Journal of Emerging Information System and Business Intelligence
ISSN: 2774-3993
Journal homepage: https://ejournal.unesa.ac.id/index.php/JEISBI/

IT Risk Management Planning on Avesina Application RSUD Waluyo Jati Kab. Probolinggo Using OCTAVE Allegro

Safaru Khoiron Jamil[1], Ghea Sekar Palupi [2]
[1,2]*State University of Surabaya, Surabaya, Indonesia*
[1]safarukhoiron.20083@mhs.unesa.ac.id , [2]gheapalupi@unesa.ac.id

ABSTRACT

The application of information technology at RSUD Waluyo Jati Kraksan can pose a risk. The example of information technology risks that have occurred is the occurrence of additional working hours caused by system errors in the Avesina application related to room procurement. The purpose of this study is to determine the IT risks that arise from the implementation of the Avesina application, and provide the necessary mitigation in managing these risks. The method used in this research is OCTAVE Allegro. Before determining the risk, asset profiling and wadan of the asset are carried out. The risks arising from the implementation of the avesina application are data input errors, application hacking, applications can be easily accessed by unauthorized people, and account sharing. There are several stages used to determine the mitigation approach. Of the four risks, it was found that only two risks needed to be mitigated. The mitigation provided focuses on the asset containers that need to be controlled, namely the SIM RS Unit and management. The mitigation includes procuring a renewable security system, procuring a 2-factor authentication system, and monitoring compliance with information technology.

Keyword: RSUD Waluyo Jati Kab. Probolinggo, Hospital SIM Unit, Avesina Application, Risk Management, OCTAVE Allegro

Article Info:
Article history:
Received December 05, 2024
Revised March 25, 2025
Accepted March 29, 2025

Corresponding Author
Safaru Khoiron Jamil
State University of Surabaya, Surabaya, Indonesia
safarukhoiron.20083@mhs.unesa.ac.id

1. INTRODUCTION

Information technology utilized in companies/agencies is important and inseparable from their business processes [1]. Companies/agencies using information technology can support business processes, but under certain conditions it can cause unwanted risks [2]. One of these companies/agencies is a hospital. However, the application of information technology can also pose a risk to the company/agency [3].

Risk is an uncertain condition, can occur at any time, and can cause losses [4]. Risks can come from several sources, such as the environment, planning, geopolitics, economic conditions, and natural disasters [5]. Information technology risk is the potential for implementation failure so that it can disrupt business processes which include utilization, development, operation, and maintenance [6]. The impact if information technology risk is not managed properly can hinder business processes, so it can cause losses [7]. IT risk management is the process of identifying, assessing, and controlling risks associated with a company's IT assets to reduce the impact of risks on the company/agency's business areas [8].

RSUD Waluyo Jati Probolinggo Regency is one of the hospitals owned by the Probolinggo Regency Government. At this time, RSUD Waluyo Jati Probolinggo has implemented information technology used in the electronic medical record process. The application used in electronic medical records is Avesina. This application is used by all medical personnel and para-medical personnel to assist in examining and recording actions both giving drugs and any therapy that has been given to patients.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a method used to identify and evaluate information security risks. OCTAVE Allegro can increase security on information assets owned by companies/agencies [9]. OCTAVE Allegro focuses on Information Assets. These information assets do not only focus on one type, but can cover all areas of assets owned by the agency/company [10]. OCTAVE Allegro also pays attention to the environment of these assets, both in terms of technical, physical, and management [11]. OCTAVE Allegro also pays attention to the external environment of the company that intersects with information assets [12]. Then, the obstacles that have occurred during the implementation of Avesina are the addition of erratic working hours so that it can reduce the focus and psychology of human resources, so that it can cause errors in data input. The obstacles that have occurred are in accordance with the impact areas in OCTAVE Allegro.

From the background above, risk management planning is needed to find out what risks arise and what mitigation needs to be done. This research aims to provide an overview of what risks arise and what actions need to be taken so as not to interfere with existing business processes.

2. METHODS

Research methodology is a series of stages that will be used to carry out research [13]. The research methodology used will be used to solve the problems that arise in the problem formulation. This research method uses OCTAVE Allegro.

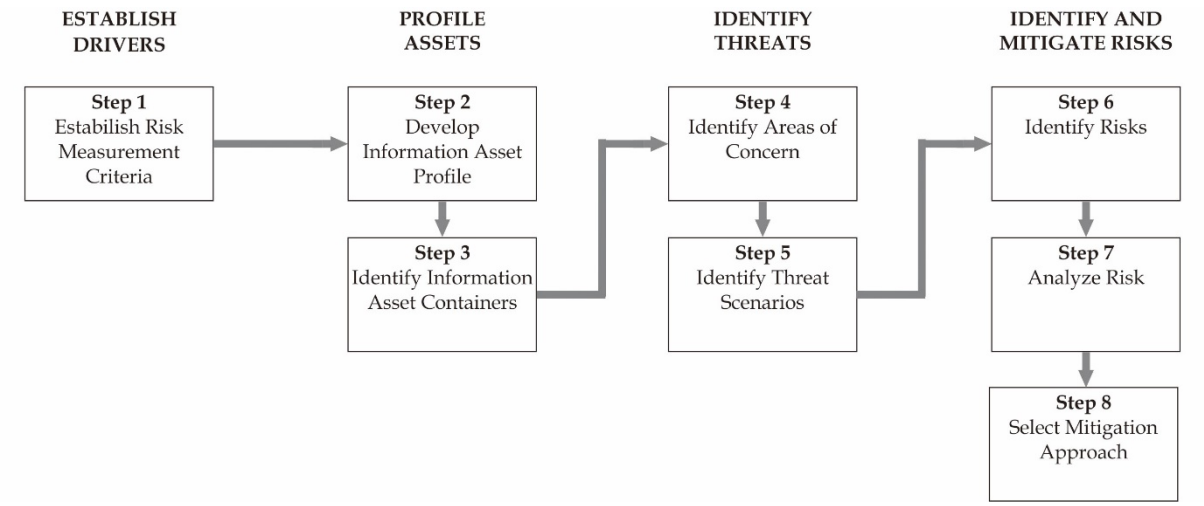

Figure 1. OCTAVE Allegro Method

2.1 Establish Risk Measurement Criteria

Establishing risk measurement criteria that will be used consistently and accurately can provide a definitive picture of decisions related to risk mitigation. These decisions must cover all information assets and divisions. This step also evaluates the extent of the impact on certain areas, and recognizes the most significant areas of impact on the vision and mission.

2.2 Developing an Information Asset Profile

An asset profile is a description of the representation of the asset itself, in terms of its features, qualities, characteristics, and unique values. The asset profiling process will clearly and consistently describe the asset's boundaries and adequately defined security requirements.

2.3 Identifying Information Asset Containers

A container is a place where assets are stored, transported, and processed. The container can be something that is outside the control of the company/agency, such as external parties (government, partners and service providers). The risks associated with the container are inherited from the information asset itself.

2.4 Identifying Areas of Concern

The risk identification process is carried out by brainstorming related to conditions/situations that can threaten assets. The purpose of this step is to make it easier for the analyst team to quickly describe the threat situation or condition. There are areas that will be of concern based on the characteristics of the threat and its operating conditions.

2.5 Identifying Threat Scenarios

This step expands the areas of concern in the previous step into scenarios that better characterize the nature of the threat. This step also provides an opportunity to consider the probability of threat scenarios. The results of the probability consideration can make it easier for companies/agencies to determine possible scenarios based on their operating conditions.

2.6 Identifying Risks

This step will identify the threat scenarios that have been obtained previously and find out the consequences that will occur. The activities in this step will provide certainty about the consequences that will arise if the risk occurs.

2.7 Analyzing Risk

In this step an assessment is made relating to the extent to which the company/agency if affected by the risk. The assessment that will arise considers the extent to which the company/agency is able to accept the consequences of the impact of a risk.

2.8 Selection of Mitigation Approach

In this step the company/agency determines the mitigation required and develops a mitigation strategy against the results of the identification of the previous risks. The mitigation strategy is developed by considering the asset based on its value, security requirements, container, and operating environment.

3. RESULTS AND DISCUSSION

This research was conducted with a discussion with the SIM RS Unit of RSUD Waluyo Jati Kab. Probolinggo. The SIM RS Unit is the unit responsible for managing information assets at RSUD Waluyo Jati Kab. Probolinggo. In addition, discussions were also held with the finance department and the assurance department in determining the affected areas in the first step.

3.1 Establish Risk Measurement Criteria

In determining risk measurement criteria, several discussions were held with the assurance department, the finance department and the hospital SIM unit. The results of the discussion obtained with the assurance department are as follows:

Table 1. Allegro Worksheet 5

Allegro Worksheet 5	**RISK MEASUREMENT CRITERIA LEGAL SANCTIONS**		
Affected Area	Low	Medium	High
Lawsuits	Non-frivolous lawsuits or lawsuits of less than IDR 15,000 are filed against the organization, or frivolous lawsuits filed against the organization	Non-meritorious suits or lawsuits between IDR 15,000 and IDR 500 million filed against the organization	Non-meritorious lawsuits or lawsuits greater than IDR 500 million filed against the organization
Integrity	No inquiries from the government or other investigative organizations	Government or other investigative organization requests information or records (low profile)	The government or other investigative organization initiates a very in-depth investigation into the organization's practices

Then the results of the discussion obtained with the finance department are as follows:

Table 2. Allegro Worksheet 2

Allegro Worksheet 2	**FINANCIAL RISK MEASUREMENT CRITERIA**		
Area Affected	Low	Medium	High
Operational Costs	Less than 20% increase in annual operating expenses	Annual operating costs increased by 20 to 90%	Annual operating costs increased by more than 90%
Revenue Loss	Less than 5% annual loss of opinion	Less than 5% annual loss of opinion	Greater than 20% loss of annual income
Kerugian Finansial Satu Kali	One-time financial cost less than IDR 500,000	One-time financial cost of IDR 500,000 to IDR 4M	One-time financial cost greater than IDR 4M

And the results obtained from discussions with the SIM RS Unit are as follows:

Table 3. Allegro Worksheet 1

Allegro Worksheet 1	**REPUTATION RISK AND CUSTOMER TRUST MEASUREMENT CRITERIA**		
Affected Area	Low	Medium	High
Reputation	Reputation is less affected, little or no effort/cost required to recover	Reputation is damaged, and it takes effort and money to restore it	Reputation is destroyed or damaged and cannot be restored
Customer Losses	Less than 5% customer attrition due to loss of trust	5 to 20% customer attrition due to loss of trust	More than 20% customer attrition due to loss of trust

Table 4. Allegro Worksheet 3

Allegro Worksheet 3	**PRODUCTIVITY RISK MEASUREMENT CRITERIA**		
Affected Area	Low	Medium	High
Working Hours	Staff working hours increased by less than 3 hours	Staff working hours increased between 3 to 6 hours	Staff working hours increased by more than 6 hours

Table 5. Allegro Worksheet 4

Allegro Worksheet 4	HEALTH AND SAFETY RISK MEASUREMENT CRITERIA		
Affected Area	Low	Medium	High
Life	No significant loss or threat to life of customers or staff members	The lives of customers or staff are threatened, but they will recover after receiving medical treatment.	Loss of life of customers and staff members
Health	Minimal and treatable deterioration in customer or staff health with recovery within four days	Temporary or reversible impairment of customer or staff health	Permanent disruption to important aspects of customer or staff health
Security	Security questioned	Security affected	Security breached

From the discussion results obtained in Table 1 to Table 5, a priority ranking was carried out. Affected areas that are most prioritized get the highest score, which is 5. While affected areas that are less of a priority get the lowest priority score, which is 1. The results of giving priority scores are in Table 6.

Table 6. Allegro Worksheet 7

Allegro Worksheet 7	PRIORITIZATION WORKSHEET IN THE AFFECTED AREA
Priority	Affected Area
5	Productivity
4	Finance
3	Reputation and customer trust
2	Health and safety
1	Legal sanctions

Table 6 shows that Waluyo Jati Hospital in dealing with existing risks prioritizes productivity in handling existing risks.

In this step, the finance department determines the impact area by looking at financial conditions for the last 3 years, and paying attention to the annual financial planning transition guidelines. Then the guarantee section determines the impact of the legal sanctions area seen from the amount of funds resulting from these demands. Then the results of the discussion with the SIM RS Unit are the results of general management considerations. Productivity as the top priority with the area that is the focus of attention is working hours only. This selection is because the addition of erratic working hours can result in less focus of human resources in carrying out their duties, including errors in data input.

3.2 Developing an Information Asset Profile

This information asset profile was compiled by conducting discussions with the SIM RS Unit. The information asset profile in the Avesina application is in Table 7.

Table 7. Allegro Worksheet 8

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Aset Critis	**(2) Reasons for Choosing**	**(3) Description**
Avesina Application	Electronic Medical Record Application owned by RSUD Waluyo Jati which is used to record diagnoses and actions given to patients.	Health systems that utilize the latest web-based technologies that support health information systems

(4) Owner		
RSUD Waluyo Jati Probolinggo Regency		
(5) Safety Requirements		
☐ Confidentiality	Only authorized personnel can view information assets, as follows:	a. Leadership and management b. Medical personnel c. Paramedical personnel d. Non-medical personnel
☐ Integrity	Only authorized personnel can modify information assets, as follows:	SIM RS Unit
☐ Availability	Assets should be available to authorized personnel to perform their duties, as follows:	a. Leadership and management b. Medical personnel c. Paramedical personnel d. Non-medical personnel
	Asset must be available for 24 hours	
(6) Most Important Safety Requirements		
☐ Confidentiality	☐ Integrity	☑ **Availability**

Table 7 shows that the Avesina application is considered critical due to its function as a means of electronic medical records owned by RSUD Waluyo Jati. This application can only be modified by the SIM RS Unit. Then this Avesina application can be used by leaders and management, medical personnel, paramedical personnel, and para-medical personnel in carrying out their duties. What is meant by medical personnel are doctors and specialists, both dentists, orthopedic doctors, and others. Meanwhile, para-medical personnel are nurses, pharmacists, laboratory assistants, and radiographers. Then what is meant by non-medical personnel here is the staff of the Hospital SIM Unit and all patient service administration staff. The avesina application must be available for 24 hours, in order to maximize excellent service to patients.

3.3 Identifying Information Asset Containers

The information asset container is a development of the information asset profile. To develop the information asset container, discussions were held with the SIM RS Unit with the results in Table 8, Table 9, and Table 10. In Table VIII, it is known that the avesina application is only used on PCs and servers owned by RSUD Waluyo Jati. Then in Table IX, the avesina application does not have a physical form either in the internal or external scope. Then in Table 10 it is known that the avesina application is used by all human resources at RSUD Waluyo Jati. Avesina application is not used by personnel who come from outside Waluyo Jati Hospital.

Table 8. Allegro Worksheet 9A

Allegro Worksheet 9a	**INFORMATION ASSET RISK MAP (TECHNICAL)**
Internal	
Container Description	Owner
PCs and Servers	RSUD Waluyo Jati
Eksternal	
Container Description	Owner
-	-

Table 9. Allegro Worksheet 9B

Allegro Worksheet 9b	INFORMATION ASSET RISK MAP (PHYSICAL)
Internal	
Container Description	Owner
-	-
Eksternal	
Container Description	Owner
-	-

Table 10. Allegro Worksheet 9C

Allegro Worksheet 9c	INFORMATION ASSET RISK MAP (PEOPLE)
Internal Personnel	
Name or Role/Responsibility	Department or Unit
Director and management	Leadership and management
Medical personnel and paramedical personnel	Installation and support
Non-medical personnel	Management and units
External Personnel	
Contractors, Vendors, Etc.	Organization
-	-

3.4 Identifying Areas of Concern

Identifying areas of concern is a process of finding risks that might occur. The risks that might occur are obtained from the results of discussions with the SIM RS Unit. From the results of these discussions, the following results were obtained:

Table 11. Result of Identifying Areas of Concern

IT Assets	Area to Watch	Actor	Selection Rationale	Motive	Results	Safety Requirements
Avesina Application	1. Data input errors	User	Users incorrectly input patient data, both doctor's actions, drugs, and support given to patients	Users are not focused so they accidentally enter the wrong data	a. Modified b. Disruption	Users are not focused on inputting data
	2. Application Hacks	External	Avesina app is controlled by an unauthorized person	Disrupt hospital productivity, monitor and obtain required data, and modify existing data	a. Disclosure b. Modification c. Disruption	The hospital SIM unit has not yet updated the security system on the Avesina application
	3. Applications can be easily accessed by unauthorized persons	User	Users do not log out of the application after using and/or sharing their username and password.	Users do not know the importance of maintaining application login security	a. Disclosure b. Modification c. Disruption	The application has not implemented a login session, and has not locked the username that is not authorized to operate the application.

IT Assets	Area to Watch	Actor	Selection Rationale	Motive	Results	Safety Requirements
	4. Account sharing	User	Username and password are given to others for work purposes	Helping the person concerned	Disclosure	Account sharing

Table 11 shows that there are 4 risks that might occur in the avesina application. The risk comes from user and external actors. The reason for the actors to carry out these risks is accidental, caused by fatigue, non-compliance with information technology security, and failure to prevent unauthorized entry. The motives carried out both accidentally and intentionally by users, as well as unauthorized parties want to disrupt the existing binsi process. The results caused by existing risks can be more than 1, which includes: disclosure, modification, interference, and destruction. However, in this research, the risks that arise do not result in the destruction of information assets. Security requirements can be violated due to user fatigue, application security has not been updated, no login session, and no 2-factor authentication.

3.5 Identifying Threat Scenarios

The identification of threat scenarios begins with filling out a threat scenario questionnaire. The results of the scenario become a reference in determining the priority of the possibility of risk occurrence. The identification of threat scenarios was carried out by discussing with the SIM RS Unit. The following are the results of the identification of threat scenarios:

Table 12. Threat Scenario Identification Results

IT Assets	Area to Watch	Probabilitas Kejadian
Avesina Application	1. Data input errors	Medium
	2. Application Hacks	Low
	3. Applications can be easily accessed by unauthorized persons	High
	4. Account sharing	High

Dari Tabel 12 diketahui bahwa risiko yang muncul memiliki probabilitas yang berbeda-beda. Namun risiko yang punya potensi tinggi adalah berbagi akun dan aplikasi dapat mudah diakses oleh orang yang tidak berwenang. Risiko peretasan memiliki probabilitas rendah, dan kesalahan input memiliki potensi yang sedang.

3.6 Identifying Risks

Identifikasi risiko merupakan tahapan untuk mengetahui dampak yang ditimbulkan. Dalam melakukan identifikasi dilakukan dengan berdiskusi bersama dengan Unit SIM RS. Berikut hasil identifikasi risiko:

Table 13. Risk Identification Results

IT Assets	Area to Watch	Consequences to Organization/Assets
Avesina Application	1. Data input errors	Data entered is not appropriate so that it can result in service errors that can cause a decrease in reputation and customer trust and legal sanctions.

IT Assets	Area to Watch	Consequences to Organization/Assets
	2. Application Hacks	The medical record process is disrupted, hindering productivity when conducting patient examinations and providing actions.
	3. Applications can be easily accessed by unauthorized persons	The occurrence of misuse of applications, and misuse of authority in the operation of applications so that it can lead to lawsuits
	4. Account sharing	Unauthorized parties have access to applications in the hospital, which can cause disruption to productivity and lead to legal sanctions.

The impact of emerging risks can disrupt business processes. Then the risk can also cause data discrepancies that result in legal sanctions. Risks that arise can also result in the avesina application being controlled by unauthorized parties.

3.7 Analyzing Risk

This risk analysis step is a search for consequences that will occur. In conducting risk analysis, discussions were held with the hospital's SIM unit. To determine risk identification, the scores were divided into the following: 1=low, 2=medium, 3=high. The score comes from the value multiplied by the priority. Priority comes from Table VI. Then the relative score is the sum of the existing scores. The following are the results of the risk analysis in Table 14.

Table 14. Risk Analysis Result

IT Assets	Area to Watch	Affected Area	Priority	Value	Score (Priority x value)	Relative Risk Score
Avesina Application	1. Data input errors	Reputation and customer trust	3	2	6	32
		Finance	4	2	8	
		Productivity	5	3	15	
		Health and safety	2	1	2	
		Legal sanctions	1	1	1	
	2. Application Hacks	Reputation and customer trust	3	3	9	44
		Finance	4	3	12	
		Productivity	5	3	15	
		Health and safety	2	3	6	
		Legal sanctions	1	2	2	
	3. Applications can be easily accessed by unauthorized persons	Reputation and customer trust	3	3	9	44
		Finance	4	3	12	
		Productivity	5	3	15	
		Health and safety	2	3	6	
		Legal sanctions	1	2	2	
	4. Account sharing	Reputation and customer trust	3	2	6	30
		Finance	4	1	4	
		Productivity	5	3	15	
		Health and safety	2	1	2	
		Legal sanctions	1	3	3	

From the analysis results in Table 14, the existing risks have a high impact on the impact area. Of the 4 risks, the risk of applications can be easily accessed by unauthorized persons and application hacking. The risk with a relative score is account sharing, then the risk of data input errors.

3.8 Selection of Mitigation Approach

To select mitigations, mapping is done using a relative risk matrix. Relative risk matrix in Table 15.

Table 15. Relative Risk Matrix

		Score		
		45-30	29-16	15-0
Priority	High	*Pool 1* (mitigated) 3. Applications can be easily accessed by unauthorized persons (44) 4. Account sharing(30)	*Pool 2* (mitigated/delayed) -	*Pool 2* (mitigated/delayed) -
	Medium	*Pool 2* (mitigated/delayed) 1. Data input errors (32)	*Pool 2* (mitigated/delayed) -	*Pool 3* (postponed/accepted) -
	Low	*Pool 3* (postponed/accepted)2. 2. Application Hacks (44)	*Pool 3* (postponed/accepted) -	*Pool 4* (accepted) -

From Table 15, the risk mitigation approach is continued. The results of the mitigation approach are in Table 16.

Table 16. Risk Mitigation Approach

IT Assets	**Area to Watch**	**Approach**	**Mitigation**	
			Containers	**Control**
Avesina Application	1. Data input errors	Delayed	-	-
	2. Application Hacks	Delayed	-	-
	3. Applications can be easily accessed by unauthorized persons	Mitigated	Management	The Planning, Development, Monitoring, and Evaluation Section needs to emphasize the importance of maintaining application security by paying attention to user logout.
Avesina Application			SIM RS Unit	Create a login section scheme, and make it easier for users to LogOut
				Regular user login monitoring, security system updates, and secure application development [14].
	4. Account sharing	Mitigated	SIM RS Unit	Provide a 2-factor authentication system for logging in to the application to ensure the login process is done by the account owner.
				Implementation of account usage policies, improving account security, monitoring user activity, and limiting user access [15].

From Table 16, it is known that the risk mitigation approach in this study is mitigated and postponed. Postponed risks do not need to be continued at the mitigation stage. Mitigation is only given to risks that are in pool 1 of Table 15. In Allegro's OCTAVE method, there are 4 choices of mitigation approaches, namely: accepted, postponed, mitigated, and transferred. In

this research, there are no risks/areas of concern for mitigation approaches in the form of acceptance and transfer.

CONCLUSION

The conclusion of this research is that there are 2 out of 4 areas that need to be considered for mitigation. These areas are account sharing and the application can be easily accessed by unauthorized people. While areas that need attention and do not require mitigation are data input errors, and application hacking. Allegro's OCTAVE method provides mitigation by focusing on information asset containers. In this study, asset containers that need to be considered in determining risk mitigation include management and the SIM RS Unit in the form of monitoring users so as not to violate application security, creating login sessions, and creating 2-factor authentication logins.

ACKNOWLEDGEMENTS

Suggestions for future researchers are:

1. Information technology in hospital institutions needs to be realized to have an impact on business processes;
2. OCTAVE Allegro has a broad and deep focus, but a more up-to-date method is needed according to the latest information technology conditions;
3. The rapid development of information technology requires research to be expedited in order to meet the need;
4. This research has limitations in data collection that is less able to bring up field facts, so the depth of analysis is very lacking.

REFERENCES

[1] M. Ayuningtyas and Tanaem Penidas Fiodinggo, “Information Technology Asset Security Risk Management at the Secretariat of the Salatiga City DPRD Using ISO 31000,” *Journal of Information Systems and Informatics*, vol. 4, no. 1, pp. 92–105, 2022, [Online]. Available: http://journal-isi.org/index.php/isi

[2] A. Della Ariesta, Suprapto, and A. R. Perdanakusuma, “Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi pada PT. MyECO Teknologi Nusantara menggunakan Framework COBIT 2019 Proses EDM03 dan APO12,” Malang, 2022. [Online]. Available: http://j-ptiik.ub.ac.id

[3] M. S. A. Setiawan, E. M. Safitri, M. A. T. Taufiqurahman, and M. A. Pratama, “Analisis Manajemen Risiko Keamanan Sistem Informasi Rocketic.id menggunakan Metode OCTAVE dan FMEA,” *Jurnal Sistem dan Teknologi Informasi (JustIN)*, vol. 11, no. 3, p. 504, Jul. 2023, doi: 10.26418/justin.v11i3.66628.

[4] Tjahjono, Budiyanto, and Khuzaini, “RISK MANAGEMENT AT RURAL BANK WITH ISO 31000 APPROACH,” Surabaya, Mar. 2022.

[5] I. P. S. Arta *et al.*, *MANAJEMEN RISIKO*, 2021st ed. Bandung: PENERBIT WIDINA BHAKTI PERSADA BANDUNG, 2021. [Online]. Available: www.penerbitwidina.com

[6] N. L. Putri and A. F. Wijaya, “Information Technology Risk Management in Educational Institutions Using ISO 31000 Framework,” *Journal of Information Systems and Informatics*, vol. 5, no. 2, pp. 630–649, Jun. 2023, doi: 10.51519/journalisi.v5i2.468.

[7] Evinia and M. N. N. Sitokdana, “Risk Management Based IT Analysis Using ISO 31000 (Case Study: PT Bawen Mediatama),” *Journal of Information Systems and Informatics*, vol. 5, no. 1, pp. 380–390, Mar. 2023, doi: 10.51519/journalisi.v5i1.420.

[8] M. A. Tasya, D. D. J. Suwawi, and R. G. Utomo, “Information Security Risk Analysis of State-Owned Bank Information Technology (IT) Assets Using the Octave Allegro Method,” Sep. 2022.

[9] G. Sitorus, R. Fauzi, and R. A. Nugraha, “ANALISIS RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE OCTAVE ALLEGRO PADA DINAS KOMUNIKASI DAN INFORMATIKA JAWA BARAT,” Bandung, Aug. 2020.

[10] A. Zulfia, E. L. Ruskan, and P. Putra, “Penilaian Risiko Aset Informasi dengan Metode OCTAVE Allegro: Studi Kasus ICT Fakultas Ilmu Komputer Universitas Sriwijaya,” *JOINS (Journal of Information System)*, vol. 6, no. 1, pp. 40–47, May 2021, doi: 10.33633/joins.v6i1.4088.

[11] R. Ramadhintia and R. Bisma, “Jurnal Sistem dan Teknologi Informasi Analisis Manajemen Risiko Aplikasi Ujian Online dengan Metode OCTAVE Allegro pada lembaga pendidikan,” *JUSTINDO (Jurnal Sistem dan Teknologi Informasi)*, vol. 6, no. 2, pp. 62–73, 2021, [Online]. Available: http://jurnal.unmuhjember.ac.id/index.php/JUSTINDO

[12] N. Budarsa, G. Indrawan, and A. Gunadi, “ANALISIS RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE OCTAVE ALLEGRO DAN ANALYTICAL HIRARCHY PROCESS PADA DATA CENTER PEMERINTAH KABUPATEN BULELENG,” *Jurnal Ilmu Komputer Indonesia (JIK)*, vol. 7, no. 1, pp. 11–20, Feb. 2022.

[13] F. R. Fiantika *et al.*, *METODOLOGI PENELITIAN KUALITATIF*, 1st ed., vol. 1. Padang: PT. GLOBAL EKSEKUTIF TEKNOLOGI, 2022. [Online]. Available: www.globaleksekutifteknologi.co.id

[14] A. Budiman, S. Ahdan, and M. Aziz, “ANALISIS CELAH KEAMANAN APLIKASI WEB E-LEARNING UNIVERSITAS ABC DENGAN VULNERABILITY ASSESMENT,” 2021.

[15] N. Fauziah and H. Permana, “TADBIR: Jurnal Manajemen Pendidikan Islam PEMERATAAN AKSES PENDIDIKAN SISTEM INFORMASI MANAJEMEN PADA LEMBAGA PENDIDIKAN ISLAM,” *TADBIR: Jurnal Manajemen Pendidikan Islam*, vol. 10, no. 2, pp. 59–74, Feb. 2022.