Risk Assessment Analysis on Library Information System using OCTAVE Allegro Framework

Nela Fitria Ningsih
Department of Information System Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
The current technology has become very important in the world of work, ranging from large companies and agencies. Behind all this, of course, there are advantages and disadvantages of IT in each company. Starting from *corrupt*, viruses to IT support in a company. INLISLite is a*software*library automation applicationthat has been built and developed by the National Library of the Republic of Indonesia since 2011. To analyze the risks that can occur in the INLISLite library information system using the *Framework* OCTAVE Allegro. This risk assessment is carried out by analyzing the risks obtained from the interview process, observation, and questionnaires. The next step is the data obtained will be processed using the OCTAV Allegro framework with 8 stages, namely, building risk criteria, identifying risks, analyzing risks and choosing risk mitigation approaches to reduce threats that will occur. The results of the research that has been done on the INLISLite Library Information System at the Library Service Center for the Regional Library and Archives of DIY, obtained theapproach is *Mitigate* 4, *Defer is* 1, and *Accept is* 2. Therisk value is *relatively* highin *Physical Container* with a total score of 29, namely a natural disaster that caused the INLISLite library at the DIY Regional Library and Archive Service Library Service Center to stop, while therisk value was *relatively* lowfound in the *Technical Container* with a total score of 15, namely the presence of a *bug/error* so that the INLISLite library information system was disrupted or stopped temporarily.

Keywords
INLISLite Library Information System, Risk Assessment, OCTAVE Allegro.

1. INTRODUCTION
Information technology or also known as IT is very useful for work efficiency. Behind all that, of course, there are advantages and disadvantages of IT in each company. Starting from lost data, *corrupt,* viruses to IT support in a company. Of course, companies have information assets ranging from *hardware, software,* information systems to humans, which are the most important assets for an organization or company that must be protected from security risks [1]. Existing information assets are very complex so that they are managed properly [2].This study will analyze the INLISLite Library Information System which is a *software* library automation applicationbuilt and developed by the library.National Republic of Indonesia (Perpusnas) since 2011 [3].

Risk is always associated with the possibility of something unforeseen/unwanted happening. The loss is actually a form of uncertainty that should be understood and managed effectively by the organization as part of the strategy so that it can be added value and support the achievement of organizational goals. Broadly speaking, risk management is formed by taking into account two other things that interference threat *(threat)* and consequences[4]. There are various concepts of information systems, compatibility is one of the keys to successful implementation and acceptance of information systems [5].

One of the methods used for information technology risk management analysis in the INLISLite Library system version 3.1 is the OCTAVE Allegro method. The OCTAVE Allegro method is one of three variants of the methodology used to identify and evaluate information security risks from OCTAVE. Two of the three variants of the methodology, namely the OCTAVE method and OCTAVE-S, OCTAVE Allegro is used in this research because the goal that OCTAVE Allegro wants to achieve is a broad assessment of the operational risk environment of an organization with the aim of producing better results without the need for deep knowledge. regarding risk assessment [6].

2. LITERATURE STUDY
2.1 Definition of Risk
Risk is a word hear almost every day. Usually the word has a negative connotation, something don't like, something want to avoid. Risk can be defined as an adverse event [7]. Another definition that is often used for investment analysis is the possibility that the results obtained deviate from what is expected. Standard deviation is a statistical tool that can be used to measure risk. Another measurement is using probability [8]. Risk is the possibility of events that deviate from what is expected. However, this deviation will only appear when it is in the form of a loss. If there is no possibility of loss, then this means that there is no risk [9]. There are 4 kinds of risk factors, namely physical danger, moral hazard, and legal hazard [10]. Risk is the prospect of a preferred outcome (operational as a standard deviation [11].

2.2 Understanding Information Systems Information
Systems are a combination of System and Information, thus it can be defined that Information Systems are a collection of sub-systems that are integrated and collaborate to solve problems Information systems can be defined technically as a set of five interconnected components that have the function of collecting (retrieving), processing, storing and distributing information. 13]

Another definition according to [14] Information systems can be defined technically as a set of five interrelated components that have the function of collecting (retrieving), processing,

storing and distributing information to support decision making, coordination and coordination. control. There are 3 types of information, namely, Transaction Processing System (TPS), Management Information System, Decision Support System, Executive Information System [15].

2.3 Information Security Information

Security is an effort that aims to protect information assets from possible threats. In this way, information security can indirectly guarantee business continuity, reduce risks that occur and optimize investment returns [16]. Security issues trigger adjustments to control access to the network to protect against intruders [17]. The definition of information security is also the protection of information and information systems from unauthorized access, use, disclosure, tampering, modification or destruction. Maintaining information security is as important as maintaining company business processes. Damaged or failed information can affect the company's business processes as well [18].

The main aspects of information system security consist of *Confidentiality* (confidentiality), *Integrity* (integrity), availability (availability) or often abbreviated as CIA [19] as shown in Figure 1.

Figure 1. CIA Triad

2.4 Understanding INLISLite

INLISLite version 3.1 is a further development of the lunna software *(Software)* the INLISLite library automation application version 2.1.2 which has been built and developed by the National Library of Indonesia since 2011. Along with the development of the library world, especially in Indonesia, National Library of Indonesia considers it necessary to facilitate the spirit of library managers in all regions to start implementing library automation towards the realization of a library. digital. INLISLite is web based and uses LAN.

INLISLite version 3.1 was developed as a one-stop software for library managers to implement library automation while developing digital libraries/managing and serving digital collections. INLISLite was officially built and developed by the National Library of Indonesia in order to collect national collections in the Indonesian Digital Library network, in addition to assisting efforts to develop information and communication technology-based library management and services throughout Indonesia [20].

2.5 OCTAVE Allegro Method The OCTAVE Allegro

Approach introduced is designed to allows a broad assessment of the organization's operational risk environment with the aim of producing stronger results without the need for extensive risk assessment knowledge. This approach differs from the previous OCTAVE approach by focusing primarily on information assets in the context of how they are used, where they are stored, transported, and processed, and how they are used. exposed to threats, vulnerabilities, and disruptions as a result. Like the previous method, OCTAVE Allegro can be conducted in a workshop style, collaborative setting and is supported by guides, worksheets, and questionnaires, which are included in the appendix of this document[21]. OCTAVE Allegro is also suitable for use by individuals who wish to conduct risk assessments without extensive involvement, expertise, or organizational input [22]. OCTAVE Allegro is recommended for risk assessment of information containers [25]. The 8 steps contained in the OCTAVE Allegro method are as shown in Figure 2.

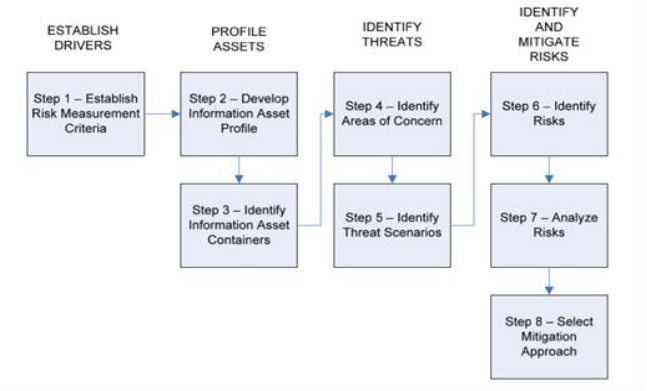

Figure 2. OCTAVE Allegro Steps

3. METHODOLOGY

This research was carried out in several stages of the process used to collect the required data. These stages are divided into the following subchapters:

1. Observation
   The observation method is the main stage of data collection for research. Observations were made by visiting the Library Service Center of the Grhatama Pustaka Yogyakarta Unit and asking the parties concerned. Research by observing directly and observing what is being carried out so that researchers know what is in INLISLite version 3.1 and its regulations. Researchers made observations on the INLISLite library system version 3.1 and found out how far the information system was operating properly. Observation aims to obtain the basic information needed, then identify the problems that will be studied in this study.
2. Literature Study Literature
   study is a method for solving problems by tracing the sources of writings that have been made before. These references can be found from books, journals, research reports and websites on the internet. The topic that can complete this research is the topic of research using OCTAVE Allegro.
3. Interview Interview
   method is one way to collect data, namely getting information by asking directly to the parties involved at the Library Service Center of the Grahatama Unit Yogyakarta. The interview process was carried out to conduct a preliminary study and collect data from respondents for each step taken. Interviews were conducted with the informants, namely:Mr. Nasrul Wahid, SIP as the supervisor during the research at the

Library Service Center of the Grahatama Unit Yogyakarta and Mr. Zulfa Kurniawan, SIP as the person in charge of INLISLite version 3.1.

4. Questionnaire
   The questionnaire method is one way to collect data, namely to obtain information by compiling a list of questions that will be distributed to respondents to fill out. In this questionnaire, the researcher uses a risk assessment based on the OCTAVE Allegro guidelines.

4. RESULTS AND DISCUSSION

The stages of risk assessment that will be carried out on the INLISLite Library Information System will refer to the 4 stages and 8 stages that exist in Octave Allegro, namely:

1. Step 1 - Determining Risk Assessment Criteria

In this first step establishing *Origizational Drivers* which aims to evaluate risk on INLISLite 3.1 Information System. In this step there are two activities, namely as follows:
In this activity 1, establish a series of qualitative measures (risk measurement criteria) that are used to evaluate the impact of significant risks on the organization. Determine the impact area to identify the extent of the risk impact. Impact areas were chosen, namely:

a. Reputation and trust *Customer*
   Impact Areas reputation and trust *Customer* concerned with reputation and confidence of all employees (internal) and public parties (external) that uses the library information system INLISLite against the impacts associated with the risk.
b. Financial
   Impact area Financial concerns the costs incurred by the Library Service Center of the DIY Regional Library and Archives Service as a result of the occurrence of a risk.
c. Productivity The productivity
   impact area concerns how E-Services Science (ELSA) provides services to employees and the general public. *This impact area* also concerns IT administrators in ensuring services run properly.
d. Security and health The
   impact of the security and health area concerns the safety and health of users (employees and participants/general public) and IT administrators when a risk occurs.
e. Fines and legal sanctions
   impact area of fines and legal sanctions concerns the fines and penalties given to IT administrators who use the wrong service if it results in damaged applications and information services.

In activity 2 in the first step of the OCTAVE Allegro method, namely identifying *Impact Areas* on a scale of 1-5, number five is for *Impact Areas* the most importantand for a scale of 1, namely for *Impact Areas* that are not too important. Table 1 is the result of the conclusion of activity 1 in determining the impact area affected to the unaffected. Assessment of the impact area from the most important to the least important can be seen in table 1.

Table 1.*Impact Area Prioritization*

Allegro Worksheet 7	
Impact Areas	**Priority Scale**
Customer Reputation and Trust	5
Operational Costs	3
Productivity	4
Safety and Health	2
Fines and Legal Sanctions	2

The most important priority is Reputation and Customer Trust because the INLISLite library system is very closely related to Reputation and Trust Customer because if there is a data error or data that does not match the real thing, so this condition can cause discomfort or dissatisfaction to the Customer. The second priority is Productivity. This productivity will affect the agency if the INLISLite system experiences problems and damage so that it can interfere with the library service process. So that it will greatly impact on service activities and productivity through this INLISLite system. The third priority is operational costs related to finance and maintenance and repair costs if there are problems with the INLISLite system. For this reason, operational costs are needed to keep the system running properly in order to be able to carry out library services.The fourth priority is safety and health, fines and legal sanctions. *The impact of this* safety and work area includes the impact of using the system on the safety and health of its users. However, so far there has been no risk that has occurred and has an impact on the INLISLite system on the safety and health of users. Impact Areas of fines and legal sanctions include the rules contained in the agency if an employee commits fraud against the system. But this has never happened to the agency so that there are almost no rules regarding fines and legal sanctions against system fraud.

2. Step 2 - Identifying an Information Asset Profile

The second step in OCTAVE Allegro is to develop an information asset profile. In this step, the development of information assets is carried out. Information assets contained in the system are identified to identify vulnerabilities that may exist in INLISLite information assets. The results of the identification of INLISLite information assets are described in table 2.

Table 2.*Critical Information Asset Profile*

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) Critical Asset What is a critical information asset?	**(2) Rationale for Selection** Why are information assets important in organizations?	**(3) Description** What is the description of the information asset?

Member data and book collection	data Member data and collection data are very important because they include information on member data and book collections in the library, therefore if there is damage it will greatly disrupt the service process on the INLISLite information system.	D This collection data is data for books which include title, author, publisher, year of publication, inventory, because this data is also an information asset owned by INLISLite to find out how many books there are because every year there are additions, and borrowing by librarian.
(4) Owner(s) Who owns the information asset?		
Library Service Center for the Regional Library and Archives of the Special Region of Yogyakarta		
(5) Security Requirements What are the security requirements for information assets?		
Confidentiality	Who gets access rights Only IT and automation managers. unless granted access by the INLISLite system maintainer himself. In order to maintain the confidentiality of the data and the right of access is always maintained	
Integrity	To mrnjaga integrity INLISLite changes and modification of the data can only be done by an authorized person	
Availability	Data can only be accessed in grhatama library, accessible to the public it is simply a catalog of books	
(6) Most Important Security Requirement What the most important security requirements for these information assets?		
✔ **Confidentiality**	Integrity	Availability

The process of identifying and *profiling* critical information assets gets the results as shown in table 2 which explains that *security requirements* for information assets contained in the INLISLite Library Information System require the most important security in *Confidentiality*. Member data and book collection data are critical data in the INLISLite Library Information System, for that integrity is very important so that it is not easily accessed by irresponsible people. However, other security needs are also needed to balance the safeguarding of information assets so that they are always safe and information assets in the INLISLite Library Information System can run according to their needs and functions.

3. Step 3 - Identifying Information Asset Containersstep

The thirdis 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. *containers* Information assetconsist of three parts, namely *technical containers*, *physical containers*, and *people containers* , each of which includes external and internal sides. From the results of interviews that have been carried out, it is found that the *Technical Container* is focused on the *server* which is managed by the Library Service Center for the Regional Library and Archives Service (BPAD) DIY. *Physical Container* focuses on the physical presence in BPAD DIY which is used to manage existing services in the library, then *People Container* focuses on the people in the agency's library environment both internally and externally.

4. Step 4 - Identifying Areas of Concern This

Step 4 is part of the third phase of OCTAVE Allegro. The fourth step of OCTAVE Allegro is the development of the information asset risk profile process. Identification of *areas of concern is* done by looking for the possibilities of situations that can interfere with the work of information assets. It aims to find out what situations and conditions will affect information assets. Identification of areas of concern consists of 3 parts, namely *technical containers, physical containers, and people containers* which are sourced from interviews that have been carried out in step 3. The results of the identification of *areas of concern are* summarized in table 3.

Table 3. ***Area of concernconcern***

No	Area ofconcern	Code	Security Requirments
Technical Container			
1	cessation of information systems INLISLite because of damage to the server	TC-1	1) avaibility
2	the presence of *bugs / errors* and causing disruption of library services	TC-2	1) avaibility
3	disruption of library services for an interruption of internet connectivity	TC-3	1) avaibility
4	Security in the system so that the system can be *Hacked* or exploited by unauthorized parties	TC-4	1) Confidentiality 2) Integrity
Physical Container			
5	The stoppage of INLISLite library services due to errors caused by unexpected events, namely natural disasters	PhC-1	1) Avaibility
People Containers			
6	Member data processing and b collection The wrong size will causeerrors *input* databy the library service, allowing data that does not match the actual	PC-1	1) Integrity

7	Distribution ofaccess rights (*username* and *password*) administratoras a result of social engineering	PC-2	1) Integrity 2) Confidentiality

5. Step 5 - Identification of Threat Scenarios

The fifth step in OCTAVE Allegro is identifying threat scenarios. Identification of threat scenarios is done by using the *Threat Scenarios Questionnaires – Allegro Appendix C questionnaire*. In this questionnaire there are three parts, namely *technical, physical,* and *people containers.* The results of the answer to the *Technical* Container, which shows that there is a possible threat from parties at the Library Service Center of the DIY Regional Library and Archives Service (internal) which causes the disclosure of information assets to unauthorized parties so that it cannot be used properly. In *Physical Containers*, there is a possible threat of the disclosure of physical information assets from data to unauthorized parties intentionally or unintentionally by employees within the agency. And there is a threat of modification of information assets and can be disrupted and possibly permanently damaged or temporarily lost so that the system cannot run properly. On *Peoplecontainer*, there is a possible threat of disclosure of information assets so that they cannot be used properly due to the actions of unintentional internal people, there is also the possibility of disclosure to unauthorized parties and can be modified so that damage to information assets occurs.

6. Step 6 - Identifying Risks

In step 6, calculating the amount in thescore, *Impact Area* namely by reviewing the *Risk Measurement Criteria* that has been obtained in step 1. The way to calculate the score for each *Impact Area* is by multiplying thevalue *Impact Area* obtained in table 4.8 above sequentially. The way to calculate the score for each impact area is as follows:

a. If the value or value in the impact area is low, then the value of the value of priority is multiplied by number 1.
b. If the value or value of the impact area is of medium value, then the value of the value of priority is multiplied with number 2.
c. If the value or value in the impact area is high, then the value of the value of priority is multiplied by number 3.

Furthermore, the results of the calculation of scores for each impact area can be seen in Table 4.

Table 4.*Impact Area*

Impact Areas	Value of Priority	Impact Score		
		Low (1)	Medium (2)	High (3)
Reputation and Trust	5	5	10	15
Productivity	4	4	8	12
Operational Costs	3	3	6	9
Fines and Legal Sanctions	2	2	4	6
Safety and Health	1	1	2	3

From the scores obtained for each *Impact Area*, both areas of productivity, reputation and trust, operational costs, fines and sanctions as well as safety and health. Then these values are added up in the risk profile section. Based on the results of interviews that have been conducted, the main priority of the five *Impact Areas* starts from the Reputation and Customer Trust area, because it is a library that prioritizes customer service and trust. If the system is disturbed, then library services cannot be delivered properly. This will result in the reputation and trust of customers in INLISLite, because they cannot carry out activities, such as borrowing, returning books or viewing personal data. And then the financial impact will increase, in order to make improvements or system updates. In the end, all of these things will affect the working hours of employees who increase, so there is a possibility that the health of employees will decrease.

7. Step-7 Risk Analysis

In this step perform a risk analysis on each *Areas Of Concern* and the consequences that occur based on the *Relative Score* by considering the *Risk Measurement Criteria* created in step 1.

Next, analyze the total amount of risk in all areas of concern which is the result of identifying previous threats by creating a profile and then determining the pool in each risk profile in the risk area of concern using Allegro Worksheet 10 as shown 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	Cessation of information systems INLISLite because of damage to the server	Low (5)	Low (3)	Low (12)	Low (1)	Low (2)	23	**High**	*Defer*
TC-2	There is a bug/error that causes disruption to library services	Low (5)	Low (3)	Low (4)	Low (1)	Low (2)	15	**Medium**	*Accept*
TC-3	Obstruction of library services due to internet connectivity disruption	Low (5)	Low (3)	High(15)	Low (1)	Low (2)	16	***High***	*Accept*
TC-4	Poor system security so that the system can be hacked or exploited by unauthorized parties	*Medium (10)*	Low (3)	Low (4)	Low (1)	Low (2)	20	***Medium***	*Mitigate*
PhC-1	cessation of library services due to errors caused by unforeseen events unexpected natural	*Medium (10)*	*Low (3)*	High (12)	Low (1)	Low (2)	28	***High***	*Mitigate*

	disaster								
PC-1	Incorrect processing of member data and book collections will cause data input errors by the library service, allowing data not to match the actual data	*Medium (10)*	Low (3)	Low (4)	Low (1)	Low (2)	20	***Medium***	*Mitigate*
PC-2	Distribution ofaccess rights (*username* and *password*administrator) as a result of social engineering	*Medium (10)*	Low (3)	Low (4)	Low (1)	Low (2)	20	***Medium***	*Mitigate*

After the risk is complied based on the total risk score , the next step is to do carry out grouping made it slightly threats contained in each container to facilitate in carrying out mitigation. The results contained in the table above is showing that *a technical container* has at most risk threat, that is numbered 4. While the *of physical container* risk of threatshas to be 1 and the *people of container* totaled 2. such as table 6.

Table 6. Number of threatsgrouping

mitigation Approach	Technical Container (TC)	Physical Container (PhC)	People Container (PC)
Mitigate	1	1	2
Defer	1	0	0
Accept	2	0	0
Total	**4**	**1**	**2**

The results in the table above show that *technical containers* have the most threat risks, which are 4. While *physical containers* have high threat risks. total 1 and *people container* totaling 2.

8. Step-8 Choosing a Mitigation Approach

Step 8 in OCTAVE Allegro is choosing a mitigation approach. The mitigation approach can be done by grouping each identified area of concern based on the relative risk score in the previous table. The results of recommendations for mitigation plans are reducing threat risks based on areas of concern which can be seen in table 7.

Table 7. Grouping based on the Mitigation Approach Mitigation

Mitigation Approach	**Code**	***Areaof Concern***	**Recommendation**
Mitigate	TC-4	system security so that the system can Hackers or exploited by unauthorized parties	Close *ports* (computer networks) that are not needed in an effort to secure the server, and replace the *port* original. *Installationfirewall*, antivirus so that no viruses, trojans or malicious code can enter the system.
	PhC-1	cessation of library services due to errors caused by unexpected events, namely natural disasters.	Routinely *backup* data so that data is always stored safely and in the event of a natural disaster, lost or damaged data can be *recovered.*
	PC-2	Distribution ofaccess rights (*username* and *password*administrative) as a result of social engineering	Adding a 2-step verification feature requires a password or verification code to enter the system, where the password or verification code can only be sent to a phone number or e-mail the owner of the account. And performchanges *password* periodic
Defer	TC-1	Cessation INLISLite information system because of damage to the server	Using the air conditioner to keep the temperature and the temperature of the room to keep them cool so that the device is protected from risks due to *Overheat.*Check internet connection and regularly clear *cache* and *cookies*. And also to *restart* the database *Service*
Accept	TC-2	The presence of bugs / errors that menyebabkann disruption of library services	Fixing systems that are experiencing *a bug / error* so that no more errors in the student data and perform testing of software and software quality assurance

	TC-3	Inhibition library services due to an interruption of internet connectivity	Acting *Control* networks by monitored and diperihara security systems are reviewed regularly then choose a *provider* networkto ensure the smooth process of system INLISLite

Based on the results of table 7 it can be seen that the approach to mitigate (reduce) conducted in the area of concern with codes TC-4, PhC-1, PC-1 and PC-2, defer approach is carried out in the area of concern with code TC-1, and accept approach is carried out in the area of concern with TC code -2, and TC-3.

5. CONCLUSION

Risk assessment on the INLISLite Library Information System at the Library Service Center of the DIY Regional Library and Archives Service, carried out with a series of guide steps for the OCTAVE Allegro method, starting with determining and defining the impact area in the information asset, then determining the critical assets of the information asset, identifying the container from information assets consisting of Technical Containers (TC), Physical Containers (PhC), and People Containers (PCs), and determine the threats from each container, determine the severity of risks and make mitigation recommendations for each threat.The results of the research that has been done on INLISLite Library Information System in the Central Library Services Department of Library and Regional Archives DIY obtainedapproach *mitigate* amounted to 4, *defer* numbered 1 and *accept* 2. The value amounted torisk *relatively* highcontained in *Physical Container* with number a score of 29, namely a natural disaster that caused the INLISLite Library at the DIY Regional Library and Archives Service Library Service Center to stop. While therisk value is *relatively* lowfound in *Technical Container* with a total score of 15, namely the existence of a bug/error so that the INLISLite library information system is disrupted or temporarily stopped.

6. REFERENCES

[1] Antonius, AS, Agustinus, FW 2018. *Analysis of Information Technology Risk Management at Diskominfo Salatiga City Using the Octave-s Method*. National Seminar on Indonesian Information Systems, 5 November 2018.

[2] A. Basir, A. Fadil, and I. Riadi, *Enterprise Archcitecture Planning for Academic Information Systems with TOGAF ADM. J-SAKTI (Journal of Computer and Information Science.* Vol 3, No. 1, p.1, 2019.

[3] Hakim, A, *Practical Guide to Strengthening Library Materials with the INLISLite Application Program Version 3.* Librarian in the Automation Sub-Sector of the Indonesian National Library.

[4] Tresnawati, S . *Analysis of Security and Information Risk Management Assets In Academic Information Systems at the Polytechnic TEDC Bandung Using NIST SP Framework 8000-30.* TEDC Bandung Computer Engineering. 2019.

[5] I. Riadi, IT Riyadi Yanto, and E. Handoyo, *Cyber Security Analysis of Academic Services based on Domain Delivery Services and Support using Indonesian E-Government Ratings (PEGI), Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 5, no. 4, 2020.

[6] Anggraini, E, Riadi I. *analysis of Risk Assessment on Electric Services using OCTAVE Allegro Framework.* International Journal of Computer Application. Volume 182. No 5. Mey 2021.

[7] Fuad, MN, Riadi, I. *Risk Management Assessment on Human Resource Information Technology Services using COBIT 5.* . Interna tional Journal of Computer Applications. Volume 175. No 23. October 2021 Hanafi, Mamduh. M. 2012. *Risk Management*. Yogyakarta: STIM YKPN Law.

[8] Kasidi. 2014. *Risk Management*. Bogor: Ghalia Indonesia Publisher, 2014.

[9] Aristasari, P & Riadi, I. 2019. *Risk Management in Learning Management System Using OCTAVE Allegro Framework.* Yogyakarta 2019.

[10] AJ Keown, *Fundamentals of financial management*. Yogakarta: PT RajaGrafindo Persada, 2000.

[11] Taufiq Rohmat 2013. "Management Information Systems. Yogyakarta: Graha Ilmu 2013.

[12] Kenneth E. Kendall and Julie E. Kendall 2006. *System Analysis and Design.* PT. Index, Jakarta.

[13] Kenneth. C. Laudon 2004. *Management Information Systems – Managing Digital Companies,* Kenneth c. laudon, Jan. P. laudon, Issue 10, Publisher: Salemba Empat.

[14] II Riyanarto Sarno, *Information Security Management System*. Surabaya: ITS Press, 2009.

[15] E. Kurniawan and I. Riadi, "Analysis of Academic Information System Security Levels Based on ISO/IEC 27002:2013 Standard Using SSE-CMM," *INTENSIVE J. Ilm. researcher. and Application of Technology. Sis. inf.*, vol. 2, no. 1, p. 12, 2018.

[16] Dalimunthe, N, & Sartika, D. 2016. *Information Security Risk Analysis Using the OCTAVE Allegro Method at the West Java Communication and Information Office.* Journal of Science, Technology and Industry. Vol. 13, 2 June 2016.

[17] CPM Fred Niederman, Mary Sumner, and JR., *Testing and extending the unfolding model of voluntary turnover to IT professionals*, *Hum. resort. Manage.*, vol. 45, no. 1, pp. 331–347, 2007.

[18] Fred Niederman, Mary Sumner, and JR., CPM (2007) *Testing and extending the unfolding model of voluntary turnover to IT professionals*, *Human Resource Management*, 45(1), pp. 331–347. doi: 10.1002/hrm.

[19] Sukri, M, Riadi, I. *Risk Management Analysis Administration System using OCTAVE Allegro Framewok.* . International Journal of Computer Applications. Volume 174. No 17. February 2021.

[20] Sitorus, G, & Fauzi, R. 2020. *Analysis of InlisLite Information System Service Quality Using the Libqual*

Method. E-Proceeding of Engineering. Vol. 7, 2 August 2020.

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

[22] Kuntari, NL, Chrisnanto, YH, & Hadiana, AI. 2018. *Information System Risk Management at Jeneral Achmad Yani University Using the OCTAVE Allegro Method.* National Seminar on Information Technology at Ibn Khaldun University, Bogor. 2018.

[23] Jerry FitzGerald. Ardra F. FitzGerald. Warren D Stallings. *Fundamentals Of Systems Analysis*. Second edition; New York: John Willy & Sons. 1981.

[24] Davis, Gordon B, and Margrethe H. Olson 1985. *Basic Information Systems Framework.* Second edition. Binaman Pressindo Library, Jakarta.

[25] Rosini, Rachmaniah, M, Mustofa, B. *Information Vulnerability Risk Assessment Using OCTAVE Allegro Method.* librarian journal. Vol. 14 No.1.