Analysis of Risk Assessment on Electronic Services using OCTAVE Allegro Framework

Eka Anggraini
Department of Information System Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

Awareness of the importance of information system security and its assets and impacts what might happen as a result of damage to the information system and its assets still seems to have not received the attention of most organizations. LIPI BPTBA correspondence services are managed using an information system that can manage correspondence services in the organization. This system is called TNDE (Electronic Service Manuscript Administration). TNDE allows for risks that can interfere with information assets and the main objectives of the organization but cannot be separated from problems so that it creates risks to security and information assets. This study aims to analyze risk management assessments using the framework Octave Allegro that organizations can determine risk priorities and create a mitigation approach to risks that may occur in TNDE services. Octave Allegro has four phases and eight stages, namely building risk measurement criteria, developing information asset profiles, identifying containers information asset, identifying areas of concern on aspects technical, physical, and people container, identifying threat scenarios, identifying risks, analyzing risks, and choosing an approach. Mitigate the risks that may occur. Based on the final results of interviews and risk assessments that have been carried out at the TNDE BPTBA LIPI Yogyakarta service, the results of the approach mitigate are 2, defer is 3, and accept is 2. The highest risk that needs to be prioritized is from the aspect physical container with a value of 32, while the smallest risk is a technical container with a value of 15. Thus this research that has been carried out can provide benefits for BPTPA LIPI Yogyakarta.

Keywords

Risk Assessment, OCTAVE Allegro, Mitigation.

1. INTRODUCTION

The development of information and communication technology has been widely applied within the scope of the organization. Organizations that know that information technology can increase value in their main activities and supporting activities. Information technology will be useful if its application is in accordance with the organization's vision and mission [1]. BPTBA LIPI, which is located in Gunung Kidul Regency, Yogyakarta, is one of the agencies that has applied an information system to support business processes, one of which is the Electronic Service Manuscript Information System (TNDE). The implementation of data and information management really needs to be managed by utilizing information technology to increase work effectiveness and productivity in managing data and correspondence information in an organization [2]. In the management of manuscript management services managed in an Electronic Service Manuscript System (TNDE), this service can be accessed via tnde.lipi.go.id. The application of data storage using information technology can provide many benefits to agencies, but it is not free from problems so that it can cause risks to the organization [3]. To define risks and minimize risks that may occur in the future in an organization or institution, it is necessary to carry out risk analysis and assessment of the IT services used [4]. Risk assessment analysis has several frameworks or methods that can be used to measure risk assessment services in an agency, including COBIT, OCTAVE, ITIL, NIST, RISK IT, and others. In this study, the authors used the framework of the OCTAVE Allegro method as a reference for risk assessment in this study. Therefore, the authors are interested in conducting this research to be able to assist management in making decisions about solutions to existing problems, as well as oversee the implementation of business cooperation so that it is always protected from adverse risks [5]. And the implementation of this research will be carried out with a report entitled "Analysis of Risk Assessment on Electronic Service Manuscripts Using the Octave Allegro Method".

2. LITERATURE STUDY

2.1 Management Information System

Is a system consisting of a group of people, procedures, tools, databases, and data models as its elements, when this system is responsible for collecting various data, both from within and outside the organization, then processing it. These data and provide management information to shape managers in the decision-making process [6].

2.2 Information System Information

The system is a system within an organization that meets the needs of daily transaction management, supports operations, is managerial, and strategic activities of an organization, and provides certain external parties with the required reports [7]. The information system is a collection of components that interact with each other to process input in the form of data into information that aims to achieve a common goal. [8].

2.3 Definition of Risk

Risk is the potential loss due to the occurrence of a certain event. An undesirable outcome that could lead to losses if not anticipated and not managed properly [9]. In other words, the risk is the possibility of a situation or situation that can threaten the achievement of the goals and objectives of an organization or individual [10].

2.4 Risk Management and Risk Analysis

Defining risk management is a field of science that discusses how an organization applies measures in mapping various problems that are existing by placing a variety of management approaches in a comprehensive and systematic manner [11]. Risk analysis is a form of uncertainty regarding a situation that will occur in the future with decisions made based on various considerations at this time. Measurement of risk by looking at the potential for the severity [12]. The main purpose of conducting a risk analysis is to measure the impact of a potential threat, determine how much loss is incurred due to the loss of a business potential.

2.5 Information System Security

Information Exchange Environment (IEE) Vulnerability Information has increased as threats have become more extensive and complex, therefore, information security has become a fundamental problem for businesses, organizations, and government [13]. Information security is an effort to secure information assets against threats that may arise [14]. So that information security can indirectly guarantee business continuity, reduce the risks that occur, optimize the return on investment (return on investment). The more company information that is stored, managed, and shared, the greater the risk of damage, loss, or exposure of data to unwanted external parties. [15]. The application of information security aims to overcome problems and constraints both technically and non-technically such as availability, confidentiality, and integrity so that the level of information security can be assessed. [16].

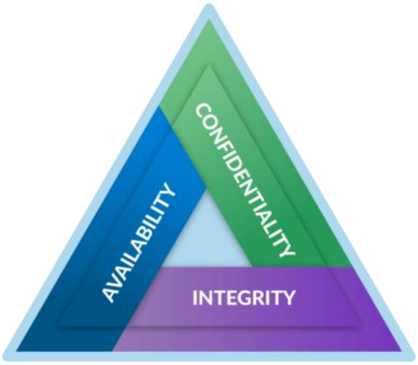

Figure 1. Principles of Information System Security

The following is a brief explanation of Figure 1, namely the Confidentiality aspect which ensures the confidentiality of data or information, ensuring that information can only be accessed by authorized persons. Integrity, which ensures that data is not altered without the permission of an authorized party, the accuracy and integrity of the information must be maintained. Meanwhile the Availability, aspect ensures that data will be available when needed, with only users authorized [16].

2.6 Risk Management Process

Process risk serves to make better decisions and increase efficiency. Risk management has three stages, namely risk identification, risk evaluation, and risk assessment [17].

2.7 Basic Principles of Risk Management

The principle of risk management to be more effective, the organization must comply with the principles of risk management, namely risk management is an integrated part of the organization's business processes, part of the decision-making process, takes into account uncertainty, is built through a systematic, structured and timely approach is transparent and dynamic [18].

2.8 Management Method

Method Information technology risk management method is a framework designed to address various risks associated with the use of information technology [19]. One of the risk management methods is Octave Allegro besides being suitable for use by individuals who wish to carry out a comprehensive risk assessment without extensive involvement of the organization [20].

2.9 Octave Allegro Method

The OCTAVE method is a methodology used to identify and evaluate information security risks [21]. The OCTAVE method is suitable for analyzing information security risks because of the risk occurrence assessment from various organizational perspectives [22]. Conduct a risk assessment based on three basic principles of security administration, namely confidentiality, integrity, and availability [23]. Octave has two variants, namely OCTAVE-s and Octave Allegro [24]. The OCTAVE Allegro method consists of eight stages which are grouped into four categories or phases. The four categories are as follows:

1) Category 1, defines what the organization directs.
2) Category 2, create a profile of assets owned by the organization.
3) Category 3, identifies the threat for each information asset in its container collection.
4) Category 4, identifying and mitigating risks to information assets and developing a mitigation approach.

The explanation regarding the phases and steps of the OCTAVE Allegro is as shown in Figure 2.

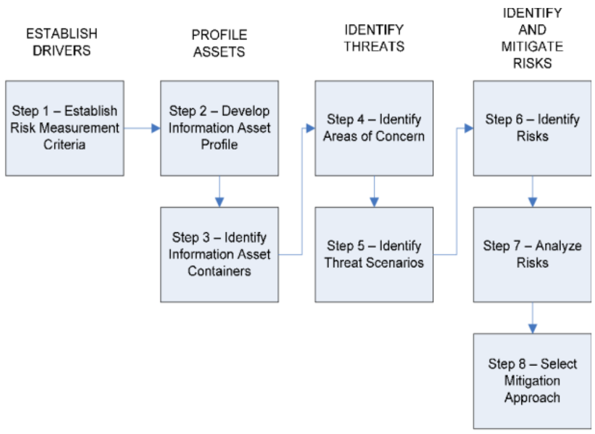
ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE RISKS
Step 1 – Establish Risk Measurement Criteria
Step 2 – Develop Information Asset Profile
Step 3 – Identify Information Asset Containers
Step 4 – Identify Areas of Concern
Step 5 – Identify Threat Scenarios
Step 6 – Identify Risks
Step 7 – Analyze Risks
Step 8 – Select Mitigation Approach

Figure 2. Phases and Stages of OCTAVE Allegro

3. METHODOLOGY

This research carried out several process stages used to collect the required data. The stages of the data collection process include:

1 Observation
An accurate and specific method of collecting data or information by observing and recording conditions in accordance with the topics to be discussed.

2 Study Literature
Data collection methods by looking for references that are relevant to the case or problem being studied to collect data or sources related to the research topic. Reference sources used are books, journal articles, research reports that have been done, and websites on the internet.

3 Interview
The interview is an activity carried out to obtain information directly by conducting questions and answers between the author and the resource person by asking research-related questions.

4 Scenarios Questionnaire

List of statements distributed to respondents to be studied and then returned to the author. The guidelines used in the making of the questionnaire in this study were OCTAVE Allegro v.1.0 with reference to "Appendix C-OCTAVE Allegro *Questionnaires*".

4. RESULTS AND DISCUSSION

The stages of risk assessment in TNDE services will refer to the four phases and eight stages that exist in Octave Allegro, namely as follows:

1. Step-1 Determining Risk Assessment Criteria

The first step determining organizational drivers to evaluate risks to TNDE service objectives. Step there are two activities. Activity 1 establishes a series of qualitative measures (risk measurement criteria) that are used to determine the impact area and evaluation of risk impacts:

a. Reputation and Trust of the User
Impact area and the reputation and trust of users related to the reputation and trust of all users who interact with the TNDE system. Whether it's employees, administrators, and heads of institutions on the impact of risks that will arise in relation to the risks that occur.

b. Financial
Impact areas and finance relate to the costs or funds that the institution will spend due to risks.

c. Productivity The productivity
Impact area relates to how the TNDE system provides services to employees. The impact area is also related to how administrators and technicians ensure the service runs well.

d. Safety and Health
Relating to the safety and health of the user, be it an administrator or an employee, in the event of a risk.

e. Fines and legal sanctions
Fines and penalties will be given to the TNDE service administrator if they are wrong, or misuse TNDE services resulting in a damaged application and service system.

Inactivity 2, a priority value is assigned to each impact area from the most important to the least important identified on a scale of 1-5, giving a scale of 5 for the important impact area, and 1 for the impact area that is not important. Very important, as in Table 1.

Table 1. Determination of Impact Areas

Priority Score 1-5	*Impact areas*
3	Reputation and Trust of Users
4	Financial
5	Productivity
1	Security and Health
2	Fines and Legal Sanctions It

It can be seen in Table 1 the value of impact areas that have the most influence on the priority namely productivity with the highest score, namely 5, because if this impact area runs well it will greatly affect existing services, so if this impact area occurs a risk will be able to affect impact areas other. The second priority is the impact on the area financially with a score of 4 which covers the financing of maintenance or system replacement. Repair costs depend on the level of damage incurred. The third priority is the reputation and trust of the user. If the reputation and trust of the user decrease, it can have a negative impact on the progress of the institution. The fourth priority is fines and legal sanctions. If IT administrators misuse information services so that unwanted things happen it will have a negative impact on TNDE services, but this is very rare and even never happened. Next, the fifth priority is safety and health, which occupies the last priority because there has never been a risk that could affect the safety and health of TNDE services.

2. Step-2 Identifying the Information Asset Profile

This stage develops an information asset profile starting with identifying critical information from the results of identifying business processes and documenting the results of identifying business processes on TNDE services. The following is the profiling of critical information assets using Allegro Worksheet 8 as in Table 2.

Table 2. Critical Information Asset Profile

	Critical Information Asset Profile	
(1) Critical Asset What are critical information assets?	**(2) Rationale For Selection** Why are these information assets important in organizations?	**(3) Description** What is the description of the information asset?
Correspondence service data which consists of Personnel Data, Incoming Mail Data, Outgoing Mail Data, and Data Disposition	Data Correspondence Services are very important because all data are interrelated with one another. Personnel data is the main data on TNDE which functions for information dissemination. If the personnel data is lost, the goals of the organization will be disturbed.	This Personnel Data contains all the information necessary for the smooth running of the corresponding business process. This data includes personal employee information such as name, address, employee title, and others.
(4) Owner (s) Who owns the information assets		
BPTBA LIPI (Lembaga Ilmu Pengetahuan Indonesia)		
(5) Security Requirements What are the security requirements for information assets?		
Confidentiality	Always maintain the confidentiality of data access rights from unauthorized parties. So that users can access only users who have been registered and verified.	
Integrity	Maintain data so that there is no change or modification from any party, only authorized users can modify this information asset.	
Availability	Data must be maintained whenever needed. This asset must be available for 24 hours.	
(6) Most Important Security Requirement *What is the most important security requirement for the information asset?*		
Confidentiality	Integrity	√ Availability

Based on the results of the critical asset profile on the information system in table 2, the results of the identification above show that the security equipment on the TNDE service information asset is Availability because data availability must be maintained because it greatly affects the overall TNDE service, if some data is lost this, it will be able to hamper the smooth running of business processes or services that exist at BPTPA LIPI.

3. Step-3 Identifying Information Asset Containers

In this step, identifying the *container* of the information asset through the interview stage, the process of identifying the information asset container consists of 3 parts, namely *technical*, *physical*, and *people* from external and internal sides by asking questions to sources. From the results of the interview, it can be seen that the summary in the technical forum focuses on the server network that is managed by the LIPI Jakarta head office. Then on the physical container, it focuses on the physical assets that exist in the LIPI agency that is used to manage existing services, then on the people container focuses on the people who are in the Gunung Kidul LIPI environment, both internal and external.

4. Step-4 Identifying Areas of Concern

Step 4 begins with the process of identifying areas of concern, by brainstorming to look for threat components from situations that might affect or threaten information assets in agencies. Identify areas of terms technical (TC), physical (PhC), and people (PC) as shown in Table 3.

Table 3. Area of Concern

No.	Areas of concern	Code	Requirements Security
Technical Container			
1.	Cessation TNDE services due to electricity supply stopped.	TC-1	1. Availability
2.	There is a problem with Internet connectivity.	TC-2	1. Availability
3.	Security in the system so that the system can be exploited by outsiders in the form of spreading *malicious code* into the server computer	TC-3	1.Confidentiality 2. Integrity
4. A	Crash on the operating system	TC-4	1. Availability
5.	Abuse Access rights such as *username* and *password*, if known by other parties	TC-5	1. Confidentiality 2 Integrity
Physical Container			
6.	Damage caused by unexpected events (being struck by lightning, short circuit, fire, or natural disaster) causes the *server to* crash.	PhC-1	1. Availability
People Container			
7.	Social engineering can lead to the disclosure of access to the server	PC-1	1. Confidentiality

Conclusions in Table 3 are that the technical container has the highest threat is numbered 5, 1 physical container, and the container 1.

5. Step 5 Identifying Threat Scenarios

The fifth step will clarify the threats that occur in each area of concern by identifying threat scenarios to determine the effect of risk on information assets, the identification process is carried out using several scenarios questionary, questions referred to in "Appendix C-Threat Scenarios Questionnaires 1-3" Which consists of 3 types of containers, namely technical, physical, and people.

At the technical facility, service stopped due to the interruption of the electricity supply, TNDE service was stopped due to slow or disconnected internet connectivity so that the service became blocked and stopped temporarily. Then a security gap in the system can be exploited by outsiders in the form of spreading malicious code into the server computer. An operating system crash can hinder the service process. Then the password and username are leaked to unauthorized parties which can result in loss of data confidentiality. Furthermore, in physical containers, natural hazards can be obtained which can occur at any time, potentially causing physical damage to infrastructure on devices related to TNDE services. Then in the people forum, there is social engineering which is carried out by direct conversation or through social media against internal agencies by external parties which can result in the disclosure of user access rights or other important information.

6. Step-6 Identifying Risks

Activity in step 6 is to determine the total score impact area by reviewing the risk measurement criteria obtained in Step 1. The levels of risk are high (n = 3), medium (n = 2), and low (n = 1). How to calculate the score for each impact area is as follows:

1. If the value of the impact area is low, then multiply it by the number 2 so that the formula becomes (nPrioritas x nLevel = 1).
2. If the value of impact area is medium, it is multiplied by the number 2 so that the formula becomes (nPrioritas x nLevel = 2).
3. If the value of impact area is high, then it is multiplied by the number 2 so that the formula becomes (nPrioritas x nLevel = 3).

The results of identification for each impact score that have been obtained can be seen in Table 4.

Table 4. Determination of Relative Risk

Impact Areas	Value Of Priority	Impact Score		
		Low (1)	Medium (2)	High (3)
Productivity	5	5	10	15
Reputation and Trust	4	4	8	12
Financial	3	3	6	9
Fines and Penalties	2	2	4	6
Safety and Health	1	1	2	3

7. Step-7 Analyzing Risks

This step analyzes the total amount of risk in all *areas of concern* which is the result of identifying previous threats by creating a profile then determine the pool in each risk profile in the risk *areas of concern* using the *Allegro Worksheet 10* as in Table 5.

Table 5. Order of Risk-based on Total Risk Score

Code	*Areas of Concern*	Reputation and Trust *User*	Financial	Productivity	Safety and health	of fines and legal sanctions	Total Risk Score	Probes	Mitigation Approach
TC-1	TNDE cessation services as electricity supply stopped.	3 (Low)	4 (Low)	10 (Med)	1 (Low)	2 (Low)	20	*Low*	*Defer*
TC-2	There is interference with Internet connectivity.	3 (Low)	4 (Low)	15 (High)	1 (Low)	2 (Low)	25	*Low*	*Defer*
TC-3	Security in the system so that the system can be exploited by outsiders in the form of spreading malicious code into computers.	6 (Med)	8 (Med)	5 (Low)	1 (Low)	2 (Low)	22	*Low*	*Defer*
TC-4	The occurrence of a crash on the operating system	3 (Low)	4 (Low)	5 (Low)	1 (Low)	2 (Low)	15	*Medium*	*Accept*
TC-5	Misuse of access rights such as username and password if the other party finds out	9 (High)	4 (Low)	5 (Low)	1 (Low)	2 (Low)	21	*Medium*	*Mitigate*
PhC-1	The occurrence of damage caused by natural disasters caused the server to crash.	6 (Med)	8 (Med)	15 (High)	1 (Low)	2 (Low)	32	*High*	*Mitigate*
PC-1	Social *engineering* can lead to the disclosure of access to servers.	6 (Med)	4 (Low)	5 (Low)	1 (Low)	2 (Low)	18	*Low*	*Accept*

After compiling risks based on the approach taken in Table 5, next is to classify the number of threats to each *container* based on the mitigation approach applied, this aims to facilitate the mitigation approach of each risk as in Table 6.

Table 6. Grouping Number of Threats

Mitigation Approach	*Technical Container* (TC)	*Physical Container* (PhC)	*People Container* (PC)
Mitigate	1	1	0
Defer	3	0	0
Accept	1	0	1
Total	**5**	**1**	**1**

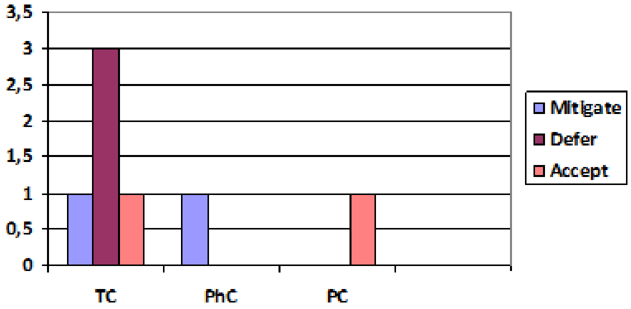

Figure 3. Grouping based on the mitigation approach

8. Step-8 Choosing an Approach Mitigation

In the eighth step, a mitigation approach will be selected which will be carried out by classifying the risk profile and ranking each risk from each of the identified concerns based on the risk value described in the previous step. Furthermore, grouping is carried out in order to summarize or simplify the risk profile and sort it according to the total score which can be seen in Table 7.

Table 7. Grouping based on the Mitigation Approach Mitigation

Approach	Code	Area of Concern	Recommendation
Mitigate	*TC-5*	Misuse of access rights such as *username* and *password*, if known by other parties	Efforts are required to have a fairly comprehensive understanding in selecting the security system that needs to be applied according to the needs of the agency.
	PcH-5	Failure caused by an unexpected event (lightning, short circuit, fire, or natural disaster) caused the *server to* crash.	The recommended effort is to *back periodically* data so that it can be stored safely in the natural disaster, lost or damaged data can be *recovered.*
Defer	*TC-1*	Termination of TNDE services due to interrupted electricity supply.	The recommended effort is to contact the ISP to make repairs or the agency to provide or use a backup power backup (Genset).
	TC-2	There is interference with Internet connectivity.	The recommended effort is to contact Telkom to make repairs.
	TC-3	Security gaps in the system so that the system	The recommended effort is to limit physical access to computers, implement

		can be exploited by outsiders in the form of spreading *malicious code* into the server computer.	mechanisms in *hardware* and operating systems for computer security and create programming strategies to produce programs reliable computer. And by installing antivirus with the *updates* latest, installing a *firewall*, and being careful with files *downloaded*.
Accept	*TC-4*	Crash in the operating system	Controls and checks a computer or network regularly
	PC-1	Social engineering can lead to the disclosure of access to the server	All employees appeal to the importance of maintaining the confidentiality of service data access rights and IT administrators must limit themselves from parties who are not authorized.

Based on the results from Table 7, it can be seen that the approach is *mitigate* carried out in the *area of concern* with the TC-5 and PhC1 codes. The approach is *defer* carried out in the *area of concern* with the TC-1, TC-2, and TC-3 codes. While the approach is accepted in the *area of concern* with TC-4 and PC-1 codes.

5. CONCLUSION

Based on the research that has been done, the conclusions drawn are as follows:

1. Risk assessment of TNDE services at BPTPA LIPI Gunung Kidul is carried out by determining the impact area in advance to determine the impact that will occur when a threat is made, identify information assets, identify containers of information assets, determine the severity of the threats and provide recommendations or mitigation strategies for each threat.
2. Based on the research results that have been carried out at the TNDE BPTPA LIPI service, the results obtained are approaches mitigate 2, defer 3, and accept the 2.highest risk is a physical container with a value of 32, namely if damage occurs due to unexpected events. (Lightning, short circuit, fire, or natural disaster) causes the server to crash. The smallest risk is a technical container with a value of 15 if there is a crash in the operating system.

6. REFERENCES

[1] NL Kuntari, YH Chrisnanto, and AI Hadiana, "Risk Management of Information Systems at Jenderal Achmad Yani University Using the OCTAVE Allegro Method," *Semnati*, pp. 551–558, 2018.

[2] ED Chairunis, "Analysis of Risk Assessment on EPrints Repository Services Using the OCTAVE Allegro Framework. Risk Assessment Analysis on EPrints Repository Services Using the OCTAVE Allegro Framework," no. September, 2019.

[3] P. Aristasari and I. Riadi, "Risk Management in a Learning Management System Using the OCTAVE Allegro Framework," pp. 1–15, 2011.

[4] M. Sukri, “Risk Management Analysis on Administration System using OCTAVE Allegro Framework,” pp. 1–6, 2020.

[5] JJL Tobing and AK Puspa, "Risk Management Analysis for Asset Evaluation Using the Octave Allegro Method," *Expert J. Manaj. Sist. Inf. and Teknol.*, vol. 5, no. 1, 2015, doi: 10.36448 / jmsit.v5i1.719.

[6] MR Weitekamp, "Management Information Systems," *Portable Heal. Adm.*, pp. 109–136, 2003, doi: 10.1016 / B978-012780590-0 / 50047-X.

[7] AL Setyabudhi, "Designing a Web-Based Information System for Attendance Data Processing and Work Leave Letter Retrieval," *JR J. RESPONSIVE Tek. Inform.*, vol. 1, no. 1, pp. 11–22, 2017, doi: 10.36352 / jr.v1i1.84.

[8] H. Ikhsan, N. Jarti, JTU Baja, P. Studi, T. Industry, and O. Allegro, "Information Technology Security Risk Analysis," vol. 2, no. 1, pp. 31–41, 2019.

[9] Catherine, Angela, C. Sylvia, and Handoko, “Risk Management Analysis of Electronic-Based Learning Systems,” *Semin. Nas. Technol. Inf. and Commun. 2019 (SENTIKA 2019)*, no. June, pp. 9–18, 2019.

[10] RRP Lawoliyo, "Risk Management Analysis for the expansion of PLTU XXX UNIT X and Y 2x50 MW," 2018.

[11] B. Wijayantini, "Risk Management Approach Model," *Jeam*, vol. XI, no. 2, pp. 57–64, 2012.

[12] A. Novia Rilyani, YA Firdaus W ST, and DS Dwi Jatmiko, "Risk Management-Based Information Technology Risk Analysis Using ISO 31000 (Case Study: i-Gracias Telkom University) Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study: i-Gracias Telkom University), ” *e-Proceeding Eng.*, vol. 2, no. 2, pp. 6201–6208, 2015.

[13] Heru pratama, "Information System Security Audit at the Samsat Office in Krui City Using Cobit 5," vol. 2015, no. Sentika, 2018, doi: 10.31219 / osf.io / pkrej.

[14] Raden Budiarto, "Information System Security Risk Management Using Fmea And Iso 27001 Methods In Xyz Organizations," *J. Comput. Eng. Syst. Sci.*, vol. 2, no. 2, pp. 48–58, 2017.

[15] AN Puriwigati and UM Buana, "Management Information Systems-Information Security," no. May, 2020.

[16] E. Handoyo, R. Umar, and I. Riadi, "Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Integration (CMMI)," *Sci. J. Informatics*, vol. 6, no. 2, pp. 193–202, 2019, doi: 10.15294 / sji.v6i2.17387.

[17] T. Wahyuni and P. Harto, "Analysus of The Effect of Cooperate Governance and Company Characteristics on The Existence of Risk Management Commites (Case study of companies listing on the IDX for the period 2008-2010)," *Diponegoro J. Account.*, vol. 1, no. 1, pp. 555–566, 2012.

[18] Setiono Winardi, “ISO 31000-2009,” pp. 4–7, 2009

[19] Alberts, CJ, & Dorofee, A., 2002. *Managing information security risks: the OCTAVE approach.* Addison-Wesley Longman Publishing Co., Inc.

[20] M. Rachmaniah and B. Mustafa, “Information Insecurity Risk Assessment Using the Octave Allegro Method,” *J. Pustak. Indonesia.*, vol. 14, no. 1, 2015.

[21] BL Mahersmi, MF Artowini, and BC Hidayanto, "Information Security Risk Analysis Using OCTAVE Methods and Control 27001 at Dishubkominfo Tulungagung Regency," *Semin. Nas. Sist. Inf. Indonesia.*, no. November, pp. 181–194, 2016.

[22] Arum, kalkim 2018. Risk *Assessment Analysis Using Allegro Octave Framework Case Study of Library Management Information System SMA Muhammadiyah 1 Yogyakarta.* Thesis, Information System, Ahmad Dahlan University, Yogyakarta.

[23] Caralli, RA, Steven, JF, Young, LR, & Wilson, RW 2007. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* USA: Carnegie Mellon University Software Engineering Institute.

[24] Jakaria, D., R. Teguh Dirgahayu, and Hendrik. Risk Management of Academic Information Systems in Higher Education Using the OCTAVE Allegro Method. *Seminar Nasional Aplikasi Teknologi Informasi (SNATI) 2013.* Yogyakarta.