Analysis Risk Assessment on Hospital Management Information System using Octave Allegro Framework

Arinda Diahapsari
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Hospital Management Information Systems (SIMRS) is an information system that supports the service process in hospital both in terms of coordination, reporting, and administrative procedures. However, in the Hospital Management Information System (SIMRS) it is necessary to carry out a risk assessment to find out what threats can occur, in this research case study a risk assessment was carried out using the *framework* OCTAVE AllegroThe application of the OCTAVE Allegro method is carried out in agencies that already have and apply information technology. The OCTAVE Allegro method has eight steps which are divided into four phases, namely the phase of determining criteria, the asset profile phase, the threat identification phase, and the risk identification and mitigation phase. The steps in the OCTAVE Allegro method include determining risk measurement criteria, creating an information asset profile, identifying information asset containers, identifying the scope of concern, analyzing threat scenarios, identifying risks, analyzing risks, and taking a mitigation approach. Based on the results of the research on the Hospital Management Information System (SIMRS) after taking interview data and observing the risk assessment obtained from a private hospital in Yogyakarta, the results of the *mitigated* were 4 and *accept* 3 with a relatively high-risk value found in the *Technical Container* with a value of 18, which is due to a disruption in the service system caused by a down server, causing all service activities at the hospital to be disrupted or even stopped. The recommendation for this risk threat is to increase the capacity of web hosting or it can also be done by IP filtering several illegal IPs that enter the system and performing *maintenance, monitoring,* and *control*.

Keywords

SIMRS, Risk assessment, Octave Allegro, Mitigation

1. INTRODUCTION

The application of risk management in the Hospital Management Information System is very important to reduce the risks and threats that will occur in the system, the threat can be in the form of stopping the hospital service system.

A management system is a collection of each procedure to be designed according to a business risk approach to plan, implement, check, maintain and improve. In an organization risk management is a process of planning, controlling, and regulating activities to reduce losses or risks.

Information technology supports the company's business so that IT risks can occur at any time. The application of risk management is the right way to minimize the losses that occur. Information technology is not only applied to the operational part of the organization but also the decision-making process by *executive management.*

The Octave Method *(The Operationally Critical Threat, Asset, and Vulnerability Evaluation)* is a method used to assess risk in an organization, the Octave Method was developed by *the Software Engineering Institute* (SEI) at Carnegie Mellon University

.This risk assessment research was conducted to find threats and vulnerabilities that could occur. in Hospital Management Information Systems. Existing threats and vulnerabilities will be analyzed to measure the impact of potential threats on the security of information assets and determine how much influence they have on business processes. The risk of damage in this study is in the form of an impact on customer reputation and trust, decreased service due to system *overload*, and failure to input data on time so that data is out of sync.

2. LITERATURE STUDY

2.1 Definition of Risk

Risk is a quantitative measure of the degree of damage that can be caused by a threat, vulnerability, or by a malicious or non-hazardous event affecting the organization's collection of information technology assets.

2.2 Definition of Hospital Information System

Information System is a hospital technical subsystem consisting of all information processes as well as related human or technical actors of each information processing role.

2.3 Definition of Information

Systems Information systems are science that combines human resources, hardware, software, communication networks, data resources, and policy procedures for storing, retrieving, transforming, and disseminating information within an organization.

2.4 Definition of System

system is a network of processes from each procedure so that they can communicate with each other which is carried out simultaneously so that they can perform an activity to complete a predetermined goal.

According to Ludwig Von Bartalaney, the system is a set of elements that contribute to each other in a relationship between these elements and the environment.

The figure shows that a series of systems are formed to complete a grand al, the input provided will be processed or studied to obtain output that with the goals of an organization. Three system structure processes can be seen in Figure 1.

Input
Process
Output

Figure 1. System StructureHospital Management Information Systems

2.4 OCTAVE Allegro Method

Method The octave allegro method is a method designed to streamline the information security risk assessment process, enabling organizations to achieve reasonable returns with minimal investment in time, personal, financial other limited resources. The OCTAVE Allegro method consists of eight steps arranged in four phases as shown in Figure 2 below.

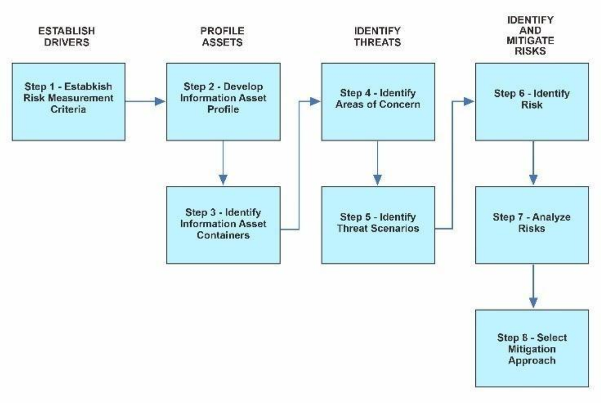
ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE RISKS
Step 1 - Estabkish Risk Measurement Criteria
Step 2 - Develop Information Asset Profile
Step 3 - Identify Information Asset Containers
Step 4 - Identify Areas of Concern
Step 5 - Identify Threat Scenarios
Step 6 - Identify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

Figure 2. The OCTAVE Allegro Method

2.5 Information

security is a form of protection for information assets from parties who do not have the authority to use the information assets. Information security is currently widely applied to the main part of management information technology by most government, commercial, and industrial organizations. Information security can be in the form of a set of mechanisms, techniques, administrative actions and processes that function to protect information technology assets from unauthorized access, appropriation, manipulation, modification, data theft, data loss, and accidental use of data and information contained in assets. -assets

2.6 Risk

Management Risk management is a technique used to obtain precise results in identifying risk events. Each risk must be able to understand the causes and consequences, usually risk in this case refers to a negative effect so that the causes of the risk must be overcome to reduce the possibility or loss to the organization.

2.7 Threat Risk

Threat Risk is an event, source, action or inaction that has the potential to cause harm to an organization's information security assets. Hackers are a source of threat, while unauthorized health insurance is an act of threat. Therefore, the threat in the image scenario is unauthorized access by *hackers* or hackers. Sources of threats can be found in a variety of ways and usually have more than one threat action.Determining threats can be done in a very subjective way so that you can use several existing methods to overcome threats that exist in an organization.Some of those categories include ISO27005, NIST SP800-30, OWASP, and BITS.

Thisidentification is done to find out how big the threat will be to an asset. Many frameworks that send threats as a combination of threat actions and threat sources can be seen in Figure 3.

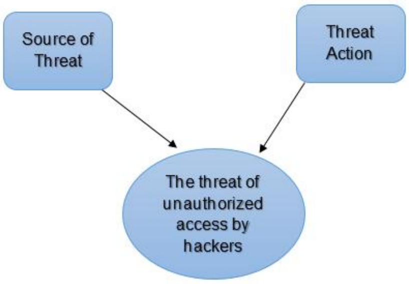

Figure 3. ThreatsRiskHospital Management Information Systems

2.8 Definition of Hospital

A hospital is an institution that provides health services to the general public in the form of inpatient or outpatient services by providing health services. such as examinations, treatment and care carried out by health professionals including doctors, nurses, pharmacists and other experts.

3. METHODOLOGY

This study has several steps used in obtaining data and materials for this research process. The steps in this research include:

1. Observation
   Observation is a method used to collect data by observing or reviewing directly on the object of research. In this study, observations were made to obtain information about the risk management of hospital management information systems.
2. Literature
   Study Literature study is a data collection technique using previous research references regarding information technology risk management analysis. References used can be in the form of *e-books*, books, journals and research report articles. Each of these references can be accessed or downloaded on the *Google Scholar*, *Institute of Electrical and Electronics Engineers (IEEE) sites,* Sinta, and Garuda.
3. Interview
   Interview is a method used to obtain data that is carried out directly on the respondent in the form of asking questions. In this study, the respondents were the staff who were responsible for the hospital management information system.
4. Questionnaire
   The questionnaire is a collection of data consisting of several written questions that will be asked to the respondents. The process of collecting data is done by giving a questionnaire sheet. The preparation of this questionnaire uses the reference guidelines of OCTAVE Allegro.

4. RESULTS AND DISCUSSION

The stages of risk assessment of the Hospital Management Information System use the stages of the OCTAVE Allegro method which consists of eight steps in four phases, namely:

1. Step 1 Determine Risk Assessment Criteria

In this first step build *organizational drivers* that are described in each step of the risk measurement criteria. In this stage there are two activities as follows:

Create a series of qualitative measurements (risk assessment criteria) that are used to evaluate the effect of significant risks on the organization. *The impact area* is part of determining how influential the risk is. The selected impact areas are

a. The impact the reputation and trust of customers have on the service system.

b. The impact of financial influence has a risk on IT investment which can disrupt the service system.

c. The impact of productivity effects has the risk of causing the system to stall.

d. The impact of the influence on safety and health has no risk on the officers.

e. The impact of the effect of fines and legal sanctions is that there are no fines and sanctions given to officers.

Gives priority value to the *impact area* with a scale of 1-5, the most influential impact area is given a value of 5 while the *impact* area that has no effect or is not at risk is given a value of 1. The results of determining the *impact area* can be concluded in table 1.

Table 1.*Impact Area Prioritization*

Allegro Worksheet 7	**Worksheet Priority Score *Impact Area***
Priority Score	***Impact Area***
1	Reputation and Customer Trust
3	Financial
2	productivity

obtained from risk determination are the impact of the financial area with a score of 3 due to IT investment in hospitals the most supportive thing for system maintenance or repair, if this IT investment is not appropriate, it can result in a system that should be treated and repaired as soon as possible due to financial constraints, it can result in the system not being maintained as much as possible so that it can pose a risk of system damage or server down which can affect the entire system. SIMRS services in hospitals. For other risks that can arise from this financial, if the cashier or finance officer incorrectly enters the nominal financial report, it can also cause the hospital to suffer losses.

The second priority is productivity with a score of 2 because it relates to the SIMRS service system being *overloaded* when accessed by officers and patients, the cause of this happens because too many *users* access so that SIMRS becomes *down* or even stops which impacts all parts of the hospital and makes the officer could not input the data promptly.

The third priority is the reputation and trust of the *customer user* with a score of 1 because it relates to incorrectly inputting patient data or drug data on SIMRS so that it can be a risk to patients and make the reputation and trust of patients to use SIMRS decrease.

2. Step 2 Develop an Information Asset Profile

This second step identifies what information assets are critical to SIMRS. The data can be obtained from interviews on business processes at SIMRS services.The most crucial information asset is the hospital's basic data because the data includes all the data in the hospital which is useful for reporting to the health office and to improve the quality of service at the hospital. or to the point of harming the hospital materially.

The results of determining the *impact area* can be concluded 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 these information assets important to the organization?	(3) **Description** What is the description of the information asset?
Hospital	Base Data is very important because the data covers the entire service in the hospital if the data is lost it will disrupt the overall performance of services in the hospital.	Hospital Base Data is the foundational data that summarizes all the data in the hospital.
(4) Owner(s) *Who owns the information asset?*		
Yogyakarta private hospital management information system		
(5) Security Requirements What are the security requirements for information assets		
Confidentiality	Protect data from unauthorized persons with access rights and maintain the confidentiality of information data to prevent data misuse. Only users who have access rights to access according to their authority.	
Integrity	Maintain data so that it remains integrated and there are no changes to data or data is modified by unauthorized persons, except for getting instructions from the person concerned to make changes if they are experiencing problems.	
Availability	Data can only be accessed.	

the *security requirement* of the information system in the Hospital Management Information System (SIMRS) service is *integrity* . Hospital basic data is critical data in the Hospital

Management Information System because it includes various important information related to all hospital data ranging from patient data, drug data to financial data in hospitals. Therefore, the integrity of the data is very important so that the data is not lost or modified by unauthorized persons. However, other security needs are also important to maintain functionality and prevent security from being compromised.

3. Step 3 Identifying *Containers* in Information Assets

The third step in this research is to identify information assets through the interview stage, namely the process of identifying information asset containers with three containers, namely, technical, physical, and people, each container identified has internal and external sides. The result of the data obtained is that information assets are processed by *bridging* between systems and the database is stored on *the primary server* which is in the same location.

4. Step 4 Identifying Problem Areas

Step 4 begins with identifying *the area of concern* , namely by dividing it into three parts *technical* (TC), *physical* (Phc), and *people* (PC). This step describes a descriptive statement in detail regarding the conditions in the organization related to what affects assets in the Hospital Management Information System (SIMRS) as in table 3.

Table 3.*Area of Concern*

No	Area Of Concern	Code	Security Requirements
	Technical Container		
1	Disruption Management Information System (SIMRS) services due to downed server	TC-1	1) Availability
2	Management Information System (SIMRS) service disruption due to internet connectivity problems	TC-2	1) Availability
3	Hospital Management Information System (SIMRS) services) due to *hardware*	TC-3	1) Availability
4	Service interruption due *crash* in the service system.	TC-4	1) Availability
	Physical Container		
5	Hospital Management Informatithe on System (SIMRS) services will stop when unexpected events occur such as natural disasters	PhC-1	1) Availability
	People Containers		
6	Abuse of access rights to make data inputted by officers out of sync and not according to the procedure.	PC-1	1) Confidentiality 2) Integrity
7	Error in data input by officers or administrators	PC-2	1) Integrity

5. Step 5 Identifying Threat Scenarios

In this fifth step, namely identifying the *area of concern* and completing the *area of concern section.* This step will document the information assets of SIMRS by giving several questions to respondents using a questionnaire that serves to determine the effect of risk on SIMRS by referring to "*Appendix C-Threats Scenarios Questionaries 1-3".* This questionnaire is divided into three parts, *namely technical, physical,* and *people containers.*

6. Step 6 Identifying Risks

This 6th step begins by calculating the number of *impact areas* by referring to the *risk measurement criteria* that have been obtained in the first step. The way to calculate the total value of each impact area is by multiplying the value of the impact area in table 1.

How to calculate the value for each impact area is as follows:

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

The results of the calculation of the value obtained for each impact area can be seen in table 4.

Table 4. *Impact Area Score*

Impact Areas	***Value Of Priority***	***Impact Score***		
		Low (1)	***Medium (2)***	***High (3)***
Financial	3	3	6	9
Productivity	2	2	4	6
Reputation and Trust	1	1	2	3

7. Step 7 Analyzing Risk

In step 7 the activity begins by analyzing the risk in each *area of concern* and determine each criterion from *low, medium,* to *high* by referring to *allegro worksheet 1* in tables 1 to 4. Next, create a risk profile for each *area of concern* to be able to analyze the total risk.Total risk analysis will then determine the pool in each area of concern that refers to the relative risk matrix, the relative risk matrix table is used to determine the area of concern for each pool while the mitigation approach table is used to explain what mitigation approach can be applied to the area of concern. The following table of risk grouping can be seen in table 5.

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

Code	***Areas of Concern***	**Reputation and Trust *User***	**Financial**	**Productivity**	**Total Risk Score**	**Probes**	**Mitigation Approach**
TC-1	Disruption of Hospital Management Information System services (SIMRS) due to server down	*High (3)*	*High (9)*	*High (6)*	18	***High***	*Mitigate*
TC-2	Disruption of Hospital Management Information System (SIMRS) services due to internet connectivity problems	*Low (1)*	*Low (3)*	*Low (2)*	8	***Low***	*Accept*
TC-3	Disruption of Hospital Management Information System (SIMRS) services due to damage *hardware*	*Low (1)*	*Medium (6)*	*Medium(4)*	11	***Low***	*Accept*
TC-4	Service interruption due *crash* in the service system.	*Low(1)*	*Low (3)*	*Low (2)*	6	***Low***	*Accept*
PhC-1	Hospital Management Information System (SIMRS) services will stop when unexpected events occur such as natural disasters	*Low(1)*	*High (9)*	*High (6)*	16	***Medium***	*Mitigate*
PC-1	Abuse of access rights to make the data inputted by officers out of sync and not according to the procedure.	*High(3)*	*Low (3)*	*Medium (4)*	10	***High***	*Mitigate*
PC-2	Error data input by an officer or administrator	*Medium(2)*	*Low (3)*	*Low (2)*	7	***High***	*Mitigate*

After compiling the results of the total risk value, the next step is to group the number of threats from each *container* that functions to facilitate mitigation which can be seen in table 6.

Table 6. Grouping of the Number of Threats

Mitigation Approach	***Technical Container* (TC)**	***Physical Container* (PhC)**	***People Container* (PC)**
Mitigate	1	2	2
Defer	0	0	0
Accept	3	0	0
Total	4	1	2

Based on the table 6 of results from grouping the number of threats, it shows that the *technical container* gets the most total threat risk value of 4. Meanwhile, for *physical containers*,the total risk value is 1, and for *people*.

8. Step 8 Choose a Mitigation Approach

Step eight is the activity that will be carried out, namely the selection of mitigation, Grouping risks by referring to the risk value. Applying a mitigation approach for each risk obtained by using the relative risk matrix The grouping is done by considering the tendency of the existing risks, continuing from step 7, which previously explained the risk profile in this study.The value of the risk that can help in making decisions about the status of risk mitigation. Decision making on risk mitigation status is carried out from the drivers of the organization.Then the risk profile is grouped in each *area of concern* that has previously been identified which can be seen in table 7 below.

Table 7. Recommendations Area of Concern based on

Mitigation Approach	***Code***	***of Concern***	**Recommendation**
MItigate	TC-1	Disruption of Hospital Management Information System (SIMRS) service due to server down	The recommended recommendation is to increase web hosting capacity or can also do IP filter several illegal IPs that enter the system and perform *maintenance, monitoring*, and *control*.
	PhC-1	Hospital Management Information System (SIMRS) service will stop when unexpected events such as natural disasters occur	. The recommended recommendation is to *backup* data to a safer place with minimal disasters and *backup* is needed so that all data remains can be used and maintained properly.
	PC-1	Abuse of access rights so that the data entered by the officer is out of sync and does not comply with the procedure	. The recommended recommendation is to provide education to *users* to maintain the confidentiality of access rights that the data contained in it is *private*.
	PC-2	Error data input by officers or administrators	The recommended recommendation is that it is necessary to re-validate the data so that there are no errors in the data and the data becomes appropriate. In addition to educating agencies, they can also implement *Privileged Access Management* , namely by controlling, managing, monitoring, and auditing *user*.
Accept	TC-2	Hospital Management Information System (SIMRS) service disruption due to internet connectivity problems	The recommended recommendation is to find and determine which locations have high (stable) network connectivity because the direction of the signal waves is erratic and spreads, making cables or the antenna shifts.
	TC-3	Hospital Management Information System (SIMRS) service disruption due to *hardware*	maintenance *hardware* components *hardware* such as computers in places with good air circulation, routinely cleaning from dust that enters the *hardware* and using a stabilizer so that the incoming electricity is stable.
	TC-4	Service interruption due *crash* in service	regularly

Based on the results table, the mitigation approach in each area of concern is carried out for the codes TC-1, PhC-1, PC-1, and PC-2. The accept approach is carried out in the area of concern with codes TC-2, TC-3, and TC-4.

5. CONCLUSION

Risk assessment on the Hospital Management Information System (SIMRS) service was carried out using the Octave Allegro method by following the entire series of steps. in this method, namely by starting to determine the *impact area* on the information asset. *The impact area* is used to determine or find out what impacts can occur. Then determine critical assets, identify *containers* to identify threats that occur and at this stage consist of three *containers* including *Technical Containers* (TC), *Physical Containers* (PhC), and *People Containers* (PC), determine the level of threat risk from each *container* possible can occur and make recommendations for mitigation of any threats that have been found.Based on the results of research that have been carried out on the Hospital Management Information System (SIMRS) service, the *mitigated* 4 and *accept* is 3. The *relatively* high-risk value is found in the *Technical Container* (TC-1) worth 18, namely the server down can be the most crucial risk that must be faced by the hospital because it can cause all services at the hospital to be disrupted or even stopped so that it can harm the hospital.The results of the research on the overall *area of concern* show that the most common approach to the classification is *mitigated*.

6. REFERENCES

[1] Anderson, EJ (2013), *Business Risk Management: Models and Analysis*. Wiley.

[2] Angraini, Megawati, & Haris, L. (2019). Risk Assessment on Information Assets an academic Application Using ISO 27001. *2018 6th International Conference on Cyber and IT Service Management, CITSM 2018*, *Citsm*, 1–4. https://doi.org/10.1109/CITSM.2018.8674294

[3] Caralli, RA, Stevens, JF, Young, LR, & Wilson, WR (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*.

[4] Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System. In *Implementing an Information Security Management System*. https://doi.org/10.1007/978-1-4842-5413-4

[5] Georgi Popov, Bruce K. Lyon, BH (2016). *Risk Assessment: A Practical Guide to Assessing Operational Risks*. Wiley.

[6] Gerson, A., Padang, R., Ambarwati, A., & Setiawan, E. (2021). *IT Risk Management Assessment Using Quantitative and Qualitative Risk Analysis*. *10*, 527–537.

[7] Gusni, RSA, Kraugusteeliana, K., & Pradnyana, IWW (2021). Analysis of Information System Security Governance Using Cobit 2019. *National Conference on Computer Science (KONIK) 2021*, *2019*, 434–439. https://prosiding.konik.id/index.php/konik/article/view/92

[8] Hadion Wijoyo, Aris Ariyanto, Agus Sudarsono, KDW (2021). Management information System. In *Angewandte Chemie International Edition, 6(11), 951–952.* (Vol. 13, April Issue). Independent Scholar.

[9] Ichsan, R., Falach, A., Abdurrahman, L., Santoso, I., & Si, S. (2021). *Octave Allegro Risk Analysis and Information Security Control Design in Hospital Management Information System Billing Module Using Octave Allegro*. *8*(2), 2709–2722.

[10] Jake Kouns, DM (2010). *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams*.

[11] James O'Brien, GM (2010). *Management Information Systems, 10th Edition* (10th Edition). McGraw-Hill/Irwin.

[12] Javaid, MI, & Iqbal, MMW (2017). A comprehensive people, process, and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). *International Conference on Communication Technologies, ComTech 2017*, 78–90. https://doi.org/10.1109/COMTECH.2017.8065754

[13] Jaya Putra, S., Nur Gunawan, M., Falach Sobri, A., Muslimin, JM, Amilin, & Saepudin, D. (2020). Information Security Risk Management Analysis Using ISO 27005: 2011 for the Telecommunication Company. *2020 8th International Conference on Cyber and IT Service Management, CITSM 2020*. https://doi.org/10.1109/CITSM50537.2020.9268845

[14] Mahardika, KB, Wijaya, AF, & Cahyono, AD (2019). Information Technology Risk Management Using Iso 31000 : 2018 (Case Study: Cv. Xy). *Sebatik*, *23*(1), 277–284. https://doi.org/10.46984/sebatik.v23i1.572

[15] Mark Talabis, JM (2012). *Information Security Risk Assessment Toolkit*.

[16] Matondang, N., Isnainiyah, IN, & Muliawatic, A. (2018). Analysis of Information System Data Security Risk Management (Case Study: XYZ Hospital). *RESTI Journal (Systems Engineering and Information Technology)*, *2*(1), 282–287. https://doi.org/10.29207/resti.v2i1.96

[17] Mishbahuddin. (2020). Improving Hospital Health Service Management. In *Yogyakarta: Stairs of Knowledge* (Issue November 2020).

[18] Mursid, CA, & Sutopo, W. (2017). Risk Management in the Process of Selecting Vendors Using ISO 31000 and Financial Statement Analysis: A Case Study of Bank Indonesia. *IDEC National Seminars And Conferences*, 1–14.

[19] Muttaqi, FK (nd). *Hospital Information System Risk Management Using NIST SP 800-30 Framework (Case Study: RSIA Eria Bunda Pekanbaru)*. *30*.

[20] Prof. Dr. Sri Mulyani, Ak., C. (2017). *System Analysis and Design Methods* (p. 267). Systematics Servant.

[21] Ramadhan, DL, Febriansyah, R., & Dewi, RS (2020). Risk Management Analysis Using ISO 31000 on Smart Canteen SMA XYZ. *JURIKOM (Journal of Computer Research)*, *7*(1), 91. https://doi.org/10.30865/jurikom.v7i1.1791

[22] Rohman, A., Ambarwati, A., & Setiawan, E. (2020). Analysis of IT Risk Management and Asset Security Using the Octave-S Method. *INTECOMS: Journal of Information Technology and Computer Science, 3(2), 298-310.*, 1–13. https://doi.org/https://doi.org/https://doi.org/10.31539/intecoms.v3i2.1854

[23] Sardjono, W., & Cholik, MI (2018). Information Systems

Risk Analysis Using Octave Allegro Method Based at Deutsche Bank. *Proceedings of 2018 International Conference on Information Management and Technology, ICIMTech 2018*, *September*, 38–42. https://doi.org/10.1109/ICIMTech.2018.8528108

[24] Setyawan, AA, & Wijaya, AF (2018). Analysis of Information Technology Risk Management at Diskominfo Salatiga City Using the Octave-S Method. *National Seminar on Indonesian Information Systems*, *November*, 59–64.

[25] Supriyadi, Y., & Hardani, CW (2018). Information system risk scenario using COBIT 5 for risk and NIST SP 800-30 Rev. 1 as a case study. *Proceedings - 2018 3rd International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2018*, 287–291. https://doi.org/10.1109/ICITISEE.2018.8721034

[26] Suryanto. (2019). *Risk Management and Insurance* (Vol. 2). Open University.

[27] Thenu, PP, Wijaya, AF, Rudianto, C., Kristen, U., & Wacana, S. (2020). Technology Risk Management Analysis Information technology risk Using COBIT 5 (Case Study: PT Global Infotech). 2(1), 1-13.