# Risk Management Analysison Administration System using OCTAVE Allegro Framework

Muh. Sukri
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

## ABSTRACT

Ahmad Dahlan University KKN services have been managed using an information system that can manage KKN services at Ahmad Dahlan University, for example KKN scheduling, determining KKN groups and determining the location and field supervisors for each unit. This system is called SIMKAT UAD (Service and community information system), SIMKAT UAD allows risks that can interfere with information assets and organizational goals. This study uses the OCTAVE Allegro framework. OCTAVE Allegro has eight stages, namely building risk measurement criteria, developing information asset profiles, identifying containers of information assets, identifying areas of concern, identifying threat scenarios, identifying risks, analyzing risks, and choosing a mitigation approach. Organizations have choices, namely accept, defer, or reduce (mitigate) the risks that may occur. Based on the final results of interviews and risk assessments conducted at the Institute for Research and Community Service (LPPM UAD) obtained The result with the mitigate approach is 4, accept number 1, and defer amount to 2. And the highest relative risk value is obtained in the physical container with the number 32, namely the occurrence of a natural disaster which causes the service to stop while the lowest relative value is obtained on the technical container, namely: disruption Services due to crashes on the service system or operating system, Misuse of access rights such as username and password. If known by other parties, other than administrators, security gaps are exploited by other parties. Each of them number 19.

### Keywords

Risk Management, OCTAVE Allegro

## 1. INTRODUCTION

The acceleration of the development of information technology is increasingly rapid in various fields, information technology is required to be more sensitive to the condition of people's lifestyle [1] The existence of information technology (IT) has now become an important thing for an organization if they want work efficiency and effectiveness. With the use and application of IT [2] The development of information systems is an effort to manage data and information, so that later data and information can be used and utilized by each business unit in higher education [3]In implementing KKN activities at the Ahmad Dahlan University institution, data and information management really needs to be managed with a system that can accommodate activities and data and information needs, including data and information management regarding KKN registration, distribution of KKN groups, sharing of implementation time, place the implementation of KKN, determining field supervisors (DPL) and the process of assessing KKN are managed in an information system. in the management of KKN services it is supported by a system, namely a community and community service information system (SIMKAT), this service can be accessed by students through ***portal.uad.ac.id***then data and information are managed by LPPM using a system called SIMKATData and information processing those who use the information system cannot be separated from problems that may result in risks within the institution itself. To minimize risk, it is necessary to carry out risk analysis and assessment of the information system or IT services used, the analysis and risk assessment carried out aims to measure the level of risk in IT services in order to minimize risks that may occur in the future in the future. an agency or institution.

Risk assessment analysis has several frameworks or methods that can be used to measure risk assessment services at an agency, including COBIT, OCTAVE, ITIL, NIST and several other methods. I will use the latest generation of the OCTAVE method as a guideline and reference for risk assessment in this study, this method is OCTAVE Allegro. Therefore, the authors are interested in conducting research on Risk Analysis and Assessment of the Ahmad Dahlan University KKN Services Using the OCTAVE Allegro Framework.

## 2. LITERATURE STUDIES

### 2.1 Information Security

Implementation of information security aims to overcome problems and obstacles both technically and non-technically such as availability, confidentiality, and integrity so that information security levels can be assessed [1]

### 2.2 Definition of Risk

Risk Is an unpleasant consequence (detrimental / dangerous) of an act or action [4] risk arises because there are conditions of uncertainty, investment can bring profit (price increases), it can also cause losses (price falls) [5]

### 2.3 The Types of Risk

Classifies risk into two, namely pure risk and speculative risk. in addition, the risk is also distinguished between dynamic and static risks that arise from a certain equilibrium condition. Risk is also subjective and objective. [5] The description of risk categories can be seen in Figure 1

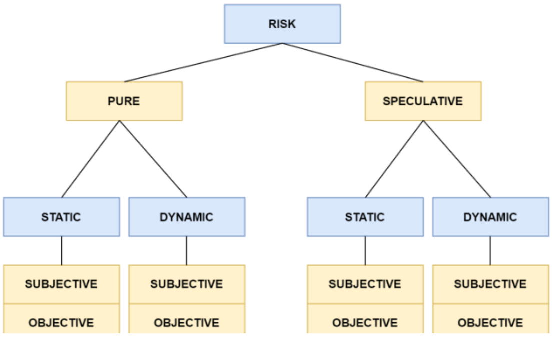

**Figure 1 Types of Risk**

## 2.4 Factors of the Risk

Factors that give rise to risk are disasters and hazards. Hazard classifications can be divided into several types, namely physical, moral, moral, and legal or regulatory hazards. [6] While the classification of the causes of risk can be divided into several types, namely physical asset risk, employee risk, and legal risk, [7]

## 2.5 Basic Principles of Risk Management

10 principles that must be adhered to in managing corporate risk management, namely: Risk is everywhere- where, risk is a threat and opportunity, risk is a combination of costs and profitable opportunities, not all risks are created equal, risks can be measured, good risk management, the key to good management is related to risks that are avoided, risks that are taken, and risks that must be exploited, The pay off better risk management is higher value, Risk management is part of every one's job, Successful risk , taking organization do not get there by accident. In its implementation, risk management principles have 3 basic principles that must be applied, namely. Proactive, collective, participative

## 2.6 Risk Management Process

The risk management process functions to make better decisions and improve efficiency. Risk management has three stages of the process, namely. Risk identification, evaluation and risk assessment. [7]

## 2.7 Risk identification and analysis The

First stage in the risk management process is the risk identification stage. Risk identification is a process that is systematically and continuously carried out to identify possible risks or losses to wealth, debt, and the company. [8] In its implementation, risk identification can be carried out with several techniques, namely brainstorming, questionnaire, industry benchmarks, scenario analysis, incident investigation, auditing, inspection checklist, HAZOP.

## 2.8 Risk Management Method

Information technology risk management method is a framework designed to address various risks associated with the use of information technology. Here are some references that will be the basis for creating the method. These methods include COBIT, OCTAVE, ITIL, NIST, and others. OCTAVE Method, OCTAVE Allegro [9]

### *2.8.1 OCTAVE Method*

The OCTAVE (Operationally Critical Threat, Assets and Vulnerability Evaluation) method conducts risk assessment based on three basic principles of security administration, namely: confidentiality, integrity, availability. OCTAVE was developed by Carnegie Mellon University's Software Engineering Institute (SEI). OCTAVE is a set of tools, techniques and methods for risk-based information system security assessment and planning. OCTAVE has three variants, namely OCTAVE, OCTAVE-S, and OCTAVE Allegro. OCTAVE Allegro. The OCTAVE method has the means and advantages of being self directed, flexible, and evolved. [9]

### *2.8.2 OCTAVE Allegro Method*

The OCTAVE Allegro method consists of eight stages which are grouped into four categories or phases, namely, in category 1 which is to determine what the organization directs, category 2 which is to create a profile of assets owned by the organization, category 3 which is to identify threats, category 4, namely identifying and mitigating which is divided into several parts [9] as for the explanation regarding the phases and steps in OCTAVE Allegro as in Figure 2

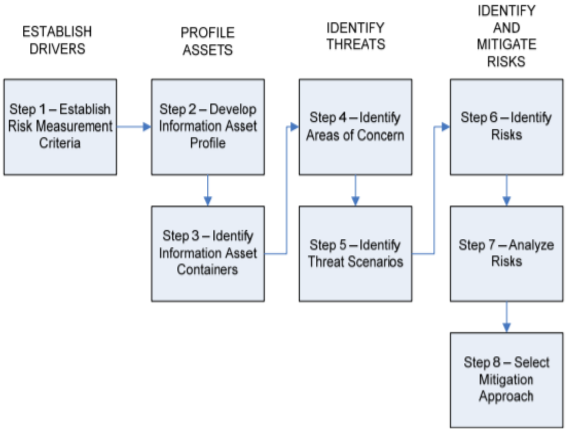
ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE RISKS
Step 1 – Establish Risk Measurement Criteria
Step 2 – Develop Information Asset Profile
Step 3 – Identify Information Asset Containers
Step 4 – Identify Areas of Concern
Step 5 – Identify Threat Scenarios
Step 6 – Identify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

**Figure 2 Phases and Stages of OCTAVE Allegro**

## 2. METHODOLOGY

Referring to the OCTAVE Allegro framework guidebook several process stages in collecting the required data. The stages of the data collection process are described in the following sub-chapters, including:

1. Observation
   Observation is an activity to review and understand a situation or event based on knowledge that aims to obtain information and problems that are obtained which will later be examined in this study. In this study, observations were made by studying and understanding the postal service *corporate*.
2. Literary
   Study Literature study is one way that can be used to collect data and information or sources related to the research topic being undertaken. Literature studies can be taken from various sources such as journals, articles, books and *ebooks project*, final references and the internet.
3. Interview
   Interview is a conversation between two or more people face to face directly between the source and the interviewer. This interview was conducted with the aim of obtaining information from reliable sources.
4. Questionnaire ScenariosThe questionnaire
   is a method of data and information inference which is done by providing a list of questions in writing to the respondent which will later be used as a reference in research. The guideline used in making the questionnaire in this study is to use the OCTAVE Allegro v.1.0 guideline with the reference "Appendix C-OCTAVE

Allegro *Questionnaires*" which is used in step 5 in risk research on postal services *corporate*.

## 3. RESULTS AND DISCUSSION

The stages of risk assessment to be carried out at the Ahmad Dahlan University Community Service Program will refer to the 4 phases and 8 stages that exist in Octave Allegro, namely:

1.Step 1 in the research stage, risk assessment, begins by determining the *Organizational Drivers* that will be used to reflect a series of risk measurements. This step has 2 activities, namely:
in activity 1 it begins by establishing a series of qualitative measures (risk measurement criteria) This action will evaluate various risk impactswhich is important for the organization. Based on the results of the interviews and the research that has been done. as well as determining *impact areas* to determine the size and extent of specific impacts, impact areas, namely:

a. Reputation and trust of the customer
*Impact area* and reputation and trust are *customer* related to the reputation and trust of all users who interact with the UAD SIMKAT system. Whether it's students, administrators, the impact of risks that will arise related to the risk that occurs

b. Financial
*Impact areas* and finance related to costs or funds that will be spent by the institution due to the risk of

c. Productivity
*Impact, the area is*productivity related to how UAD LPPM services to service management UAD KKN towards Students. It is also related to how administrators and technicians ensure the services provided run well.

d. *Impact Areas*safety and health related to safety and health at *user either* the administrator or student when there was a risk.

e. Fines and legal sanctions
*Impact area of* fines and legal sanctions related to fines and penalties that will be given to the UAD KKN service administrator if they are wrong, or misuse the UAD KKN services so that the service results in the application and service system beingdamaged.

In activity 2, priority values were assigned to each *impact area*that has been identified on a scale of 1-5, the granting of the scale is given with a number 5 for the important impact area, and a number 1 for the impact area that is not so important. As for the priority scores in each impact area in this study can be seen in table 1.

**Table 1. Determination of *Impact Area***

| Score Priority | Impact Area |
|---|---|
| 5 | Productivity |
| 4 | Reputation and trust |
| 3 | Financial |
| 2 | Fines and Penalties |
| 1 | Safety and Health |

the first priority is theon *impact the area* productivity, because it involves the services available at UAD LPPM on UAD KKN management. Good productivity is very influential on existing services so as to increase the comfort and satisfaction of each user. Furthermore, the second priority lies in the reputation and trust of the user. Because this has an impact on the reputation of the agency, if the reputation and trust of users decreases, it can have an unfavorable impact on the progress of the LPPM agency. Then in third place in the third priority is the *impact in the area which*financial includes matters of financing and system maintenance so that services are provided. there can still be prime, and can be used optimally in accordance with the existing business processes in the UAD KKN service. Furthermore, in table 4 there is *a* dendan and penalty, this *impact area impact area* is directly related to the rules and sanctions given to admins and technicians if they make a mistake that causes the system todown, but in this *impact area it*breaks very rare for LPPM agencies. so that there is no need for rules that need to be enforced. Then in the last table of safety and health. This impact area is the prioritylast because there has never been a risk that could affect the safety and health aspects of UAD SIMKAT users.

2. Step 2 at this stage is carried out by identifying a collection of critical information assets. , the identification was obtained from the identification of the UAD SIMKAT service business process.As for the collection of assets that can be found in this study, it can be seen in the table of critical asset profiles in Table 2.

**Table 2 Critical Information Asset Profile**

| | Critical Information Asset Profile | |
|---|---|---|
| **(1) Critical Asset**<br>*What are critical information assets?* | **(2) RationaleFor Selection**<br>*Why are these information assets important in organizations?* | **(3) Description**<br>*What is the description of the information asset?* |
| KKN Service Data, which is Study Program Data, Student Data, Lecturer Data, Value | Data KKN service data is data that is used daily and is the main data on business processes that exist at LPPM UAD, if KKN service data is disrupted it will hinder business processes on the UAD LPPM service, the UAD | KKN Service Data is the service data that is on SIMKAT UAD |
| **(4) Owner (s)**<br>*Who is the owner of the information asset* | | |
| Ahmad Dahlan University | | |
| **(5) Security Requirements**<br>What are the security requirements for information assets? | | |
| ***Confidentiality*** | Always Maintain the confidentiality of data access rights from unauthorized parties. So that users who can access only users who have been registered and verified with | |

| | | | |
|---|---|---|---|
| ***integrity.*** | Maintain data so that it does not experience changes or modifications from any parties, so that data integrity is maintained. | | |
| ***Availability*** | Data is always ready to be accessed anytime and anywhere. | | |
| **(6) Most Important Security Requirement**<br>*What is the most important security requirement for the information asset?* | | | |
| Confidentiality | ✔ Integrity | Availability | Others |

The results of the identification and processes *profiling* of critical information systems in table 2 show that *security requirement* the most important of the asset information system on SIMKAT UAD services is *integrity* , because maintaining data integrity is very important so that data and information assets are not easy. Amended or modified in the KKN service, considering the data on the UAD KKN service is one of the most important assets so that its integrity needs to be prioritized. However,security needs *recruitment* otherare no less important to maintain functionality

3. The third step in this research is carried out by identifying the information asset through the interview stage, the process of identifying the information asset container in 3 *containers* , namely, *technical*, *physical*, and *people*, each container identified has an internal and an external side. From the results of the interview, it can be seen that the summary of the technical container focuses on the server network that is managed by BISKOM UAD. Then on the physical container it focuses on the physical assets that exist in the LPPM UAD institution that is used to manage existing services, then on the people map focuses on the people in the LPPM UAD environment, both internal and external

Step 4 in this research This is done by identifying related areas of concern and describing the conditions related to the actual conditions in related agencies that can affect assets in UAD's SIMKAT, identification is carried out in areas of concern from the technical (TC), Physical (PhC), and people side ( PC). The identified areas of concern can be seen in table 3

**Table 3 Area of Concern**

| No | Area of concern | Code | Security Requirments |
|---|---|---|---|
| [redacted] | | | |
| 1. | Termination of SIMKAT service due to server *down* | TC-1 | 1.Avaibility |
| 2. | SIMKAT service discontinuation due toInternet connectivity interference | TC-2 | 1.Avaibility |
| 3. | Service disruption due to crash in the service system or operating system. | TC-3 | 1.Avaibility |
| 4. | Misuse of access rights such as *username* and *password*.If known by other parties, other than administrator | TC-4 | 1.Confidentialitygaps<br>2.integrityexploited |
| 5. | Securityby other parties | TC-5 | 1. Confidentiality<br>2. Integrity |
| [redacted] | | | |
| 6. | the occurrence of a natural disaster that caused the service stopped | PhC-1 | 1.avaibility |
| [redacted] | | | |
| 7. | Social *engineering* that could lead to the disclosure of *GeorgeE* and *password* administrator | PC-1 | 1.Confidentiality<br>2.integrity |

conclusion in table 3 is that the technical container has a threat The largest number is 5, 1 physical container, and 1 person container

5. The fifth step in this study is done by identifying the area of concern to include the area of concern previously in the table. 3, the identification process will be carried out through several questions using a questionnaire referred to in the “appendix threat scenarios question 1-3”. The results of the answers to each of the questions that are asked through "appendix threat scenarios question 1-3", namely:

In the technical container, the service can be stopped due to the server on UAD down due to too high user activity at the same time, such as at the same time as the card retrieval process, then at UAD SIMKAT service, it may stop at any time if the source of connectivity at the agency is lost or experiencing problems.SIMKAT UAD, can be disrupted if the operating system on the computer being used crashes. Furthermore, in the technical forum, attacks by irresponsible parties can also occur and cause the administrator's username and password to be revealed so that the computer can be exposed to a type of SQL-injection attack, then the security gap in the system if not guarded can cause attacks in the form of trojan viruses, spyware, and worms. Then in the physical container there is a disaster or environmental threat that can cause the service infrastructure to be damaged or lost. Then in the last forum, namely the people forum, social engineering was obtained on the internal agency by outsiders so that usernames and passwords could be revealed that could be misused. So it can be concluded that the most threat containers are in technical containers.

6.step-6 step in this study calculate the total score of *the impact area* by multiplying the value of *impact* area get, As for how to calculate a score for each impact area is as follows:

1. What if the value or the value on *the impact area of* low-value, *the* then the value of the v*alue of priority* can be multiplied by the number 1.
2. If the value or value in the *impact area* isvalue *medium in,* then the value in the value*of priority multiplied* can beby the number 2
3. If the value or value in the *impact area* is *high,* then the value in the value*of priority* can be multiplied by number 3

The identification results 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. In step 7, the asset profiling is carried out against the impact area that has been identified in the previous stages.The asset profile table that has been identified in this study can be seen 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** | **fines and legal sanctions** | **Total Risk Score** | **Probes** | **Mitig ation Appro ach** |
|---|---|---|---|---|---|---|---|---|---|
| TC-1 | Cessation of service SIMKAT because the server is *down* | Low (4) | Low (3) | High (15) | Low (1) | Low (2) | 25 | *High* | *Defer* |
| TC-2 | Termination of SIMKAT service due to interference with Internet Connectivity | Low (4) | Low (3) | Low (5) | Low (2) | Low (1) | 15 | *Low* | *Accept* |
| TC-3 | Service disruption due to a crash in the service system or the operating system | Low (4) | Low (3) | Medium (10) | Low (1) | Low (2) | 20 | *Low* | *Defer* |
| TC-4 | Abuse of access rights such as *username* and *password*.If known by other parties, other than theadministrator | Medium (8 | Low (3) | Low (5) | Low (1) | Low (2) | 19 | *Medium* | *Mitigateexploited* |
| TC-5 | Security gapby other parties | Medium (8) | Low (3) | Low (5) | Low (1) | Low (2 ) | 19 | *Medium* | *Mitigate* |
| PhC-1 | The occurrence of a natural disaster that caused service to stop | Medium (8) | Meedium (1) | High (15) | Low (1) | Low (2) | 32 | *High* | *Mitigate* |
| PC-1 | Social *engineering* that could lead to the disclosure *username* and *password* administrator | Low (4) | Low (3) | High (15) | Low (1) | Low (2) | 25 | *Mediu m* | *Mitigate* |

After compiling the risks based on the approach taken, the next step is to classify the number of threats present in each container so that mitigation is easier. As in table 6 and figure 3.

**Table 6 Grouping Number of Threats**

| **Mitigation Approach** | ***Technical Container* (TC)** | ***Physical Container* (PhC)** | ***People Container* (PC)** |
|---|---|---|---|
| *Mitigate* | 2 | 1 | 1 |
| *Defer* | 2 | 0 | 0 |
| *Accept* | 1 | 0 | 0 |
| **Total** | **5** | **1** | **1** |

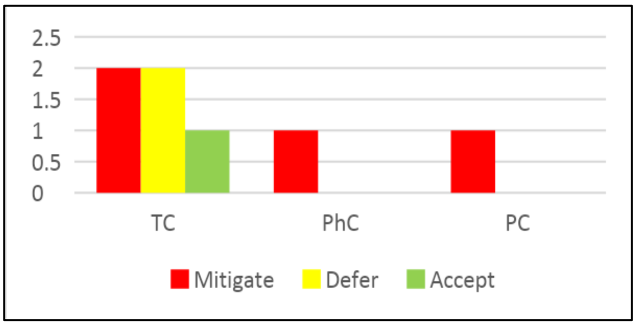

**Figure 3 Grouping Number of Threats**

8. Step 8

In Step 8, the risk profile described in Step 7 is elaborated. Selanjutkan grouping will be done in order to summarize or simplify the corresponding risk profile and sort the total score

**Table 7 Breakdown by mitigation approach**

| **Mitigation Approach** | ***Code*** | ***Of ConcernArea*** |
|---|---|---|
| *Mitigate* | *TC04* | Abuses privileges such as *username* and *password*in the know .if other hand, in addition to the administrator |
| | *TC05* | Vulnerabilities which in exploitation by others |
| | *PhC01* | occurrence of a natural disaster that caused the service stopped |
| | *PC01* | Social *engineering* that could lead to the disclosure of *George*E and *passwords* administrator |
| *Defer* | *TC01* | cessation of service SIMKAT because the server is *down* |
| | *TC03* | Disruption of service due to a crash on the system service or operating system |
| *Accept* | *TC02* | cessation of service SIMKAT due to Internet connectivity interference. |

Based on the above grouped approaches, the mitigation approach is found in TC-04, TC-05, Phc-01, PC-01. And approaches defer contained in the TC-01 and TC-03 while on approach to accept contained in the TC-02

## 4. CONCLUSION

Based on the results of research conducted on the service SIMKAT UAD, the results I discovered is the approach *mitigate* amounted to 4, *accept* amounted to 1, and *defer* numbered 2.The highest relative risk value is obtained in the *physical container* with the number 32, namely the occurrence of a natural disaster that causes the service to stop, then the lowest relative risk value is obtained in the *technical container,* namely: Disruption of services due to crashes in the service system or operating system, Abuse of rights access such as *username* and *password.*If known by other parties, other than administrators, security gaps are exploited by other parties. Each of them is 19.

## 5. REFERENCES

[1] 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.

[2] A. Wiraniagara and F. Wijaya, "Analysis of Information Technology Governance Using the Cobit 5 Domain Deliver Support and Service Framework (Case Study: Eka Tjipta Foundation, Jakarta)," vol. 5, pp. 663–671.

[3] A. Basir, A. Fadlil, and I. Riadi, "Enterprise Architecture Planning for Academic Information Systems with TOGAF ADM," *J-SAKTI (Jurnal Sains Komputan. And Inform.*, Vol. 3, no. 1, p. 1, 2019.

[4] C. Sylvia, h. Handoko, a. Woen, and c. Yang, "Risk Management Analysis of Electronic-Based Learning System," no. June, 2019.

[5] MB. Dr. Mamduh M. Hanafi,, *Risk Management*Yogyakarta: UPP STIM YKPN, 2016.

[6] SRY Ahmad, "Analysis of User Acceptance of the Application of Information Systems Using the Technology Acceptance Model," *Thesis*, vol. 4, pp. 924–929, 2012.

[7] Analysis Of The Effect Of Corporate Governance And Company Characteristics On The Existence Of The Risk Management Committee (Case Study Of Companies Listing On The Idx For The Period 2008-2010)Yogyakarta: Upp Stim Ykpn, 2009.

[8] H. Darmawi, *Risk Management / Herman Darmawi*. Jakarta: Bumi Aksara, 2010.

[9] R. a R. a. C. Caralli, JF Stevens, LR Young, and WR Wilson, "Introducing OCTAVE Allegro: Improving the Informa tion Security Risk Assessment Process, " *Young*, no. May, pp. 1–113, 2007.

[10] Aristasari, P. (2019) 'Risk Management in a Learning Management System (LMS) Using the OCTAVE Allegro Framework.

[11] Arum, kalkim 2018.Risk *Analysis ofAssessment UsingAllegro Octave Framework Case Study of Library Management Information System SMA Muhammadiyah 1 Yogyakarta*. Thesis, Information Systems, Ahmad Dahlan University, Yogyakarta

[12] 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.

[13] Chairunis, ED (2019) 'Analysis of Risk Assessment on EPrints Repository Services Using the OCTAVE Framework Allegro

[14] Dewi, NAN and I Gusti Putu Hardi Yudana. 2016. Risk Management Analysis on Academic Systems at STMIK STIKOM Bali. *National Seminar on Information and Multimedia Technology 2016* (p. 7-12). Yogyakarta: STMIK AMIKOM Yogyakarta.

[15] Husein, GM and Radiant Victor Imbar. 2015. Analysis of Risk Management for Information Technology Implementation in the Document Management System at PT. West Java Telematics (JATEL). *Journal of Informatics Engineering and Information Systems*, 1 (2), 75-87..

[16] Jakaria, D., R. Teguh Dirgahayu, and Hendrik. Risk Management of Academic Information Systems in Higher Education Using the OCTAVE Allegro Method. *National Seminar on Information Technology Application (SNATI) 2013.* Yogyakarta.

[17] Lokobal, A., Marthin DJ Sumajouw, Dan Bonny F. Sompie. 2014. Risk Management in Construction Implementation Service Companies in Papua Province. *Scientific Journal of Media Engineering*, 4 (2), 109-118.

[18] Mulyawan, Faithful, 2015. *Risk Management*, Bandung: Pustaka Setia.

[19] Nuryanto, Hery, 2012. *History of Information and Communication Technology*,Jakarta: Balai Pustaka.

[20] Rosini, Meutia Rachmaniah, and Badollahi Mustafa.

Information Vulnerability Risk Assessment Using the OCTAVE Allegro Method. Indonesian Librarian Journal, 14 (1), 14-22.

[21] Saputra, Dwi Fajar. Eprints Application Management Module. Jakarta: Jakarta State University.

[22] Saragih, SP (2018) 'Implementation of Octave-S in the Evaluation of Information System Risk Management at the Batam Health Training Center'.

[23] Supriyanto, Wahyu and Ahmad Muhsin. 2008. *Library Information Technology*. Yogyakarta: Kanisius.

[24] Suryani and Hendriyadi. 2015. *Quantitative Research Methods: Theory and Applications in Islamic Economics and Management Research*. Jakarta: Prenada Media.