Risk Assessment Analysis Website on Tech Company using OCTAVE Allegro Framework

Akmal Rizqi Azhari
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Tech Company website is an information system service that supports the ongoing processes of service delivery in the organization, including administration, portfolio, and business process management. However, in the website's information system service, risk assessment needs to be conducted to identify potential threats. In this research study, risk assessment is performed using the OCTAVE Allegro framework. Tech Company is a private enterprise located in Yogyakarta. The aim ofthis study is to provide recommendations to Tech Company Mukti Yogyakarta regarding vulnerabilities and threats that occur. Risk assessment consists of several stages, including analyzing data obtained through interviews, responses from worksheets, and questionnaires filled out by employees working at Tech Company.The OCTAVE Allegro method is divided into 8 steps, which are building risk measurement criteria; developing a profile of the information assets owned; identifying containers within theinformation assets; identifying problem areas in the three aspectsof the containers, namely technical, physical, and people;identifying threat scenarios; identifying risks; analyzing risks; and selecting mitigation and control approaches based on the suitability of the relative risk score calculations. The testing results conducted on the information system service of Tech Company yielded 4 containers with a mitigation approach, 2 containers with a defer approach, and 2 containers with an accept approach. The highest relative risk score was obtained in the Physical Container (PhC) with a total score of 28, mainly due to natural disasters. The lowest relative risk score was found in Technical Container (TC) 1 and 2, caused by disruptions in internet connectivity leading to service disruptions and temporary interruptions, as well as service interruptions caused by system updates

Keywords

Risk Assessment, Website, Octave Allegro

1. INTRODUCTION

The Information technology risk management has significant benefits for securing and protecting information assets that play a role in storage, processing, and provision of information [1]. Information is a crucial asset for organizations, and the success of planning, operations, decision-making, development, and maintenance processes relies heavily on this information to ensure optimal organizational performance. Information Security Management System (ISMS) has become a primary requirementin public service provision, leading to continuous improvement of information technology to enhance service quality [2]. Information system security plays a role in safeguarding organizational assets. Risk management is a process used to measure, identify, and manage risks using available resources. The risk management process consists of three stages: risk identification, risk analysis, and risk evaluation. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method is used to identify risks and threats [3]. Risk is a condition that can cause future losses if it occurs. This study utilizes the OCTAVE Allegro method to assess risks in the website services of Tech Company. The method provides mitigation recommendations to enhance the organization [4].Risk identification in website services requires analysis and a mitigation approach. The priority level of issues becomes the mainfocus, categorized as high, medium, and low risks. Some potential problems that may occur on the website include malware attacks, software vulnerabilities, and data theft that can disrupt the organization's business processes. Risk management is essential to minimize the likelihood of such issues in the website services of Tech Company [5].

2. STUDY LITERATURE

2.1 Definition of Risk

Risk is a quantitative measure of the level of damage that can be caused by threats, vulnerabilities, or by a hazardous or non-hazardous event that affects the collection of information technology assets owned by an organization. The impact of risk can be an event that results in loss, and it is highly likely that average losses can occur from such exposure. Losses can occur to specific assets even after information security measures have been implemented by the organization [6].

2.2 Definition of Information System

Information systems are a discipline that combines human resources, software, hardware, and policy procedures to store, retrieve, modify, and disseminate information for communicating data with various media such as physical devices, instructions, andinformation processing procedures [7].

2.3 Information System Security

Information security is a form of protection for information assets from unauthorized access. The need for information security is crucial for data integration and availability. Integration refers tothe consistency, accuracy, and reliability of data throughout its lifecycle. Data availability is essential, as stored data must be accessible to authorized users when requested. Failure to provide data availability poses a risk to an organization. In information security, policies are established for data identification, including information security policies set within the organization, communication of policies to employees and other responsible parties, and periodic policy reviews [8]. During identification, it is important to assess implementation levels and evaluate any gaps. Information security is widely implemented in the core of information technology management by government, commercial, and industrial organizations. Information security encompasses a set of mechanisms, techniques, actions, and administrative processes that aim to protect information technology assets from unauthorized access, appropriation, manipulation, modification, data theft, data loss, and unintended use of data and information contained within those assets [9].

2.4 Risk

Risk is a quantitative measure of the level of damage that can arise from threats, vulnerabilities, or hazardous or non-hazardous events that affect the information technology assets of an organization. The impact of risk can manifest as events that cause losses, and these losses are highly likely to occur from exposure tothe risk. Losses can still occur to specific assets even if information security measures have been implemented by the organization. When risk is identified as high, the focus should be on security controls, especially in dealing with ongoing conditions that require immediate attention. According to Joel G [10]. Siegel and Jae K. Shim, risk can be defined in three aspects: first, situationsin which decision-makers can achieve outcomes with known probabilities towards a set of specific results. Second, fluctuations in profits, sales, or other financial variables. And third, there are opportunities for financial problems that affect the performance and financial position of the company, such as economic risk, political uncertainty, and industry issues [11].

2.5 Risk Management

Risk management is a technique used to achieve accurate outcomes in identifying risk events. Each risk should be understood in terms of its causes and consequences, typically referring to negative outcomes, so that the causes can be addressed to reduce the likelihood or impact of losses to the organization [12].

2.6 Analysis System

System analysis is a method used to break down a system into interacting and collaborating components in order to achieve the system's goals. The purpose of system analysis is to aid decision-making by understanding the actual conditions. System analysis is also an investigation to comprehend the true state of an event or action. Overall, system analysis is a research technique conducted to study the components of a system, the relationships between these components, and to identify the strengths and weaknesses of the system [13].

2.7 Risk Assement Website

Ease of access can potentially harm developers of web app information systems as it increases the likelihood of website hacking attempts. Therefore, it is important to conduct risk assessment or risk assessment on the web portal to identify and understand the risks associated with such access. One recommended method for risk assessment is using OCTAVE. OCTAVE is known for its subjective approach to the research subject. Based on experience and OCTAVE documents, organizations that successfully implement risk assessment can maximize the use of risk management activity information and anticipate and respond to various activities that affect risk management. In this study, the web portal of Tech Company is used as a case study. Tech Company is a startup operating in the IT services and solutions sector [14].

3. METHODOLOGY

3.1 Method of Collecting Data

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 thesereferences can be accessed or downloaded on the Google Scholar, Institute of Electrical and Electronics Engineers (IEEE) sites.

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 thehospital 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 [15].

3.2 Risk Assessment Method

This research will be conducted, which adopts the stages used in the OCTAVE Allegro method for assessing risks in the information system services of Tech Company. The OCTAVE Allegro method consists of eight steps divided into four stages that are used to perform risk assessments.

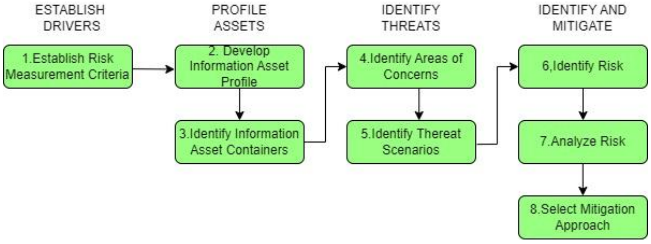
ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE
1.Establish Risk Measurement Criteria
2. Develop Information Asset Profile
3.Identify Information Asset Containers
4.Identify Areas of Concerns
5.Identify Thereat Scenarios
6,Identify Risk
7.Analyze Risk
8.Select Mitigation Approach

Figure 1. OCTAVE Allegro Step

Based on figure 1. 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, personnel and other limited resources [16].

4. RESULT AND DISCUSSION

The risk assessment process for the Company's Information System service was conducted following the 8-stage OCTAVE Allegro reference. This section aims to present the research findings. The research involved interviewing the responsible party from Tech Company. The final outcome includes the steps of the risk assessment research and the discussions derived from the conducted interviews. Before delving into the initial steps outlined in the OCTAVE Allegro Framework, a preliminary step in the form of a brief interview was conducted to gain an overview of the service processes within the Information System. This step aimed to evaluate the risk effects on the vision, mission, and objectives of the ongoing business processes.

1. Step Determine Risk Assessment Criteria

The table each aspect has been determined with the priority order of each aspect's impact areas, including:

a. The first priority is towards the aspect of reputation and user trust with a score of 5. Reputation significantly influences the level of user trust in the use of information systems.
b. The second priority is the aspect of productivity with a score

of 4. Service to prospective customers should run smoothly without any disruptions to ensure user satisfaction.

c. The third priority is the financial aspect with a score of 3. This relates to the cost of system maintenance and the possibility of upgrading to more advanced devices.

d. The fourth priority is the aspect of fines and penalties with a score of 2. Fines to be paid by the administrator are directly related to the rules and sanctions imposed by the management in the event of significant errors that could result in system failure.

e. The fifth priority is the aspect of safety and health with a score of 1. Risks that affect health and security rarely occur in information systemservices."

Table 1. ***Impact Area Prioritization***

Allegro Worksheet 7	***Worksheet Skor Prioritas Impact Area***
Skor Prioritas	***Impact Areas***
5	*Reputation and Customer Confidence*
3	*Financial*
4	*Productivity*
1	*Safety and Health*
2	*Fines and Legal Penalties*

The obtained impact areas are included in Table 1. The scoring calculation rules for each impact area value can be done as follows: If the obtained value for the impact area is low, then the value in the "value of priority" is multiplied by If the obtained value for the impact area is medium, then the value in the "value of priority" is multiplied by 2. If the obtained value for the impact area is high, then the value in the "value of priority" is multiplied by 3."

2. Develop an Information Asset Profile

This stage will involve a process of identifying a collection of critical information assets, known as the Critical Information Assets Profile. These assets are the outcome of interviews conducted on the business processes occurring within the Information Systems Service of Tech Company.

Table 2. ***Critical Information Assets Profile***

Allegro Worksheet 8	**CRITICAL INFORMATION ASSET PROFILE**	
(1) *Critical Asset* What is a critical information asset?	**(2) *Relationale for Selection*** *Why are there information asset important to the organization?*	**(3) *Description*** what is the description of the information assets?
The product catalog data contains about the offered products, including pricing information, specifications, and contact information products.	Product catalog data is crucial at company it encompasses product information reflecting the organizations performance and specific client information.	Data that includes an inventory of all data assets owned by the organization
(4) *Owner(s)* *Who owns the information assets ?*		
IT Company in Yogyakarta City		
(5) Security Requirements what are the security requirements for information assets ?		
Confidentiality	Maintaining the confidentiality of data access rights from unauthorized parties and preserving the confidentiality of the information data. All visitors can access the data, but only non-critical data can be accessed by visitors.	
Integrity	To maintain the integrity of data and prevent unauthorized alteration, modification, or unauthorizedaccess to its contents, except when instructed to make changes from within the internal scope of the institution.	
Availability	The data can only be accessed through the internal linkup of Tech Company.	

The results of the identification and profiling process of the information system services listed in Table 2, it can be concluded that the most important role is played by the integrity of assets within the Information Systems Service of Tech Company. The catalog data is a critical asset within the information system service because it contains information related to the offered products and the profiles of the ordering clients. The integrity of the information contained within it must be safeguarded for security purposes and the catalog data is critical data within in the information system service, as it contans information related to the offered product and the profils of client who place orders. The information contained within it must be maintained with integrity to ensure its security.

3. Identifying *Containers* in Information Assets

In this stage, identification is conducted to obtain information regarding the storage, transportation, and identification processes of the assets in order to explore potential risks that may occur. Information asset containers consist of three parts, namely technical containers, physical containers, and people containers, each with internal and external dimensions. The results obtained from the identification process of these information asset containers can be acquired through interviews with individuals who have a connection to Tech Company, including staff working within the organization. The quesionare consists of 3 parts: technical,physcial, and people containers. The technical scenario quesioanre will be given to the IT division team of company. And this step involves the documentation process of the information assets present in the information system services. It will also include a question and answers process using a questionare to asses the impact of risk on the information system service and the respondents, who are employes and it administator fill out the threat scenarios questionnaire and the scenarios are as follows. First Scenario internal threats within the organization could lead to the exposure of information assets, allowing unauthorized parties to use the illegally. Second scenario external threats, unintionally,disclose information assets to unauthorized individualis, petoentially leading to modification, distruptions, and damages to the system, making it inaccesible as intented.

4. Identifying Problem Areas

Identification is carried out regarding the areas of concern, which are divided into three parts: technical (TC), physical (Phc), and people (PC). This step will involve elaborating on detailed descriptive statements regarding the conditions occurring within the institution that are related to factors that can affect the assets in the Information Systems Service and at this stage, documentation will be carried out regarding the threatening information found in all activities that have been identified in the previous stages. This stage will adopt steps 6,7 and 8 of OCTAVE Allegro. In this phase, it will include details of each ponit found in the area of concern along with the potential risk consequences that may arise thereafter. Futhermore, a calculation of the relative risk score will be conducted, and risk mitigation approaches required will br develop. Result of the risk profile documentation covering the area of concern tehcnical containers 2 indicate that occurance of distruption due to system devices undergoing updates is rated as low, with a relative risk score 15.Therefore, the total risk score falls into pool4. The recomendatioan action to be taken is to accept the risk, as the threat is asseseed to be low. The decision regarding this mitigation approach depends on the specific circumstances of the problem and a reevaluation of the risk impact.

Table 3. ***Area Of Concern***

No	Area Of Concern	Kode	Security Requirments
Technical Container			
1	The cessation of company information system services is due to internet connectivity issues.	TC-1	1) Availabillity
2	The information system service of company is experiencing disruption due to updates on the system devices.	TC-2	1) Availabillity
3	The information system service of company is disrupted due to a server that is currently down.	TC-3	1) Availabillity
4	The system security vulnerability contains a loophole that can be freely accessed by unauthorized and irresponsible parties.	TC-4	1) Confidentialitty 2) Integrity
5	The information system services company are disrupted due to a crash in the service and operation system.	TC-5	1) Availabillity
Physical Container			
6	The information system service of company is interrupted due to natural disasters or environmental threats.	PhC-1	1) Availabillity
People Container			
7	There was a human error made by an employee or administrator, which was entering the data incorrectly.	PC-1	1) Confidentialiity 2) Integrity 3) Availabillity
8	The spread of administrator access rights is caused by social engineering.	PC-2	1) Integrity

Table 3 shows the results and describes the determination of mitigation aspects for each specified field.

5. Identifying Threat Scenarios

This step will involve documenting the information assets present in the information systems service. It will include a question-and- answer process using a questionnaire to assess the impact of risks on the information systems service. The reference used for this stage is "Appendix C-Threats Scenarios Questionnaires 1-3." The questionnaire consists of three sections: technical, physical, and people containers. The questionnaire for technical container threat scenarios will be given to the responsible IT staff.

6. Identifying Risk

Calculations will be performed to determine the total score for each impact area based on the reference of the risk measurement criteria obtained in the initial step. The scoring calculation for eachvalue of the impact area can be done as follows:

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

Table 4. ***Impact Area Score***

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
Financial	3	3	6	9

Table 4 shows the results and describes, after performing the calculations, scores will be obtained for each impact area, and then all the scores obtained from the coverage of that impact area. The next step is to sum up the risk profiles.

7. Analyzing Risk

risk analysis process will be conducted for each scope of areas of concern, along with determining the criteria based on low, medium, and high levels. The next stage will involve analyzing the total potential risks by assigning a pool for each scope of areas of concern, using a relative risk matrix as a reference.

Table 5. ***Relative Risk Matrix***

RELATIVE RISK MATRIX			
PROBABILITY	**RISK SCORE**		
	30 to 45	**16 to 29**	**0 to 15**
HIGH	POOL 1	POOL 2	POOL 2
MEDIUM	POOL 2	POOL 2	POOL 3
LOW	POOL 3	POOL 3	POOL 4

Table 5 shows the results and describes Mitigation approach is also needed to be taken as the appropriate step, based on the obtained risk score and its probability level, the mitigation approach.

Table 6. ***Mitigation Approach***

POOL	**MITIGATOIN APPROACH**
POOL 1	MITIGATE
POOL 2	MITIGATE OR DEFER
POOL 3	DEFER OR ACCEPT
POOL 4	ACCEPT

Table 6 shows the results and describes the identification function approach of each approach, indicating what should be done based on the areas of concern.

8. Mitigation Approach

the process of selecting mitigation measures will be carried out. This stage involves detailing the risks identified in step 7, elaborating on the aspects of the risk profile. Furthermore, it includes grouping the risk profiles and prioritizing the risks based on the aspects identified within the previously conducted areas of concern assessment. The determination of mitigation measures can be seen in the table 7. Company risk profile includes the folowinf technical contaners first with risk scores of 15 each, leading to an acceptance of the risk. Second technical containers with a risk score 25, prompts a decision to defer action due to information system distruptions caused by server downtime. Moreover, third technical with a risk score 19 necesitates mitigation measures for addresing the security.

Table 7. Mitigation Determination

No	Code	Areas of Concern	Relative Risk Score	Probabillity	POOL	Mitigation Approach
1	TC-1	information system services is due to internet connectivity issues.	15	**Low**	POOL 4	Accept
2	TC-2	information system service experiencing disruption due to updates on the system devices.	15	**Low**	POOL 4	Accept
3	TC-3	information system service is disrupted due to a server that is currently down.	23	**High**	POOL 2	Defer
4	TC-4	System security vulnerability contains a loophole that can be freely accessed by unauthorized parties.	20	**Medium**	POOL 2	Mitigate
5	TC-5	information system services are disrupted due to a crash in the service and operation system.	19	**Medium**	POOL 2	Defer
6	Phc-1	information system service is interrupted due to natural disasters or environmental threats.	28	**High**	POOL 2	Mitigate
7	PC-1	There was a human error made by an employee was entering the data incorrectly.	20	**Medium**	POOL 2	Mitigate
8	PC-2	The spread of administrator access rights is caused by social engineering.	20	**Medium**	POOL 2	Mitigate

Table 7 shows the results and describes the determination of mitigation aspects for each specified area at company.

Table 8. Recommendation Area of Concern

Mitigation Approach	Code	Area of Concern	Recomendation
Mitigate	TC-4	The presence of security vulnerabilities in the information system service of company can be accessed by unauthorized parties.	The suggested measures are regular updates with the latest version, including security fixes, operating system upgrades, web server updates, and utilizing services that provide security protocols (HTTPS).
	Phc-1	The cessation of company Information System services due to a destructive natural disaster.	The suggested effort is to prioritize recovery based on urgency and business impact, regularly perform backup data and store it separately from the primary storage location.
	PC-1	The occurrence of data input errors made by employees working at company or by administrators who have authority.	The suggested effort to validate data is by adding a warning feature before submitting it in the information system service to prevent data errors.
	PC-2	The occurrence of access rights revocation regarding the company Information System services is due to the happening of a social engineering.	The suggested efforts include adding data verification options before utilizing the service, as well as conducting training and education related to social engineering threats to enhance employees' awareness of social engineering threats.
Defer	TC-3	The disruption of company Information System service is caused by the server currently	Efforts are made by using additional servers to ensure service availability in case one server goes down, so that the traffic can be

		experiencing downtime.	redirected to another server when the main server is disrupted.
	TC-5	The cessation of Information System of company is caused by a crash in the service system or the operating system being used.	Efforts are made to conduct regular testing and maintenance to identify potential issues before a crash occurs. This includes software updates and system cleaning to ensure smooth system operation."
Accept	TC-1	The network connectivity of the Information System service at company is disrupted.	The suggested effort is to monitor the network and implement tools that can detect networks in real-time, enabling quick identification of problems.

Table 8 describes the results of the mitigate approach (carrying out risk reduction) carried out in the area of concern by TC-4, PhC-1, PC-1, and PC-2, the defer approach (delaying) carried out in the area of concern by TC-3, as well as TC-5, and the last approach, namely accept, is carried out in the area of concern by TC-1.

9. CONCLUSION

This study uses the OCTAVE Allegro method to assess the risks in the Information System of Tech Company. The following are the conclusions obtained as a result of the research that has been carried out on the Tech Company information system which was carried out using the OCTAVE Allegro method: Assessment of risk results carried out on the Information System of Tech Company by carrying out the stages of the Octave Allegro method, which begins with determining and identifying the impactareas contained in information assets, determining critical assets from information assets, identifying each container contained in information assets consisting of Technical Container (TC), Physcial Container (PhC), and People Container (PC), and the last one is determining possible threats that arise from each container and determining the critical level of risk, and making recommendations for mitigation of each threat that occurs.

10. REFERENCES

[1] 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.

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

[3] 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/ int ecoms.v3i2.1854.

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

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

[6] GM (2010). *Management Information Systems, 10th Edition* (10th Edition).McGraw- Hill/Irwin.

[7] 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.

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

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

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

[11] 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 ModuleUsing Octave Allegro*. *8*(2), 2709–2722.

[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.2017.80 65754

[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*, https://doi.org/10.1109/CITSM50537.2020.9268845

[14] 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

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

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