asset is then identified based on its location when stored, processed, and transferred. Each information asset is categorized into three types of containers, namely: technical, physical, and people. The technical container translates to hardware or software that stores the information. The physical container refers to the asset's physical location within the organization. People are the individuals who interact with the information daily. These containers are further classified as internal or external based on the organizational scope of responsibility over the container. Based on the circumstances in which the information is managed, the three containers of information assets are identified. The example on one of the information asset in this process as illustrated in Table 4.

Table 4 - Example of Asset Container Identification

Contractors and Personnel Reference Data			
Container	Scope	Description	Owner(s)
Technical	Internal	This asset is used by SIKI subsystem	IT Team of SIKI
		This data asset is utilised by the organization's datawarehouse (DWH)	IT Team of DWH
		The production server of this asset is hosted on the National Data Center (NDC)	NDC Team
	External	The contractors acces this information asset via web based SIKI	Contractor
		The development server of this information asset is hosted on the Google Cloud Platform (GCP)	Vendor
		LSBU API is used to retrieve contractors references data from this asset	IT Team of LSBU

		Perizinan Portal API is used to retrieve contractors references data from this asset automatically	IT Team of Portal
Physical	Internal	The previous iteration and the duplicate copies of this valuable data are kept on an external hard disc by manual means. The hard disc This term is utilised exclusively in cases where there are concerns pertaining to the previous iteration of the database.	IT Team of SIKI
People	Internal	IT Team of SIKI	SIKI
		IT Team of DWH	DWH
	External	IT Team of LSBU	LSBU
		IT Team of Portal	Portal
		NDC Team	NDC
		Contractors	User
		Vendor	Google

Area of Concern

During this phase, areas of concern are determined by evaluating the environment of each information asset to identify and evaluate the potential threats that could arise within the container. The necessary information to be acquired are the potential concern that may arise, how these risks manifest in associated containers, and the potential information security breaches within these containers. According to this information, the area of concern that were successfully identified are listed in the Table 5.

Table 5 - Area of Concern

ID	Areas of Concern (A)
A1	The subsystem has been targeted by a cyber attack
A2	There is a disruption or disconnection in the inter-connection pathway from the internal subsystems to the DWH
A3	A disruption in the operation of the production cloud server (GCP)
A4	A disruption in the operation of the development cloud server (NDC)
A5	Potential security vulnerabilities in API endpoints used by external system
A6	Modifications to the data standards and formats within the subsystem
A7	The subsystems do not have any form of data classification
A8	External systems lack the capability to ensure the protection of personal data
A9	Physical data backup on the external hard disk has been damaged
A10	Inside threats from subsystem administrators who unlawfully modify, add, and delete data
A11	The subsystem does not have any specific standards for credential management and user access control
A12	Lack of multi-factor authentication (MFA) when accessing the subsystems
A13	There is no monitoring or logging of user access to subsystems
A14	System administrators sharing processed sensitive data from subsystems to the public
A15	The person responsible for managing external API reveals his or her credentials to other people.
A16	A mistake in the server cloud security configuration made by the vendor
A17	Data integrity and availability during the cloud migration procedure
A18	The different server environments that are used in development and production

Threat Scenarios and Risks Identification

The compiled areas of concern then transformed into threat scenarios by simulating a real-world event according to the area of concern identified in the previous stage. This can be achieved by identifying the actors, means, motives, and outcomes for each area of concern. At this point, we also assigned probabilities to each threat discovered, with values between 1 (Low Probability) and 3 (High Probability).

This probability score (pb) will be beneficial in situations where two distinct threats occurred and had the same impact in defined impact areas, resulting in the same relative score. At the same time, the likelihood of the occurrence of the two threats could end up significantly different from one another. the risk consequences identified throughout this stage for every threat scenario discovered so far. Risk is defined as a threat combined with impact. Therefore, the following phase we will also assess the impact of each threat scenario as documented in Table 6.

Table 6 - Threat Scenario and Risk Identification

ID	Actor	Threat Scenario	(*pb*)	Consequences
T1	Hackers	Cross-Site Scripting (XSS) attacks that generate online gambling links on the server continously by exploiting webserver vulnerabilities	**2**	The system was disabled, the stakeholders unable to access the subsystem for a period of eight hours. Impact in the decrease in public confidence
				The increased frequency of attacks leads to greater resource utilization on the cloud server, resulting in the going over of the allocated budget for cloud server expenses
T2	Eksternal Systems	Networks between DWH and subsystems accidentally disconnected due to network configuration changes following the latest guidelines	**1**	The datawarehouse does not consist current data, resulting in the display of inaccurate data on both the public and executive dashboards
T3	Third Party	Failure to effectively communicate production server specifications prevented the server from handling subsystem workload	**2**	The functional subsystem stopped working due to system overload, requiring downtime and specs upgrades just to bring the system to its normal operation
..	..	..	**..**	..
T18	IT Team	Administrators often fail to implement security configurations in production that were present in the development environment due to differences between the two environments	**2**	Administrators have difficulty implementing a list of Common Vulnerabilities and Exposures (CVE) on the operating system due to inconsistent configuration. The production environment's systems are becoming increasingly susceptible to information security incidents.

Each of these risks may or may not impact the entire SoIS if they occur. Given that this research focuses on the interconnected nature of SoIS, we will also assess the potential impact through interoperability analysis. For this each risk is categorized by its corresponding SoIS ID, as different risks may have the same impact on the SoIS as seen on Table 7.

Table 7 - Interoperability analysis

SoIS ID	*interoperability analysis*	Threat IDs	Impact
S1	Downtime in a single subsystem disrupts the overall operation of the SoIS, leading to data inconsistencies and process backlogs.	T1, T2, T3, T16, T18	High
S2	Delays in feature deployment within the development environment create cascading effects across interconnected subsystems.	T4	Low
S3	A data breach in one subsystem compromises the security posture of the entire SoIS.	T5, T14, T10, T15	High
S4	Inconsistent data transfers between subsystems increase the risk of data loss, potentially halting SoIS operations.	T6	High

S5	The absence of robust data classification practices heightens the likelihood of inappropriate data sharing within the SoIS.	T7, T8	Low
S6	Data integrity issues introduce inconsistencies that result in service bottlenecks across the SoIS	T17	Medium
S7	Poorly managed access controls expose interconnected subsystems to security breaches within the SoIS.	T11, T12, T13	High

Risk Analysis

After identifying the list of risks, a risk analysis is conducted to determine each risk's relative value based on its impact on the pre-defined criteria. This can be done using the formula (1):

$$Score = \left(\sum_{i=1}^{4}(P_i \; x \; I_i)\right) x \; (pb) \qquad (1)$$

- Priority score value (P_i) is a constant value that has been specified from the start, based on Table 1 which are:
    - ○ P_1 (Reputation and Stakeholder Trust) = 3
    - ○ P_2 (Legal/Regulatory Compliance) = 2
    - ○ P_3 (Budget) = 1
    - ○ P_4 (Operational) = 4
- The impact score value (I_i) is derived from the condition of each risk, matched to the Impact Area Relative Score Distribution as the example on Table 2. Each category (minimal, low, moderate, and high) is assigned a value ranging from **0** to **4**.
- Probability (pb) is the likelihood of a risk occurrence, with a qualitative value between one (1) to three (3) as stated in Table 6.

Based on the risk formula for each of the risk that are already defined, the relative score is calculated as presented in Table 8.

Table 8 - Total Relative Score

Threat ID	I_1	I_2	I_3	I_4	*subtotal*	(pb)	**Score**	**Rank**
T1	2	0	2	3	20	2	40	1
T2	2	0	0	1	10	1	10	18
T3	1	0	0	2	11	2	22	8
T4	0	1	0	1	6	2	12	15
T5	2	1	1	3	21	1	21	11
T6	2	0	0	1	10	3	30	4
T7	2	0	1	1	11	2	22	9
T8	3	0	0	0	9	2	18	13
T9	1	0	1	2	12	1	12	16
T10	3	1	1	3	24	1	24	7
T11	1	2	0	1	11	2	22	10
T12	2	1	1	2	17	2	34	2
T13	1	2	1	2	16	2	32	3
T14	3	1	0	0	11	1	11	17
T15	1	2	0	2	15	2	30	5
T16	2	0	1	3	19	1	19	12
T17	3	1	1	1	16	1	16	14
T18	2	1	1	1	13	2	26	6

Risk Treatment and Mitigation

Risks then categorized according to their final score. First, the risks were sorted in order of their severity. Afterwards, they were allocated to four pools using quartiles to categorized the sorted data based on their relative magnitude as seen on Table 9.

Table 9 - Risk Treatment

Pool	**Treatment**	**Detail**	**Threat IDs**
1	*Mitigate*	Is the risk that has the highest impact on the organization and needs immediate mitigation.	T1, T12, T13,T6, T15
2	*Mitigate or Defer*	It is a risk that is quite high in impact, but the organization may decide to postpone mitigation if the interoperability impact analysis is low.	T18, T10
3	*Defer or Accept*	These are the risks with a moderate impact on the organization. Depending on the interoperability impact analysis, risks in this pool can be postponed or accepted.	T3, T7, T11, T5, T16, T8
4	*Accept*	It is a risk that, according to the organization's concerns, is considered to have minimal impact so that the organization can decide to accept the risk.	T17, T4, T9, T14, T2

For risks with a high impact on the interconnected systems as a whole (SoIS), as outlined in Table 7, we select the more safer mitigation measures for those specific risks. A summary of the treatments applied to all identified risks is presented in

Table 10 - Recapitulation of Risk Treatment

Treatment	**Threat IDs**	**Total**
Mitigate	T1, T6, T10, T12, T13, T15, T18	7 Risks
Defer	T3, T5, T7, T11, T16	5 Risks
Accept	T2, T4, T8, T9, T14, T17	6 Risks

Control Integration

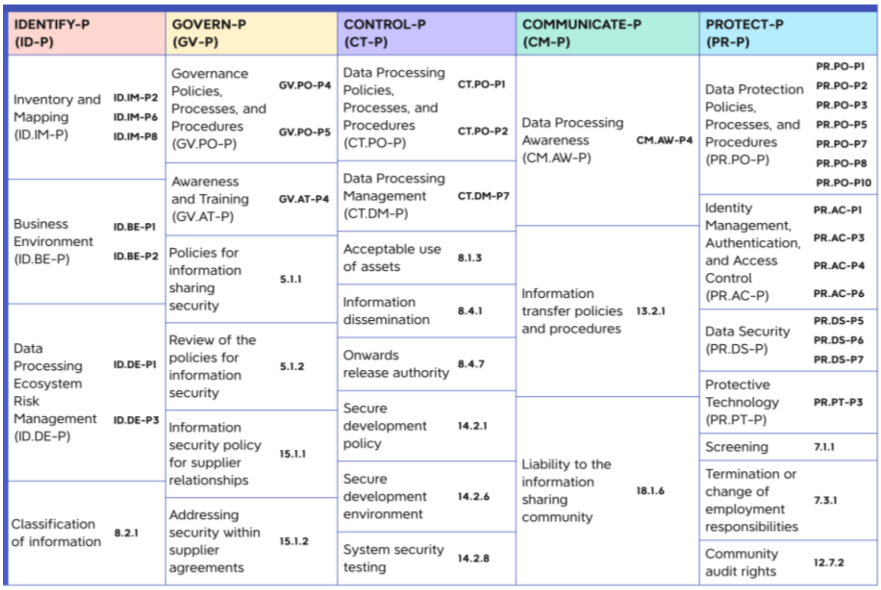
According to the outcome, as mentioned earlier, the next step is implementing the specified mitigation strategy by giving a control recommendation based on integrating NIST PF and ISO 27010:2015. For this, we need to create control integration first before continuing to do so. All the identified risks will be used to map the new framework, as seen in the example in

Table 11 - Clauses Selection from NIST PF and ISO 27010:2015

Threat ID	**Control Integration**
T1	PR.DS-P5: Protections against data leaks are implemented.
	PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.
	PR.PO-P10: A vulnerability management plan is developed and implemented.
	13.2.1 Information transfer policies and procedures
T2	PR.PO-P2: Configuration change control processes are established and in place.
	PR.PT-P3: Communications and control networks are protected.
	PR.PO-P3: Backups of information are conducted, maintained, and tested.
...	...
T18	PR.PO-P1: A baseline configuration of information technology is created and maintained incorporating security principles.
	PR.DS-P7: The development and testing environment(s) are separate from the production environment.

	14.2.1 Secure development policy
	14.2.6 Secure development environment
	14.2.8 System security testing

ISO 27010:2015 is utilized when the reference controls from the NIST PF do not fully address that particular risk. After mapping all relevant risks to their corresponding controls, we identified 45 controls as our proposed framework from both NIST PF and ISO 27010:2015, based on the risks identified in the previous steps. These controls span across five functions, following the structure of the NIST PF, as illustrated in Fig. 4.



IDENTIFY-P (ID-P)

- Inventory and Mapping (ID.IM-P): ID.IM-P2, ID.IM-P6, ID.IM-P8
- Business Environment (ID.BE-P): ID.BE-P1, ID.BE-P2
- Data Processing Ecosystem Risk Management (ID.DE-P): ID.DE-P1, ID.DE-P3
- Classification of information: 8.2.1

GOVERN-P (GV-P)

- Governance Policies, Processes, and Procedures (GV.PO-P): GV.PO-P4, GV.PO-P5
- Awareness and Training (GV.AT-P): GV.AT-P4
- Policies for information sharing security: 5.1.1
- Review of the policies for information security: 5.1.2
- Information security policy for supplier relationships: 15.1.1
- Addressing security within supplier agreements: 15.1.2

CONTROL-P (CT-P)

- Data Processing Policies, Processes, and Procedures (CT.PO-P): CT.PO-P1, CT.PO-P2
- Data Processing Management (CT.DM-P): CT.DM-P7
- Acceptable use of assets: 8.1.3
- Information dissemination: 8.4.1
- Onwards release authority: 8.4.7
- Secure development policy: 14.2.1
- Secure development environment: 14.2.6
- System security testing: 14.2.8

COMMUNICATE-P (CM-P)

- Data Processing Awareness (CM.AW-P): CM.AW-P4
- Information transfer policies and procedures: 13.2.1
- Liability to the information sharing community: 18.1.6

PROTECT-P (PR-P)

- Data Protection Policies, Processes, and Procedures (PR.PO-P): PR.PO-P1, PR.PO-P2, PR.PO-P3, PR.PO-P5, PR.PO-P7, PR.PO-P8, PR.PO-P10
- Identity Management, Authentication, and Access Control (PR.AC-P): PR.AC-P1, PR.AC-P3, PR.AC-P4, PR.AC-P6
- Data Security (PR.DS-P): PR.DS-P5, PR.DS-P6, PR.DS-P7
- Protective Technology (PR.PT-P): PR.PT-P3
- Screening: 7.1.1
- Termination or change of employment responsibilities: 7.3.1
- Community audit rights: 12.7.2

Fig. 4. The Proposed Risk-Based Framework

Gap Analysis

The proposed framework is used to evaluate the current condition of the organization. As outlined in the preceding chapter, this assessment considers three primary indicators: organizational (O), technical (T), and personnel (P). The analysis is based on data collected during the data-gathering phase. The target score is set at a level of three (3), which aligns with the "Repeatable" tier in the NIST PF Implementation Tiers, reflecting a systematic and consistent approach to managing privacy risks.

By assigning a score to each indicator, we are able to determine the organization's average performance across each control. Additionally, a gap analysis is conducted for each control, calculating the difference between the current state and the desired target. Since the three indicators reflect the organization's approach to risk management, the scores provide insight into how resources have been allocated to mitigate risks thus far. The gap analysis score, therefore, represents the extent to which the organization's resources are being utilized to achieve the ideal or target profile. An example of how the scoring process is applied to a number of controls can be seen in Table 12, and this process will be conducted to all the 45 controls.

Table 12 - Organization's Current Condition

Controls	**Description of Current Condition**	**Indicator**			**Avg**	***Gap***
		O	**T**	**P**		
GV 5.1.2	Currently, no review of policies or protocols is conducted when there is a change in the members involved in the interconnection.	1	1	2	1.33	1.67
PR.PO-P2	In the context of interconnection, this has not yet been implemented. Configuration changes in a system are only identified by external organizations when an error or issue	1	3	1	1.67	1.33

	arises. Additi onally, there are no binding regulations in place regarding this matter.					
CT 8.4.1	The information received is utilized, processed, and shared according to its function and the initial scope of the interconnection agreement. However, this has not yet been enforced at the technical staff level, and there is no established mechanism for verification.	3	2	2	2.33	0.67
. . .	. . .	.	.	.	..	..
PR.AC-P4	Separation of duties has been implemented; however, the principle of least privilege is not always applied across all systems. Similarly, other security principles are not consistently enforced throughout the organization.	3	3	2	2.67	0.33
PR 12.7.2	There currently needs to be authority to audit the information security of other interconnected systems. Now, audits can only be carried out by Data and Information Technology Center (Pusdatin). This control is for an accepted risk.	3	3	3	3.00	0.00

If we look at how the score on each control based on the current condition on the organization in we can really see that the organization needs to strengthen the governing process of all the party involved in manging this interconnected systems (SoIS).

Table 13 - Average Score and Gap Value on Each Function

Functions	**Avg Value of Each Function**	***GAP***
IDENTIFY	2.67	0.33
GOVERN	*2.38*	*0.62*
CONTROL	2.56	0.44
COMMUNICATE	2.67	0.33
PROTECT	2.61	0.39
Average	**2.58**	**0.42**

The “Govern” function scores far below the average of all functions as can be seen in Table 13, meaning that the potential risk will arise mostly in the governing process of the interconnected system. This is also reflected in the gap score, which mean the organization’s resource might be substantial to fix this issue.

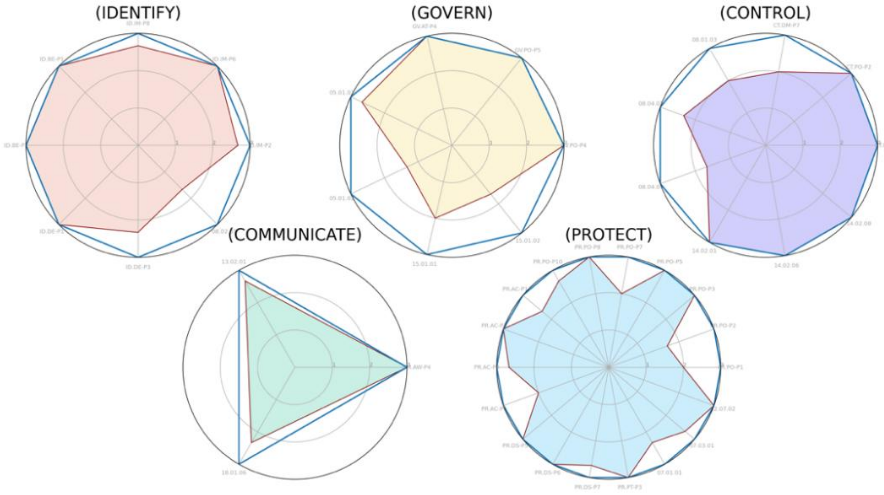


Fig. 5. Gap Analysis Result

Fig. 5 illustrates the assessment results for each function across the proposed controls. Of the 45 controls evaluated, 21 are found to be in ideal conditions, while the remaining 24 require improvement to reach the desired state. The gap values for these controls range from 0.33 to 1.67, indicating areas where enhancements are needed. Recommendations are provided for these areas based on the gap analysis. It is expected that the organization will reduce these gap values by implementing the recommendations aligned with the proposed framework.

Recommendations

As mentioned in the previous chapter, all the identified risks are already mapped into each of the 45 controls. In which every control can have more than one risk associated with it. This is because several risks might use the same control to mitigate the risks. So now, across all the controls from the proposed framework, we can calculate the average score from that particular control using the identified score in the early step. Based on the value of the average score on each control, we then categorized it into high, mid, and low risk (as in the impact of the control had to overcome the risk). We also categorized the gap analysis score into high, mid, low, and zero resources (as in many resources the organization needs to provide, to implement the control).

Many studies have typically given the highest priority recommendations to those with the highest gap values. However, in government entities with limited budgets, recommendations must be sorted based on how the organization can improve its information security posture with the smallest resources to reduce risks as much as possible.

Table 14 – Prioritized Recommendations

Controls	Ri	Rs	**Pr**	**Recommendations**
ID.IM-P8	High	Low	**1**	Formalize business process flows from work units into official guidelines, approved by all parties involved in the interconnection.
GV 5.1.1	High	Low	**1**	Implement a ticketing system for coordination and monitoring of information-sharing policies.
PR.PO-P10	High	Low	**1**	Establish policies ensuring vulnerabilities are tracked, fixed, and reported for continuous improvement.
PR 7.3.1	High	Low	**1**	Incorporate responsibilities in employee contracts, regularly monitor these in the interconnected system, and enhance workflow after employee departures.
ID.IM-P2	Mid	Low	**2**	Inventory parties and responsibilities in the interconnection and formalize them in official documents.
CT.DM-P7	High	Mid	**2**	Implement a policy to include usage permissions on sensitive information sent through APIs.
CT 8.1.3	High	Mid	**2**	Establish policies ensuring shared information management responsibilities, with logging capabilities for audit purposes.
CT 8.4.1	High	Mid	**2**	Improve the system hub to monitor data flow, adding tracking codes to shared information.
CM 13.2.1	Mid	Low	**2**	Adopt formal procedures based on industry standards for secure information exchange.
PR.AC-P1	High	Mid	**2**	Implement centralized credential policies like SSO for users and administrators, ensuring credentials follow industry standards in the SDLC.
PR.AC-P4	Mid	Low	**2**	Educate technical staff on information security principles such as least privilege and conduct regular security refreshers.
PR 7.1.1	High	Mid	**2**	Assess technical staff screening processes across interconnected organizations before granting access to sensitive data.
ID.DE-P3	Mid	Mid	**3**	Ensure comprehensive interconnection compliance policies with legal enforcement mechanisms.
GV 5.1.2	High	High	**3**	Review of information security policy and its implementation with quantitative monitoring, including organizational changes in interconnection.
CT 8.4.7	High	High	**3**	Implement policies and improve the system hub to monitor information flow between DJBK and external parties, adding tracking codes to identify when, from where, and to whom the information is shared.

PR.PO-P1	Mid	Mid	**3**	Aggressively enforce baseline system configuration standards pre-release.
PR.AC-P6	Mid	Mid	**3**	Expand policies to track interconnection system devices and limit access based on organizational missions.
PR.DS-P7	Low	Low	**3**	Secure sufficient budget for separate development servers for every organization's information systems.
ID 8.2.1	Mid	High	**4**	Develop interconnect data dictionary policy with data sensitivity level classification for information security.
GV 15.1.1	Low	Mid	**4**	Vendor and third-party security standards are included in IT contracts, supplementing Contracts and NDAs.
CM 18.1.6	Low	Mid	**4**	Create legal frameworks to address intentional or accidental sensitive information disclosures.
PR.PO-P7	Low	Mid	**4**	Draft IR, DR, and BCP documents for interconnection business processes and emphasize their importance to all parties involved.
GV 15.1.2	Low	High	**5**	Policies, monitoring systems, and understanding of parties in interconnected systems to ensure the identity of third parties and review of their work.
PR.PO-P2	Low	High	**5**	Develop procedures and give understanding to all the personnel to make configuration changes with the approval of all interconnection parties.

Ri = Risk Score; Rs = Resources requirements (based on *gap value*); Pr = Priority

Once all recommendations have been given a priority score as stated in Table 14, the organization must implement them according to their program and budget. The control recommendations are prioritized based on the criticality and likelihood of risks, ensuring that the organization can allocate resources effectively and address the most pressing security concerns. This study gave the organization 24 recommendations to address information security vulnerabilities, that mainly exist due to the nature of the interconnected systems/SoIS.

CONCLUSION

The findings of this research conclude that conventional security approaches are insufficient to address the dynamic and interdependent nature of interconnected systems (SoIS). The proposed framework mitigates these risks by providing prioritized control recommendations and a structured implementation plan to enhance the security and privacy of interconnected systems. The prioritization ensures that the most critical controls receive immediate attention, while other measures are integrated gradually based on resource availability and risk severity. This approach is particularly relevant in government settings, where budget constraints may limit the ability to address these risks comprehensively.

Acknowledgment

The authors would like to express their deepest gratitude to all those who contributed to completing this research. Special thanks are extended to the relevant government entities who provided valuable insights and data. We also acknowledge the support and guidance from BINUS University, particularly from the academic advisors, whose expertise and feedback were essential in shaping this study.

REFERENCES

[1] Bass, L., Clements, P., & Kazman, R. (2003). *Software Architecture In Practice*.

[2] Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. https://doi.org/10.1184/R1/6574790.V1

[3] Ceccarelli, A., Bondavalli, A., Froemel, B., Hoeftberger, O., & Kopetz, H. (2016). Basic Concepts on Systems of Systems. In A. Bondavalli, S. Bouchenak, & H. Kopetz (Eds.), *Cyber-Physical Systems of Systems: Foundations – A Conceptual Model and Some Derivations: The AMADEOS Legacy* (pp. 1–39). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-47590-5_1

[4] International Organization for Standardization. (2015). *ISO/IEC 27010:2015 Information technology—Security techniques—Information security management for inter-sector and inter-organizational communications*. Retrieved from https://www.iso.org/standard/68427.html

[5] Ionita, D. (2013, July 31). Current established risk assessment methodologies and tools [Info:eu-repo/semantics/masterThesis]. Retrieved August 21, 2024, from https://essay.utwente.nl/63830/

[6] Irsheid, A., Murad, A., AlNajdawi, M., & Qusef, A. (2022). Information security risk management models for cloud hosted systems: A comparative study. *Procedia Computer Science*, *204*, 205–217. https://doi.org/10.1016/j.procs.2022.08.025

[7] Ki-Aries, D., Faily, S., Dogan, H., & Williams, C. (2022). Assessing system of systems information security risk with OASoSIS. *Computers & Security*, *117*, 102690. https://doi.org/10.1016/j.cose.2022.102690

[8] Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information Security Risk Assessment. *Encyclopedia*, *1*(3), 602–617. https://doi.org/10.3390/encyclopedia1030050

[9] Lubbe, H., & Serfontein, R. (2023). A Framework for Information Security Risk Management from an Interoperability Perspective. In A. Gerber & M. Coetzee (Eds.), *South African Institute of Computer Scientists and Information Technologists* (pp. 165–179). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-39652-6_11

[10] National Institute of Standards and Technology. (2020). *NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0* (No. NIST CSWP 10; p. NIST CSWP 10). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.10

[11] Neto, V. V. G., Cavalcante, E., El Hachem, J., & Santos, D. S. (2017). On the Interplay of Business Process Modeling and Missions in Systems-of-Information Systems. *2017 IEEE/ACM Joint 5th International Workshop on Software Engineering for Systems-of-Systems and 11th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems (JSOS)*, 72–73. https://doi.org/10.1109/JSOS.2017.7

[12] Olivero, M. A., Bertolino, A., Dominguez-Mayo, F. J., Matteucci, I., & Escalona, M. J. (2022). A Delphi study to recognize and assess systems of systems vulnerabilities. *Information and Software Technology*, *146*, 106874. https://doi.org/10.1016/j.infsof.2022.106874

[13] Paniagua, C., Eliasson, J., & Delsing, J. (2019). Interoperability Mismatch Challenges in Heterogeneous SOA-based Systems. *2019 IEEE International Conference on Industrial Technology (ICIT)*, 788–793. https://doi.org/10.1109/ICIT.2019.8754991

[14] Rath, D. K., & Kumar, A. (2021). Information privacy concern at individual, group, organization and societal level—A literature review. *Vilakshan - XIMB Journal of Management*, *18*(2), 171–186. https://doi.org/10.1108/XJM-08-2020-0096

[15] Saleh, M., & Abel, M.-H. (2018). System of Information Systems to support learners (a case study at the University of Technology of Compiègne). *Behaviour & Information Technology*, *37*(10–11), 1097–1110. https://doi.org/10.1080/0144929X.2018.1502808

[16] Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14–30. https://doi.org/10.1016/j.cose.2015.11.001

[17] Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security*. Cengage Learning.