Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 3, June 2023, pp. 591-599

DOI: https://doi.org/10.52436/1.jutif.2023.4.3.978
p-ISSN: 2723-3863
e-ISSN: 2723-3871

INFORMATION SECURITY RISK MANAGEMENT DESIGN OF SUPERVISION MANAGEMENT INFORMATION SYSTEM AT XYZ MINISTRY USING NIST SP 800-30

Ricko Dwi Pambudi[*1], Kalamullah Ramli[2]

[1,2]Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia
Email: [1]ricko.dwi@ui.ac.id, [2]kalamullah.ramli@ui.ac.id,

(Article received: March 31, 2023; Revision: May 04, 2023; published: June 26, 2023)

Abstract

SIMWAS is an information system at the XYZ Ministry that is used to manage supervisory activities and follow up on supervisory results. SIMWAS is an important asset that contains all internal control business processes, but in practice, SIMWAS information security risks have not been managed properly. To overcome these problems, information security risk management is needed at SIMWAS. This study aims to design and analyze SIMWAS information security risk management using the NIST SP 800-30 framework. NIST SP 800-30 focuses on a particular infrastructure and its boundaries. Since the purpose is to perform a technical risk analysis of the core IT infrastructure, it is highly prescriptive. It has nine primary steps to conduct risk assessment. The NIST SP 800-30 framework is used to design and analyze SIMWAS information security risks by identifying threats, vulnerabilities, impacts, likelihoods, and recommendations for controls. SIMWAS information security risk assessment is carried out by analyzing data obtained from the results of interviews, observations, and document reviews. The results of this study show that SIMWAS information security has four low-level risks, eight moderate-level risks, and five high-level risks. Very low and low risk levels are acceptable according to the risk appetite of the business owner, but moderate, high, and very high-risk levels require risk avoidance, risk transfer and risk reduction. The XYZ Ministry need to carry out residual risk analysis and cost-benefit analysis from implementing controls in each risk scenarios.

Keywords: *Information Security, NIST SP 800-30, Risk Management, SIMWAS.*

1. INTRODUCTION

The widespread use of information technology opens up numerous opportunities for the automation of management procedures and an improvement in the effectiveness and quality of services delivered. Furthermore, the adoption of IT solutions in the public sector demonstrates the need for service realization security [1]. The XYZ Ministry has developed a Digital Indonesia Roadmap for 2021–2024, which covers four strategic sectors, including digital government [2]. It is designed to support and encourage efficient, effective, and transparent public services [3].

The use of information technology in administering government has been regulated in Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (EBGS) [4]. To support EBGS and its commitment as a trusted advisory and strategic partner to all related partners, the Inspectorate General of the XYZ Ministry carried out the development of the digitalization of supervision by establishing the Inspector General's Decree No. 11 of 2022 concerning the Grand Design of XYZ Ministry Supervision Digitization for the years 2022–2024 [5]. Efforts have been made to build an information system as a monitoring tool; one of these information systems is called the Supervision Management Information System (SIMWAS).

SIMWAS is an application to manage supervisory and supervisory support activities. SIMWAS consists of three modules: audit, TLHP, and e-SPJ. SIMWAS is an important asset for the Inspectorate General's business processes. The value of SIMWAS assets includes all internal control business processes and supervisory support, such as follow-up of internal and external inspection results to the budget accountability process.

Based on the Guidelines for the Secretariat General of the XYZ Ministry No. 01 of 2018 concerning the Information Technology Governance of the XYZ Ministry, it is necessary to apply risk management to the SIMWAS application [6]. In addition, Government Regulation Number 60 of 2008 concerning Government Internal Control Systems requires leaders of government agencies to exercise control over the implementation of information systems proportionally according to the size, complexity, and nature of their duties and functions [7].

Information systems are important assets for organizations, as are other assets that must be maintained and protected from various kinds of

threats and vulnerabilities [8], [9]. Information security risk management is necessary to safeguard this data and guarantee its confidentiality, integrity, and accessibility [10], [11]. Finding and implementing the proper security controls is crucial to sustaining effective security risk management [12]. SIMWAS is an important asset for the ongoing supervision process at the XYZ Ministry. Therefore, the information security of SIMWAS must be maintained in terms of the confidentiality, integrity, and availability of its data and services.

The Inspectorate General of the XYZ Ministry has developed a risk profile related to the organization using the main performance indicator approach. However, the Inspectorate General has not prepared a risk profile related to information security at the technical level of related information systems, such as the SIMWAS application. Based on the results of interviews with SIMWAS system managers, the initial development of SIMWAS has used the Software Development Life Cycle (SDLC) methodology. System development starts from the business process discussion phase through the user acceptance test (UAT) process and system security testing before the application is launched. However, in the operation and maintenance phase there is no control if changes occur while the program is running. The risk assessment in the operational phase has not been carried out by the SIMWAS owner. These conditions indicate that risk management has not been carried out for SIMWAS information security. Therefore, the confidentiality and integrity of data and the availability of SIMWAS services have the potential to be disrupted. Implementation of information security risk management is believed to be one of the efforts to ensure SIMWAS information security. The designed information security risk management is expected to be able to provide information security control recommendations according to the needs of the organization in handling risks based on the results of the assessment.

It is impossible to isolate this work from earlier research. Research on design information security risk management comes in many different forms. In 2018, the research entitled "Information Security Risk Management in the Ministry of Finance's Agency Level Financial Application System (SAKTI)" was conducted by E. Supristiowadi and Y. G. Sucahyo [13]. This study aims to design information security risk management at the SAKTI Ministry of Finance that can guarantee the availability of SAKTI services using ISO 27005, ISO 27002, NIST SP 800-30, NIST SP 800-26, and NIST SP 800-53. The research results include information security risk management, which includes the identification of vulnerabilities and threats as well as control strategies that must be implemented to mitigate risks.

Another research study entitled "Risk Assessment Using NIST SP 800-30 Rev. 1 and ISO 27005 Combination Technique in Profit-Based Organizations: A Case Study of ZZZ Information System Application in ABC Agency" was conducted by Al Fikri et al [14]. The research focuses on assessing information security risks for an application by applying a combination of ISO/IEC 27005 and NIST SP 800-30 techniques to a profit-oriented organization, namely ABC Agency. This study shows that risk assessment with this combination technique can be used in non-profit organizations by providing a detailed explanation of the steps involved in using this combination technique.

Izatri et al. in 2020 researched risk assessment using NIST SP 800-30 at the Gresik Regional Library [15]. Natural disasters, HR, and technological risk categories were among those identified inside the organization. By installing generators and servers, the greatest risk assessment can be mitigated. The three stages of the NIST SP 800:30 framework include risk analysis, risk determination, and recommendations for risk prevention.

Then, in 2021, L. C. Vynda et al conducted research-related information risk management analysis at the Institute for Agricultural Technology Assessment using the NIST SP 800-30 method [16]. The result is the risk management of the BPTP Lampung information system, which has ten associated risks, and recommendations to reduce the impact of the risks that occur.

In 2022, M. S. Hardani and K. Ramli [17] conducted research entitled "Design of Security Risk Management Information Systems Resources and Equipment Management of Post and Information Technology (SIMS) Using the NIST 800-30 Method." In this research, the design and analysis of SIMS risk management were compiled using the NIST 800-30 framework. The research resulted in the identification, mitigation, and evaluation of existing risks, as well as recommendations for the necessary controls for SIMS.

The main purpose of this study is to design information security risk management for SIMWAS. The framework chosen for this study was NIST SP 800-30 [18] because it has advantages over other frameworks, including details in conducting assessments and providing good and broad control recommendations. In comparison to other frameworks, NIST SP 800-30 focuses on a particular infrastructure and its boundaries. Since the purpose is to perform a technical risk analysis of the core IT infrastructure, it is highly prescriptive. In addition, NIST is able to integrate risk analysis into every part of the SDLC. Based on the NIST SP 800-30 framework, SIMWAS information security risk management resulted in 17 risks with 4 low-risk levels, 8 moderate risk levels, and 5 high-risk levels. The remaining sections of this study are organized as follows: The introduction is explained in Section 1. Research methodologies are presented in Section 2. The results and analysis of the study are presented in Section 3. The discussion is explained in Section 4.

The conclusion of the study and future work are explained in Section 5.

2. RESEARCH METHODS

This section presents the research design, research flow, and methods of collecting and processing data from research instruments. This research flow was carried out by reviewing literature studies, interviewing organizational staff, and collecting the required data. Then an analysis is carried out to evaluate and improve the security of information systems in organizations by implementing information security risk management.

2.1. Research flow

The research flow begins with problem identification, literature study, data collection, information security risk management design, and conclusions. The NIST SP 800-30 framework was used in this research's development of information security risk management for SIMWAS. The research process in this work can be broadly summarized in Figure 1.

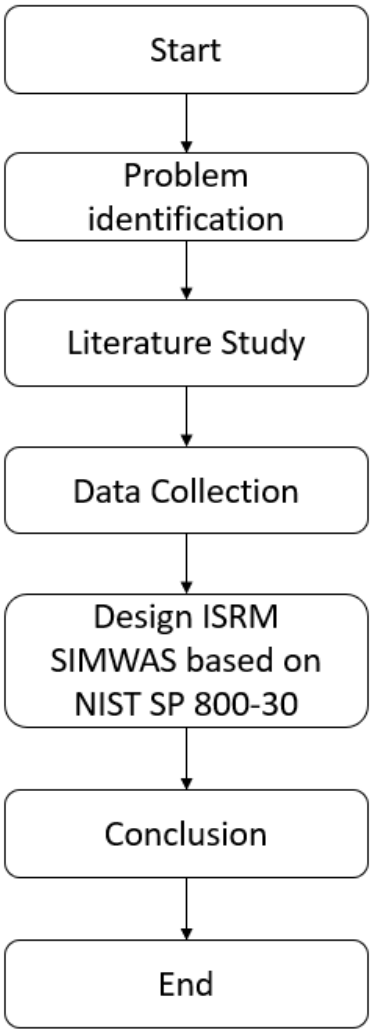

Figure 1. Research Methodology

The research begins with identifying the problem, conducting a literature study, data collection, design information security risk management based on NIST SP 800-30, and conclusions. Explanation of each stage of the research is explained in the following sub-chapter.

2.2. Problem Identification

The absence of information security risk management within the organization prompted the authors to identify problems based on available information, which led to the problem statement that the organization did not have SIMWAS information security risk management.

2.3. Literature Study

This section conducts a literature review based on several existing theories and approaches. A literature study was carried out on information security, risk management, the information security risk management framework, previous research, and related regulations.

2.4. Data Collection

This study relied on qualitative data collection methods. Qualitative research methods aim to analyze and describe phenomena or research objects through the social activities, attitudes, and perceptions of people individually or in groups.

This study uses two types of data, namely primary data and secondary data. Primary data is data that comes directly from the source, such as data from interviews, observations, and questionnaires [19]. Interviews are one-on-one or group interactions conducted over the phone, in person, or via a conference call [20]. Secondary data is information derived from literature studies, books, organizational policies, and documents.

2.5. Design Information Security Risk Management

This section presents the design of information security risk management based on NIST SP 800-30. NIST SP 800-30 is a Risk Management Guide for Information Technology System published by the National Institute of Standards and Technology. The risk assessment methodology encompasses nine primary steps. The NIST SP 800-30 risk assessment can be carried out by conducting questionnaires or interviews with system managers, reviewing documents, and using automated scanning tools. This stage produces risk identification and risk assessment. Based on the NIST 800-30 framework, there are several stages of risk assessment, as shown in Figure 2 [18].

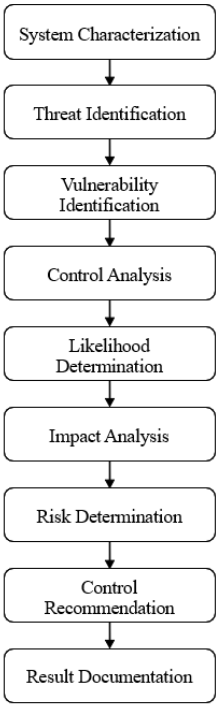

Figure 2. NIST SP 800-30 flowchart

The explanation of Figure 2 is as follows:

1. System Characterization

At this stage, the boundaries of the IT system are identified, along with the assets configuring the system. System characteristic components for information systems include hardware, software, network equipment, data, and information.

2. Threat Identification

In this phase, the potential threats to the information system under evaluation are identified. Any condition or event that has the potential to damage the information system is the threat's source. Threats could originate from humans, equipment, and nature.

3. Vulnerability Identification

This vulnerability identification aims to idetify system vulnerabilities (flaws or weaknesses) that can be exploited by potential threat sources.

4. Control Analysis

This step aims to analyze the controls that have been implemented by the organization to minimize potential threats and possible system vulnerabilities.

5. Likelihood Determination

To obtain an overall likelihood rating of the potential vulnerabilities that can be carried out within the potential threat.

6. Impact Analysis

The next step in measuring the level of risk is to determine the adverse impact that results from the successful exploitation of a threat from a vulnerability.

7. Risk Determination

Risk determination aims to assess the level of risk to information systems.

8. Control Recommendation

The control recommendations are the outcomes of the risk assessment process and provide input to the risk mitigation process, which evaluates, prioritizes, and implements the suggested procedural and technological security controls.

9. Result Documentaion

The final step is documenting the results in the form of reports or official organizational documents.

3. RESULT

The analysis in this study focuses on the process of implementing risk strategies utilizing the NIST SP 800-30 framework and providing recommendations based on the results of the risk findings.

3.1. System Characterization

The initial risk assessment begins with identifying the existence of information technology systems and the assets within them. The SIMWAS system was built, developed, and maintained by the Inspectorate General of the XYZ Ministry. SIMWAS' infrastructure and network were provided by the Center for Data and Information Facilities of the XYZ Ministry.

Table 1. Threat Identification

No	Threat Sources	Motivation	Threat Action
1	Insiders	Curiosity, Ego, Intelligence, Monetary Gain, Revenge Unintentional errors, and omissions	Computer abuse, system sabotage, system instruction, unauthorized system access, sale of personal information, wrong data input, data theft
2	Hacker, cracker	Monetary Gain, Challenge Ego, Rebellion	Hacking, social engineering, DoS, malware, system intrusion, break-ins, unauthorized system access
3	Terrorist	Blackmail, Destruction, Exploitation, Revenge	Bomb/terrorism, information warfare, DDoS, System penetration, System tampering
4	Network	Retrieving data	Man in the middle (MITM), failure of the information system network connection
5	Storage Device	-	Disk error, disk full
6	IT Equipment	-	Server failure (down/crash), data backup failure, OS update failure, outdated technology
7	Power Supply	-	Loss of power supply, UPS battery is damaged
8	Natural disaster	-	Fire, earthquake, flood

System characteristic components for information systems include hardware, software, network equipment, data, and information. SIMWAS servers run the Apache web server, MySQL, and the standard PHP program.

3.2. Threat Identification

From the results of the observations, several threats were identified. Table 1 displays the results in the following way.

Table 1 shows the identified threats consisting of 8 threat sources. Insiders, hacker, cracker, and terrorist are threats come from human. Network, storage device, IT equipment, power supply are threats from equipment. Natural disasters are threats come from nature.

3.3. Vulnerability Identification

Vulnerability identification cannot be separated from threat analysis in evaluating IT systems. It identifies vulnerabilities or weaknesses that could be exploited by a threat actor to disrupt the current IT system. Nessus, a penetration testing tool (pentest), is needed for discovering vulnerabilities in SIMWAS. The pentest approach is used to simulate the outcomes of potential attacks by attackers on current IT systems to identify any vulnerabilities in these systems. Table 2 displays the vulnerability identification results.

Table 2. Vulnerability Identification using Nessus

No	Vulnerability	Nessus Level	Description
1	Apache 2.4.x < 2.4.46 vulnerability 2.4.46 advisory	Critical	Apache httpd installed on the remote host is before 2.4.46. It is vulnerable to CVE-2020-11984, CVE-2020-11993, and CVE-2020-9490.
2	Apache 2.4.x < 2.4.47 Vulnerability in 2.4.47 changelog	Critical	The Apache httpd version is before 2.4.47. It is vulnerable to CVE-2021-30641, CVE-2020-35452, CVE-2021-26690, CVE-2020-13950, CVE-2020-13938, and CVE-2019-17567.
3	Apache 2.4.x < 2.4.52 Vulnerability Buffer Overflow	Critical	Apache's httpd version is before 2.4.52. It is vulnerable to mod_lua. It can cause a buffer overflow in the mod_lua multipart parser.
4	Apache 2.4.x < 2.4.53 Vulnerabilities in 2.4.53 advisory	Critical	The Apache httpd version is before 2.4.53. It is vulnerable to CVE-2022-22719, CVE-2022-22720, CVE-2022-22721, and CVE-2022-23943.
5	Apache 2.4.x < 2.4.54 Vulnerabilities in 2.4.54 advisory	Critical	The Apache version is before 2.4.54. It is vulnerable to CVE-2022-26377, CVE-2022-28330, CVE-2022-28614, CVE-2022-28615, CVE-2022-29404, CVE-2022-30522, CVE-2022-30556, and CVE-2022-31813.
6	DoS / SSRF	Critical	A crafted URI submitted to httpd configured as a forward proxy (ProxyRequests on) might cause a crash (NULL pointer dereference) or allow requests to be forwarded to a defined Unix Domain Socket endpoint in configurations that mix forward and reverse proxy declarations (SSRF).
7	Apache < 2.4.49 Vulnerabilities in 2.4.49 changelog	Critical	The web server was affected by vulnerability CVE-2021-40438.
8	Apache < 2.4.49 Multiple Vulnerabilities in 2.4.49 changelog	Critical	The Apache httpd version is before 2.4.49. It is affected by vulnerabilities in CVE-2021-39275 and CVE-2021-34798.
9	Apache >= 2.4.17 < 2.4.49 Vulnerability mod_http2	High	The Apache httpd version is greater than 2.4.17 and before 2.4.49. It is vulnerable to mod_proxy which led to request cache poisoning.
10	Apache >= 2.4.30 < 2.4.49 Vulnerability mod_proxy_uwsgi	High	Apache httpd version is greater than 2.4.30 and is before 2.4.49. It is affected by a vulnerability as mod_proxy_uwsgiand can cause a crash (DoS).
11	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	High	It is affected by SWEET32. The SWEET32 attack is an SSL/TLS vulnerability that allows an attacker to compromise HTTPS connections using a 64-bit block cipher.
12	SSL Medium Strength Cipher Suites Supported (SWEET32)	High	The application of SSL ciphers with a middling level of encryption. Any encryption that employs the 3DES encryption suite or at least key lengths of at least 64 bits but not more than 112 bits is considered medium strength by Nessus.

According to Table 2, Nessus has identified 12 system vulnerabilities consisting of 8 critical and 4 high based on the Nessus level.

3.4. Control Analysis

At this stage, the control analysis of SIMWAS is carried out by the Center for Data and Information Facilities of the XYZ Ministry as an infrastructure and network provider.

3.5. Likelihood Determination

The likelihood determination step determines how likely it is that threats will exploit SIMWAS vulnerabilities, failing SIMWAS services. The likelihood of a risk occurring can be divided into five levels. Table 3 is a description of the criteria for determining the level of likelihood in the organization.

Table 3. Likelihood criteria

Level	Likelihood Criteria	
	Occurrence Frequency	**Possible Potential Occurrence**
Very low (1)	Very rare Only occurs in very abnormal conditions or occurs once every 3 years.	This only happens occasionally. Likely to occur over a long period (more than 5 years)
Low (2)	Rarely occurs. occurs outside of normal conditions or occurs intermittently within 3 years.	It occurs only in conditions out of habit; the possibility of happening is small. Occurs over a long period (less than 5 years)
Moderate (3)	Quite often Events occur regularly and under normal circumstances.	Quite likely to occur in various conditions. Occurs between 1 and 3 years.
High (4)	Often The occurrences are quite frequent, occurring between 6 and 15 times per year under normal conditions.	Most likely to occur under various normal conditions Occurs within a specific time frame (between 3 and 12 months)
Very high (5)	Very often It always occurs in every incident between 3 and 5 times every month.	It must happen all the time under various normal conditions. Occurs in a very short period (less than 3 months) for unusual events

Table 3 showed that the level of likelihood consist of very high, high, moderate, low, and very low. The criteria of likelihood are occurrence frequency and possible potential occurrence.

3.6. Impact Analysis

After determining the likelihood of the occurrence of a risk, the impact analysis is carried out. The risk impact demonstrates the extent to which threats that take advantage of SIMWAS's vulnerabilities have an effect. If a risk is documented, the level of impact is a measurement of the potential impact that could result from that risk. Table 4 shows the criteria for determining the impact level.

According to Table 4, the level of impact consists of very high, high, moderate, low, and very low. Impact criteria are based on potential impact resulted in performance, operational, and finance.

Table 4. Impact Criteria

Level	Impact Criteria		
	Performance	**Operational**	**Finance**
Very low (1)	Interruption 1-2 days	Minor disturbance	Losses up to IDR 5 million
Low (2)	Interruptions up to a week	Performance drops by 20 to 40%	Loss IDR 5 million to 10 million
Moderate (3)	Interruption of 1- 2 weeks	Performance drops from 40 to 60%	Loss IDR 10 million to 25 million
High (4)	Interruptions up to a month	Performance drops from 60% to 80%	Loss IDR 25 million to 50 million
Very high (5)	Interruptions > 1 month	Performance drops >80%	Loss > IDR 50 million

3.7. Risk Determination

The likelihood level multiplied by the severity of the impact can be used to get the risk value. The risk matrix is shown in Table 5.

Table 5. Risk Assessment Matrix

Risk Matrix		Impact				
		1	**2**	**3**	**4**	**5**
Likelihood	1	VL	VL	L	L	M
	2	VL	L	M	M	M
	3	L	M	M	H	H
	4	L	M	H	H	VH
	5	M	M	H	VH	VH

Table 6. Risk Assessment

Risk	Likelihood	Impact	Risk Level	Risk Code
Server down	1	5	Moderate	R1
Data loss	3	5	High	R2
Malware attack	4	3	High	R3
Power loss	2	3	Moderate	R4
Flood	1	4	Low	R5
Fire	1	4	Low	R6
Earthquake	1	4	Low	R7
Wrong data input	1	3	Low	R8
Unauthorized system access	2	5	Moderate	R9
Sensitive Data Exposure	3	4	High	R10
MITM	2	5	Moderate	R11
Remote DoS	5	2	Moderate	R12
Remote Code Execution (RCE)	4	2	Moderate	R13
DDoS attack	5	2	Moderate	R14
SWEET32 attack	4	3	High	R15
Network Sniffing	2	4	Moderate	R16
Data breach (Social Engineering)	4	4	High	R17

According to Table 5, a risk score of less than 2 is considered very low (VL) risk, a risk value of 3 to 4 is considered low (L) risk, a risk value of 6 to 11 is considered moderate (M) risk, a risk value of 12 to 19 is considered high (H) risk, and a risk value of 20 to 25 is considered very high (VH) risk. Accepting risk is appropriate for very low and low-risk levels, but risks with moderate to very high levels must be addressed to reduce the level of risk.

The next step is assessing the identified risk to determine the risk level. The risk assessment is shown in Table 6.

Table 6 showed that risk assessment of SIMWAS has 17 risks, consisting four low-level risks, eight moderate-level risks, and five high-level risks.

3.8. Control Recommendation

The goal of this step is to reduce SIMWAS's risk level. Making control recommendations is important after performing a risk assessment with five risk categories and risk values ranging from 1 to 25. The control recommendation for the organization is displayed in Table 7.

Table 7. Control Recommendation

Risk Code	Control Recommendation
R1	Simulation training by conducting a switch over to DRC or another site backup.
R2	Perform regular server backups
R3	Automatically update antivirus patches
R4	Check the UPS and generator periodically
R5	Place the server in the building on the top floor
R6	Provide fire extinguishers around the server room
R7	Conduct regular training for employees who have SIMWAS users
R8	Protect the server room building by earthquake resistant devices
R9	Organizations enforce a maximum number of account sessions at one time
R10	Strengthening encryption data at rest and in transit, disabling caching for sensitive data
R11	Disable SSL 2.0 and SSL 3.0 and use TLS 1.2 (or higher)
R12	Update the Apache HTTP Server to the most recent version.
R13	Update the Apache to the most recent version.
R14	Upgrade WAF and anti-DDoS regularly
R15	Reconfigure the SSL/TLS servers impacted to remove support for obsolete 64-bit block ciphers.
R16	Conduct network monitoring for unusual activity continuously
R17	Conduct security awareness training. Multi-Factor Authentication

The SIMWAS information security risk control recommendations as shown in Table 7 can be classified into technical controls and non-technical controls. The technical controls are R2, R3, R4, R5, R6, R8, R9, R10, R11, R12, R13, R14, R15. Non-technical controls in the form of security awareness training, simulation training and improving network security monitoring.

3.9. Result Documentation

The results of the risk assessment analysis from SIMWAS are documented in the final step. To build risk management, documentation that covers vulnerabilities, threats, risk assessment, and control recommendations for the risks present in SIMWAS must be completed.

The SIMWAS risk profile may be displayed in Figure 3 once the organization has decided on an acceptable risk level.

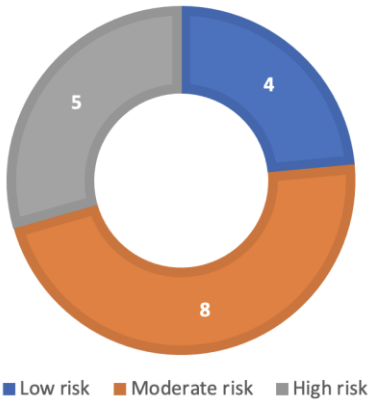

Figure 3. SIMWAS Risk Profile

The results of this study show that SIMWAS information security has four low-level risks, eight moderate-level risks, and five high-level risks.

4. DISCUSSION

SIMWAS is a very important asset for XYZ ministry, and it is necessary to implement risk management to guarantee the information security of SIMWAS. This study used the NIST SP 800-30 framework, which provides a detailed explanation of the steps to conduct the information security risk management process. The NIST SP 800-30 framework can be used at the operational and technical levels and is appropriate for non-profit organizations.

After the results of the risk assessment are documented, the results are validated by conducting interviews with the business owner and internal experts within the organization to obtain certainty about whether the results of the study are accepted by the organization. The results of interviews with business owners and experts constitute data validation which includes results of threat identification, vulnerability identification, risk assessment results, and selection of control recommendations. From the results it is known that all the risks obtained are in accordance with the existing operational system. For risk control recommendations to help solve problems and become

space for the SIMWAS system to develop in current conditions. The feedback justifies that the business owner has accepted the results of the design that was made in this study. The business owner accepts to implement the control recommendations provided.

Information security risk management of SIMWAS resulted in 17 risks, consisting of 12 risks from human threats, 3 risks from natural threats, and 2 risks from equipment. Humans are potentially harmful threat sources due to their motivation and ability to obtain the resources necessary for an attack. If the research results are mapped into the information security component, the greatest risk lies in the aspects of availability and confidentiality. Furthermore, if it is mapped into the information technology infrastructure domains [21], the biggest risks are in the user domain, system/application domain, and computers used by application administrators (workstation domains). Risk control recommendations are necessary to mitigate the risk. From the risk scenarios that have been identified, the organization can take steps to reduce the level of impact or the likelihood of an incident occurring. This study provides 17 control recommendations and treatment plans as in Table 7 that can be used as a guide for organizations to deal with existing risks. There are 14 technical control and 3 non technical control which need to be implemented. Five high risks are top priority for immediate implementation of security controls. Then, eight moderate risks become the next priority, where the application of security controls can be carried out in stages. Furthermore, four low risks are other priorities that must be decided whether improvement is still needed or accepts the risk. In addition, risk assessment can be evaluated periodically to see the effectiveness of the implementation of controls that have been implemented by the organization. For this reason, the Inspectorate General of the XYZ Ministry needs to form a SIMWAS Information Security Risk Management Team to carry out information security risk management activities so that they always take lessons learned from the results of information security risk management.

This research has the impact of helping the Inspectorate General of the Ministry of XYZ as a risk owner unit to improve information security in accordance with the duties and functions as an electronic system operator by implementing a risk management process based on the NIST SP 800-30 standard. SIMWAS information security risk management that has been designed is expected to be adopted by other agencies that have similar characteristics.

5. CONCLUSION

SIMWAS requires information security risk management to maintain the sustainability of internal control business processes. In this study, the information security risk management of SIMWAS was conducted based on the NIST SP 800-30 framework.

According to the process of identifying and assessing the information security risk of SIMWAS, it can be concluded that SIMWAS information security has 17 risks. The results of this study show that SIMWAS information security has four low-level risks, eight moderate-level risks, and five high-level risks.

The results of this study are expected to assist organizations in managing and maintaining SIMWAS information security. Control recommendations for identified risks are given to reduce the impact of information security risks on SIMWAS.

The limitations in this study can be used as developments in further research, such as the need to carry out residual risk analysis and cost-benefit analysis from implementing controls in each risk scenario and drafting a contingency plan for SIMWAS as part of risk mitigation.

ACKNOWLEDGEMENTS

The publication of this research is funded by the Ministry of Communication and Information Technology of the Republic of Indonesia.

REFERENCES

[1] E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, "Information security assessment in public administration," *Comput Secur*, vol. 90, Mar. 2020, doi: 10.1016/j.cose.2019.101709.

[2] XYZ Ministry, *XYZ Ministerial Regulation Number 2 of 2021 concerning the XYZ Ministry Strategic Plan for 2020-2024*. 2021.

[3] H. Rochmansjah, "Application of Good Governance Principles in Government: Perspective of Public Services," 2019. [Online]. Available: http://ijsoc.goacademica.com

[4] Presidential Regulation, *Regulation of The President of The Republic of Indonesia Number 95 of 2018 Concerning Electronic-Based Government Systems*. 2018.

[5] Inspector General of the XYZ Ministry, *Decree of the Inspector General number 11 of 2022 concerning the Grand Design of Digitizing Supervision of the XYZ Ministry for the 2022-2024 Fiscal Year*. 2022.

[6] Secretary General of the XYZ Ministry, *Guidelines for the Secretary General of the XYZ Ministry Number 01 concerning Information Technology Governance of the XYZ Ministry*. 2018.

[7] Presiden Republik Indonesia, *Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah*.

2008.

[8] E. Bergström, M. Lundgren, and Å. Ericson, "Revisiting information security risk management challenges: a practice perspective," *Information and Computer Security*, vol. 27, no. 3, pp. 358–372, Jun. 2019, doi: 10.1108/ICS-09-2018-0106.

[9] Evan Wheeler, *Security Risk Management Building an Information Security Risk Management Program from the Ground Up*. USA: Syngress, 2011.

[10] H. I. Kure and S. Islam, "Assets focus risk management framework for critical infrastructure cybersecurity risk management," *IET Cyber-Physical Systems: Theory & Applications*, vol. 4, no. 4, pp. 332–340, Dec. 2019, doi: 10.1049/iet-cps.2018.5079.

[11] E. J. Wibowo and K. Ramli, "Impact of Implementation of Information Security Risk Management and Security Controls on Cyber Security Maturity (A Case Study at Data Management Applications of XYZ Institute)," *Journal of Information System)*, vol. 18, no. 2, pp. 1–17, 2022, doi: https://doi.org/10.21609/jsi.v18i2.1146.

[12] J. Payette, E. Anegbe, E. Caceres, and S. Muegge, "Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects," 2015. [Online]. Available: www.timreview.ca

[13] E. Supristiowadi and Y. G. Sucahyo, "Manajemen Risiko Keamanan Informasi Pada Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI) Kementerian Keuangan," *INDONESIAN TREASURY REVIEW*, vol. 3, no. 1, pp. 23–33, 2018, doi: https://doi.org/10.33105/itrev.v3i1.20.

[14] M. al Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, "Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency," in *Procedia Computer Science*, Elsevier B.V., 2019, pp. 1206–1215. doi: 10.1016/j.procs.2019.11.234.

[15] DI. Izatri, NI. Rohmah, and RS. Dewi, "Identifikasi Risiko pada Perpustakaan Daerah Gresik dengan NIST SP 800-30," *Jurnal Riset Komputer*, vol. 7, no. 1, pp. 50–55, 2020.

[16] V. Levy Cahyani, Aristoteles, A. Yani, and Tristiyanto, "Analisis Manajemen Risiko Sistem Informasi Balai Pengkajian Teknologi Pertanian Lampung Menggunakan Metode NIST SP 800-30," *Jurnal Pepadun*, vol. 2, no. 1, pp. 13–20, 2021, doi: https://doi.org/10.23960/pepadun.v2i1.21.

[17] M. S. Hardani and K. Ramli, "Perancangan Manajemen Risiko Keamanan Sistem Informasi Manajemen Sumber Daya dan Perangkat Pos dan Informatika (SIMS) Menggunakan Metode NIST 800-30," *JURIKOM (Jurnal Riset Komputer)*, vol. 9, no. 3, p. 591, Jun. 2022, doi: 10.30865/jurikom.v9i3.4181.

[18] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology."

[19] J. W. Creswell and J. D. Creswell, *Research Design Qualitative, Quantitative, and Mixed Methods Approaches*, Fifth. Sage Publication, Inc, 2018.

[20] J. Recker, *Scientific Research in Information Systems A Beginner's Guide Second Edition*. Springer, 2021. doi: https://doi.org/10.1007/978-3-030-85436-2.

[21] D. Gibson and A. Igonor, *Managing Risk in Information Systems Third Edition*. Jones & Bartlett Learning, 2022.