Analysis of Risk Management Digital Library Services using Octave Allegro Framework

Eriza Annisa Suharyanti
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information SystemUniversitas
Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
A library service that provides information on collections of books and journals that can be accessed online is called the Digital Libraryvia digilib.uad.ac.id. Digital Library allows for risks that can interfere with information assets and organizational goals. This study uses the Octave Allegro framework which aims to analyze risk assessments so that organizations can choose a mitigation approach to risks that may occur and provide recommendations. The data collection process was carried out by means of interviews, filling out worksheets and questionnaires. The results of this study are expected to be able to calculate how many priority threats are based on the greatest possibility and the appropriate mitigation approach, and can provide recommendations on the form of strategies that can be taken to reduce risks according to the approach taken. Risk assessment on the form of strategies related to mitigation measures focuses on three levels of container categories, namely technical containers, people containers, and physical containers on the form of risk priorities.

Keywords
Risk assessment, Risk management, Digital Library, Octave Allegro**.**

1. INTRODUCTION
Digital Library owned by organization is a library that provides information on collections of books and journals that can be accessed online. Digital library content resides on local or remote computer servers, but can be accessed quickly and easily over computer networks. As technology develops, the application of information technology to the Digital Library system cannot be separated from threats and risks that may occur. IT security risks that may occur at the organization library can be overcome through IT security risk management. On this study, researchers used the Octave Allegro method to perform risk management analysis on the Digital Library Information System.

2. LITERATURE STUDY
2.1 Previous Research Studies
Analysis of Risk Assessment on EPrints Repository Service Using the Octave Allegro Framework shows the results on the form of threat priorities based on the greatest possibility and the appropriate mitigation approach as well as recommendations for developing the system.[1] From Octave Allegro it can be seen the risks that may arise from the impact of the threat.[2] Analysis of Risk Management on the organization to explaon risk management using the Octave Allegro method on the e-learning system resulted on a modeling of the e-learning system management framework.[3] Octave Allegro is one of the information system risk management methods that can be applied to universities without requiring extensive involvement on the organization and focusing on information assets that are critical for the organization's

sustainability on achieving the organization's mission and goals.[4] The use of the Octave Allegro method can identify each important information asset, set clear boundaries for assets, identify security requirements for these assets and identify all lecturer information system containers at education.[5]

2.2 Risk Management Concept
2.2.1. Definition of Risk
According to Mehr & Cammack on Hasymi, 1982:11, risk is an "unexpected possibility". According to Abbas Salim, 1989: 3, risk is uncertainty or uncertainty that may give rise to losses. According to Mamduh M.Hanafi, 2006:1, risk is "an adverse event".[6]

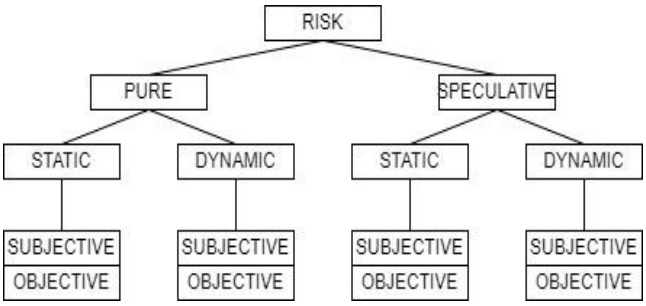

Figure1.Categories of Risk

2.2.2.Categories of Risk
Based on Figure 1, the risks are grouped by category of pure risk and speculative risk. Risk can also be distinguished between dynamic risk and static risk. Based on its nature, risk can be subjective and objective.[7]

2.2.3. Definition of Risk Management
Risk management is a comprehensive set of policies, procedures, which are owned by the organization, to manage, monitor, and control the organization's exposure to risk.[8] Risk management is aimed at reducing the possibility of losses from the risks faced.[9] Comprehensive management of the risks faced by the organization for the purpose of increasing company value. [10]

2.2.4. Basic Concept of Risk Management
Risk Management is more effective on large and complex portfolios. The nature of the instrument used to determines the parameters of the Risk Management strategy. The Risk Management System must be systematic and followed consistently but not rigid and flexible. On today's business

environment, the complexity of Risk Management has become very high and the process has become increasingly difficult.[11]

2.2.5.Risk Management Cycle

Based Figure 2 there are 6 cycles of risk management. First, identify and then study the characteristics of these risks, and evaluate them. Next, prioritize risk. The next step is to manage risk and then revisit, which is to re-evaluate the steps that have been taken.[12]

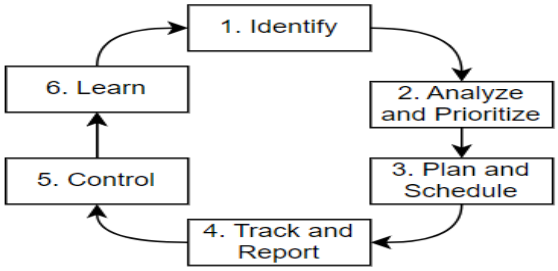

Figure2. Risk Management Cycle

2.2.6.Risk Management Process

The first process begins with identifying the risks faced by identifying risks that will be measured and analyzed on the next activity and produce a listof risk priorities. Furthermore, after the order and priority of risks are owned, the risks are then managed, followed by the preparation of mitigation plans and contingency plans, especially for risks with top priorities. Finally, supervision is carried out for further additions and improvements to the company's risk planning

2.3. Digital Library Concept

2.3.1. Definition of Digital Libraries

Digital Library or Digital Library can provide convenience that allows users to access electronic resources with fun tools for unlimited time and opportunities.[13]

2.3.2. Characteristics of Digital Libraries

Using computers to manage resources. Using electronic channels to connect providers with information users. Using electronic transactions. And use electronic means to store, manage, and transmit information to users. [14

2.3.3. Advantages of Digital Libraries

The advantages of digital libraries are saving space, multiple access, not constrained by space and time, collections can be on the form of multimedia, and low costs.

2.4. Definition of Library

A more general and broader definition of a library includes a room, building, part of a building, or other building, which contains a collection of books arranged on such a way that readers can easily find and use them when needed..[15]

2.5. Information Technology Concept

2.5.1. Information Technology

Information Technology can be described as technology that uses computers as the maon device on processing data into useful information.[16]

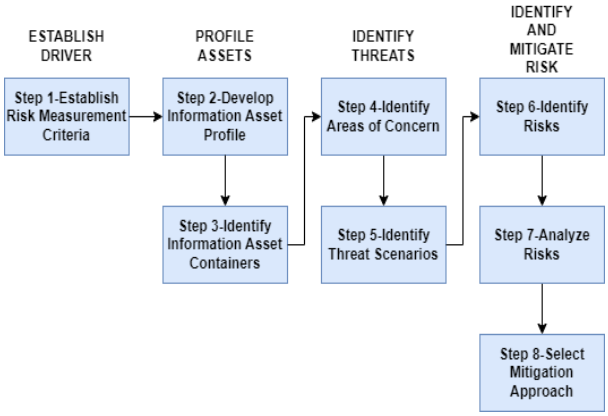

Figure 3.Step of Octave Allegro Method

2.6. Risk Management Method

2.6.1.Octave Allegro Method

Octave Allegro differs slightly from other Octave approaches on that this framework describes how information assets are owned by an organization, agency or company on the context of how they are used, where they are stored, transmitted, and processed, and how the threats, vulnerabilities, and asset disruption occurs.[17] This method consists of 8 steps, namely establishing criteria for measuring risk, creating an information asset profile, identifying information asset containers, identifying problem areas to be considered, identifying threat scenarios, risk identification, risk analysis, and choosing an approach as shown on Figure 3.

3. METHODOLOGY

This study uses several data collection techniques as follows:

3.1. Observation

The author conducts observations by observing and recording the use of Digital Libraryservices.

3.2. Study of Literature

This is done by searching, reading, and collecting references that are relevant to the research topic using reference sources from books, articles, journals, and several final assignments.

3.3. Interview

Data collection is done through face-to-face and direct question and answer.

3.4. Questionnaire

Data collection techniques through a list of questions distributed to respondents.

4. RESULTS AND DISCUSSION

4.1. Step 1 – Define Risk Assessment Criteria

The results on Table 1 show that the impact areas affected are reputation and trust, operational or financial costs, and productivity. Meanwhile, security and health as well as fines and legal sanctions are not affected.

Table 1. Impact Area Prioritization

Allegro Worksheet 7	**Worksheet Skor Prioritas *Impact Area***
Priority Score	***Impact Area***
4	Reputation and Trust
3	Financial
5	Productivity
2	Safety and Health
1	Fines and Penalties

4.2. Step 2 – Identifying Information Asset Profile

The second step on the Octave Allegro method is to develop an information asset profile. At this stage, the development of information assets is carried out. The information assets contained on the system are identified to identify vulnerabilities that may exist on the information assets of the organization Digital Library System

Table2. Critical Information Asset Profile

Allegro Worksheet 8		
CRITICAL INFORMATION ASSET PROFILE		
(1)Critical Asset What is critical information assets?	***(2)Retionale for Selection*** Why information assets important on organizations?	***(3) Description*** What is the description of the information asset?
Research data on which there are final project data (thesis and thesis), book data	Research data is one of the wealth of the academic community owned by organization, if the research data is disturbed it will hamper business processes on organization Digital Library System service.	Research Data is service data that exists on the organization Digital Library System.
(4) Owner(s) Siapa pemilik aset informasi tersebut?		
Organization		
(5) Security Requirements Who owns the information asset?		
Confidentiality	Always maintaon the confidentiality of data access rights from unauthorized parties. So that users can access only registered and verified users.	
Integrity	Maintaon data so that it does not experience changes or modifications from any parties, so that data integrity is maintained.	
Availability	Data always ready to be accessed anytime and anywhere.	
(6) Most Important Security Requirement What is the most important security requirements for the information asset?		
Confidentiality	✔*Integrity*	*Availability*

The results of the identification and profiling process of critical information systems on Table 2 show that the most important security requirement of the asset information system on the organization Digital Library System service is integrity, because maintaining data integrity is very important so that data and information assets are not easily changed or compromised. Modifications to the Research Data service, considering that research data is one of the most important assets so that its integrity needs to be prioritized. However, the security needs of other requitments are no less important to maintaon their functionality

4.3. Step 3 – Identifying Containers from Information Assets

The third stage is identifying the containers of information assets. At this stage the information asset containers where the assets are stored, transported, or processed are identified to find out where there are possible risks that can occur. Information asset containers consist of three parts, namely technical containers, physical containers, and people containers, each of which includes external and internal sides. From the results of the interview, it was found that the technical aspect of the container system focuses on the server network managed by organization as an external party. On the physical container aspect, information assets do not focus on physical assets on the form of stored documents. Meanwhile, on the people container section, information assets focus on the Digital Library System Admin and the Heads of Staff. Ur. The library and those who are entitled to full access are the Adminand technicians at organization.

4.4 Step 4 – Identifying *Areas of Concern*

On step 4, the identification of areas of concern, namely Technical (TC), Physical (PhC), and People (PC). Table 3 below is a table list of identified areas of concern.

Table3. Area of Concern

No	**Area of concern**	**Code**	**Security Requirments**
Technical Container			
1	Organization Digital Library System service stopped due to internet connectivity problems	TC-1	1) Avaibility
2	Organization Digital Library System service interruption due to system device being updated/repaired	TC-2	1) Avaibility
3	Organization Digital Library System service disruption due to server down	TC-3	1) Avaibility
4	System security vulnerabilities that can be accessed by other parties	TC-4	1) Confidentiality 2) Integrity
5	Discruption of service due to crashon the service system or operating system	TC-5	1) Avaibility

Physical Container			
6	Natural disasters or environmental threats cause services to stop	PhC-1	1) Avaibility
People Containers			
7	Error inputting data by the employee or administrator	PC-1	1) Confidentiality 2) Integrity 3) Avaibility
8	The distribution of access rights (username and password) of administrators as a result of social engineering	PC-2	1) Integrity

Based on the results on the table above, there are 6 risks of disruption to the technical containers aspect, 1 risk of disruption to the physical containers aspect, and 4 disruption risks to the people containers aspect.

4.5. Step 5 – Identifying Threat Scenarion

On this step, the identification of areas of concern is carried out to complete the areas of concern obtained from the previous step by using a questionnaire to determine the effect of risk. . Scenario 2 shows that there is a possibility of threats made by accident from outside (external) libraries and organization. Scenario 3 shows that there are several situations that allow problems such as damage to the system and hardware, the presence of viruses, disruption of the power supply, network problems, and disasters. On the physical containers section, scenario 1 indicates that there is a possibility of a threat to be revealed and modifications to information assets occur sothat it is possible for damage to occur. Scenario 2 shows that a disaster, whether caused by nature or by humans, can cause disturbance or loss. On the people containers scenario 1, it shows that there is a possible threat from internal parties that will reveal information assets and the possibility of modifications resulting on damage to information assets. While scenario 2 shows that there is a possibility of threats from outside the agency (external) that can modify or disclose information to unauthorized parties causing damage.

4.6. Step 6 – Identifying Risk

On this step, it starts by calculating the number of impact area scores by looking back at the risk management criteria that have been obtained on Step 1 as shown on Table 4. The way to calculate the score for each impact area is as follows:
1. If the value or value on the impact area is low, then the value of the value of priority is multiplied by the number 1.
2. If the value or value on the impact area is of medium value, then the value of the value of priority is multiplied by number 2.
3. If the value or value on the impact area is high, then the value of the value of priority is multiplied by number 3.

Table4. Score Impact Area

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

4.7. Step 7 – Risk Analysis

On this 7th step, a risk analysis will be carried out on all areas of concern, after which it determines all the criteria for low, medium, and high. TC-1 indicates that the occurrence of interference with internet connectivity on the Digital Library System service is of low value. TC-2 indicates thatthe organization Digital LibrarySystem service is interrupted because the system device being updated or repaired is at a medium value. TC-3 shows that the organization Digital LibrarySystem service is interrupted because the server is down at a high value. TC-4 indicates that there is a gap on system security that can be accessed by unauthorized parties at medium value. TC-5 indicates that the organization Digital LibrarySystem service stops due to a service crash or the operating system is at medium value. PhC-1 shows that the organization Digital Librarysystem service has stopped due to a disaster is at a high value. PC-1 shows that the occurrence of data input errors by the employee or administrator is at a medium value. PC-2 shows that the distribution of administrator access rights (username and password) as a result of social engineering is of medium value.

4.8. Choosing Mitigation Approach

On the 8th step, a mitigation selection will be carried out, carrying out an elaboration of the risk profile described on the 7th Step. TC-1 shows that the occurrence of interference with internet connectivity on the Digital Library System service is of low value and the action that needs to be taken is accept. TC-2 shows that the organization Digital LibrarySystem service is interrupted because the system device is being updated or updated is at a low value and the action that needs to be taken is defer. TC-3 shows that the organization Digital LibrarySystem service is disrupted because the server is down at a high value and the action that needs to be taken is defer (delay) for some time and will perform on the scheduled system when the server is down. TC-4 shows that there is a gap on system security that can be accessed by unauthorized parties at a medium value and the action that needs to be taken is mitigate or defer can be done with the need for education and socialization regarding the importance of maintaining confidentiality, maintaining confidentiality of access rights and maintaining integrity personal data and system data. TC-5 shows that the organization Digital LibrarySystem service stops due to a crash on the service system or the operating system is at a medium value and the approach that needs to be taken is mitigate or defer. PhC-1 shows that thediscontinuation of the organization Digital LibrarySystem service due to a disaster is at a high value and the approach that needs to be taken is to mitigate or defer. The suggested approach of the actions that need to be taken is mitigate to take a decision on this mitigation approach depending on the condition of the problem that occurs and review the impact of the risk by maintaining a backup of

system service data. PC-1 shows that the occurrence of data input errors by the employee or administrator is at a medium value and the approach that needs to be taken is mitigate or defer. The recommended approach for the actions that need to be taken is to mitigate, namely by re-checking the population data before submitting it to the system. PC-2 shows that the distribution of administrator access rights (username and password) as a result of social engineering is of medium value and the approach that needs to be taken is to mitigate or defer. The suggested approach of the action that needs to be taken is mitigated, namely by providing regular briefings and socialization related to the importance of maintaining the confidentiality of access rights and integrity of system services. Then after compiling the risk based on the total risk score, the next step is to group the number of threats on Table 5.

Table5. Grouping Number of Threats

Mitigation Approach	Technical Container (TC)	Physical Container (PhC)	People Container (PC)
Mitigate	1	1	2
Defer	3	0	0
Accept	1	0	0
Total	5	1	2

5. CONCLUSION

Based on research conducted on the Digital Library System service at the organization library, which obtained the mitigate approach amounting to 4, defer amounting to 3, and accepting amounting to 1. With a relatively high risk value found on Physical Container (PhC) with a total risk of 29, namely because a natural disaster occurred which caused the Digital Library System service to stop. Meanwhile, the relatively low risk value is found on Technical Container (TC) with a total risk value of 15, which is caused by interference with internet connectivity so that theDigital Library System service is interrupted or temporarily stopped.Based on the risk research that has been carried out, it is recommended that the organization library take control actions related to information assets to minimize risks to the organization system service.For future research, it is recommended to conduct a risk analysis using other methods that have the same function and purpose in order to obtain more accurate risk assessment results for similar case studies.

6. REFERENCES

[1] Chairunis, E, D. (2019). Risk Assessment Analysis on Eprints Repository Service Using OCTAVE Allegro Framework. Thesis, Information Systems, Ahmad Dahlan University, Yogyakarta.

[2] Kuntari, Laras, N., Yulison Herry Chrisnanto, Asep Id Hadiana. 2018. "Information System Risk Management at Jenderal Achmad Yani University Using the Octave Allegro Method". National Seminar on Information Technology, Ibn Khaldun University, Bogor 2018. Pp-1-8.

[3] Dewi, N.A.N. & Yudana, I.G.P.H. 2016. Analysis of Risk Management on the Academic System at STIKOM Bali. National Seminar on Information Technology and Multimedia 2016 (pp. 7-12). Yogyakarta: STMIK AMIKOM Yogyakarta.

[4] Seta, H.B., & Rahayu, T. 2017. Risk Management of Online-Based Learning Applications at Universities Using the Octave Allegro Method. Journal of the National Seminar on Information Technology and Multimedia, 7-12.

[5] Ikhsan, H. & Jarti, N. 2018. Analysis of Information Technology Security Risk Using Octave Allegro. Responsive Journal (pp. 31-41).

[6] Azhar Susanto. (2009). Management Information System, Bandung: Linggar Jaya.

[7] Hanafi, M.M. 2009. Risk Management. Yogyakarta: UPP STIM YKPN.

[8] Warburg S.B.C (2004) The Practice of Risk Management, Euromoney Book.

[9] Kasidi. 2014. Risk Management. Bogor: Ghalia Indonesia.

[10] Mamduh M.Hanafi (2012) Risk Management (second edition). Yogyakarta: UPP STIM YKPN.

[11] Tampubolon (2004) Risk Management. Jakarta: Alex Media Komputindo.

[12] Hanafi, M.M. 2009. Risk Management. Yogyakarta: UPP STIM YKPN.

[13] Saleh, A.R. (2005). Building a Digital Library. (Widyawan, Translation) Jakarta: Sagung Seto.

[14] Pendit, L.P. (2007). Digital Library. Jakarta: Sagung Seto.

[15] Sutarno, N.S. 2006. Libraries and Society. Jakarta: Sagung Seto.

[16] Sutabri, T. (2014) Introduction to Information Technology. Yogyakarta: Andi.

[17] Caralli, R.A., Steven, J.F., Young, L.R. Wilson, R. 2007. Introducing Octave Allegro: Improving the Information Security Risk Assessment Process.

[18] Ali, I. 2016. Security of Digital Collections with a Risk Management Approach. National Library (pp. 16-17).

[19] Bahrudin, M. & Firmansyah. 2018. Information Security Management in Libraries Using SNI ISO/IEC 27001 Framework. (pp. 46-47).

[20] Djojosoedarso, S. 2003. Principles of Risk Management and Insurance, Edition. Revision. Jakarta: Four Salemba.

[21] Mahardika, F. 2017. Information Security Risk Management Using the NIST SP 800-30 Framework. Journal of Informatics: Journal of Development (p. 2-3). Sumedang: STMIK Sumedang.

[22] Siahaan, 2009. Risk Management in Companies and the Bureaucracy. Surabaya: Gramedia.

[23] Sutarno, N.S. 2006. Libraries and Society. Jakarta: Sagung Seto.

[24] Yusuf, P.M. 2013. Information, Communication, and Literature Science. Jakarta: Earth Literacy.

[25] Arista, P. (2019). Risk Management in Learning Management System (LMS) Using OCTAVE Allegro Framework. Yogyakarta: Ahmad Dahlan University.