Risk Assessment in Empowered Village Information System Services using Octave Allegro Framework

Cantika Juandy Putri Katiandagho
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

The development of science and information technology in the current era plays a very important role in development and management. The use of information technology in an organization cannot be separated from various problems that can affect organizational performance. Some of the problems that can occur include server down due to network or data center disruptions, as well as website break-ins through the insertion of online gambling links. This study aims to conduct a risk assessment on the Empowered Village Information System and prepare recommendations to reduce these risks. Risk assessment was carried out using OCTAVE Allegro, which consisted of 8 steps divided into 4 phases, namely, the establish drivers phase with the step of establishing risk measurement criteria, the profile assets phase with the step of developing an information asset profile and identifying information asset containers, the identify threats phase with the step of identifying areas of concern and identifying threat scenarios, and the phase of identifying and mitigating risks with the step of identifying risks, analyze risks, and choose mitigation approaches. Based on the results of the calculation, 4 approaches were found to reduce risk (mitigate), and 1 approach to accept risk (accept). A relatively high level of risk was identified in Technical Container (TC-1) with a Relative Risk Score of 34, especially in areas of concern server down caused by network or data center aspects. A relatively low risk was identified in the Technical Container (TC-3) with a Relative Risk Score of 23, especially in areas of concern for electricity supply that caused the server to shut down. The results of this study are expected to be a guide for organizations to overcome problems and improve security and readiness for potential future threats in the Empowered Village Information System.

Keywords

Technology, Risk Assessment, Qualitative, OCTAVE Allegro.

1. INTRODUCTION

Science and information technology development play crucial roles in development and management. Almost all sector activities use information technology to help business processes [1]. The Empowered Village Information System is designed to strengthen village development and management, improve administrative efficiency, and support community participation [2].

Imogiri Village, Kapanewon Imogiri, Bantul Regency, D.I Yogyakarta is one of the areas that applies Empowered Village Information System technology. The Combine Resource Institution developed the system in 2017, referring to the Law of the Republic of Indonesia Number 14 of 2008 concerning Public Information Disclosure. The Imogiri Village Empowered Village Information System provides information about administration such as village profiles, village governments, community institutions, village data, and articles. Unwanted events can occur anytime, making it important for organizations to manage risks that could compromise information assets [3]. The risk management process, known as risk analysis, identifies and assesses threats to confidentiality, integrity, and availability [4].

This study uses the OCTAVE Allegro method to outline and analyze risks. OCTAVE Allegro was chosen for its ability to optimize the information security risk assessment process, focusing on the information assets that are used, stored, shared, and how the information is exposed to threats [5]. This study aims to assess risks and prepare recommendations for risk reduction in the Village Information System.

2. LITERATURE STUDY

2.1 Information System

The system must meet each user's needs and specifications to store, process, and manage information [6]. Information is the provision of information or data received by each component of the system as a result of management to obtain relevant knowledge [7]. An information system is designed to manage data quickly and accurately, reduce time problems, and increase efficiency [8].

2.2 Empowered Village Information System

Empowered village information system is an approach that combines information system concepts with empowered village principles to improve information management and community empowerment. The Village Information System is a village e-government project that functions as an application that assists village governments in storing data [9].

2.3 Information System Security

To handle and control Information Systems Security, it is important to consider three main aspects which are [16]:

1. Confidentiality: Guarantees that information can only be accessed by authorized authorities
2. Integrity: Ensures that data is not altered without permission from the authorities, as well as maintaining the accuracy and integrity of information.
3. Availability: Ensures that data can be accessed when needed, anytime and anywhere.

2.4 Risk Management

Risk management is a continuous process of identifying, analyzing, evaluating, and controlling potential risks that may arise in achieving organizational goals. This process includes developing strategies to minimize the negative impact of risk. Effective risk management encompasses a variety of processes, methods, and techniques that assist organizations in making informed decisions and better managing uncertainty [10].

2.5 OCTAVE Methodologies

There are 3 types of OCTAVE methodology, namely:

2.5.1 Method OCTAVE

The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method is a framework for information risk management and cyber security. This method is a tool, strategy, and approach used to provide an assessment and planning of information systems security strategies based on the identification, prioritization, and management of data security risks [11].

2.5.2 OCTAVE-S methods

The OCTAVE-S method is an OCTAVE approach designed for small organizations. This method can help in conducting risk assessments and finding the key IT assets of the organization. OCTAVE-S can also identify vulnerabilities and threats to those IT assets and assess the level of possible threats [12].

2.5.3 Method OCTAVE Allegro

The OCTAVE Allegro method is part of certain initiatives. OCTAVE Allegro is a simplified process that provides robust risk assessment results with less time and resources, and requires no experience in information systems security or risk management [13]. The steps of OCTAVE Allegro can be seen in Figure 2.

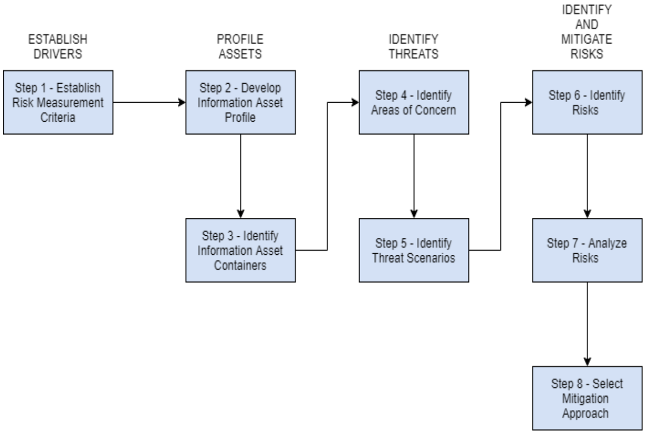
ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE RISKS
Step 1 - Establish Risk Measurement Criteria
Step 2 - Develop Information Asset Profile
Step 3 - Identify Information Asset Containers
Step 4 - Identify Areas of Concern
Step 5 - Identify Threat Scenarios
Step 6 - Identify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

Figure 1. Steps of the OCTAVE Allegro method

3. METHODOLOGY

3.1 Data Collection Methods

This study used various methods to collect the necessary data. The method is described through the following sub-subs:

1. Observation
   The observation method is a way of collecting data through direct observation of the Imogiri Kalurahan Empowered Village Information System. Observations are made to gather basic information about the study. This basic information is used to identify problems to be studied in research [14]. Observation can help in understanding the context of the research environment in more depth.
2. Literature Study
   A literature study is a method of collecting data by looking for written sources related to an event or problem in research. These written sources include books, magazines, and academic articles. This method can also help in understanding relevant theories and concepts and contribute to the field of study.
3. Interview
   An interview is a data collection technique that involves the process of interaction with resource persons. In this case, ask questions directly to the relevant parties [15]. The interviews were conducted in two places, namely the Imogiri Village, and the Bantul Communication and Information Office.
4. Questionnaire
   A questionnaire is a tool or instrument used to collect data from respondents in the form of written questions. The research questionnaire is based on references from the OCTAVE Allegri v.1.0 OCTAVE Allegro approach, the questionnaire refers to the section "Appendix C-OCTAVE Allegro Questionnaires" [19]. The questionnaire refers more to the information security methodology.

4. RESULTS AND DISCUCCION

4.1 Step 1: Establish Risk Measurement Criteria

Step 1 has 2 activities. Activity 1 is a risk measurement criterion based on interviews that determines the quality of each area according to the risk (low, medium, high). Areas assessed for quality include user reputation/trustworthiness, financial, productivity, health and safety, and fines/legal sanctions [18]. Here are the impacted areas selected in Activity 1:

1. Areas of impact of Reputation in Village Information Systems: dampak reputasi dapat bervariasi dari rendah hingga tinggi. Low occurs if the issue is internal and does not affect the user, such as a technical error that is not publicly known. Medium impact requires public calibration, such as correcting misinformation or explaining issues that can affect public perceptions. High Impact involves situations that require a reputation recovery campaign through the media, such as a wide-impact system failure. User trust is also affected on the same scale: the Low impact affects only a few users without a significant change in trust, the Medium impact causes discomfort in some users, while the High impact causes a loss of trust by many users, which affects village operations and can decrease public participation in village programs.
2. Areas of financial impact in Village Information Systems: dampak finansial mencakup variasi biaya yang terkait dengan kerusakan atau pemeliharaan sistem. Low impact occurs when damage is repaired at no additional cost, such as routine repairs that are already included in the operating budget. The impact of Medium involves replacing hardware such as routers that require costs, but are still within the village budget. High impacts occur if severe damage requires the replacement of the entire system at a significant cost and over budget, forcing villages to seek additional funding. An in-depth evaluation of the potential long-term impact and strategies for addressing unexpected costs is also important for financial planning.
3. Areas of impact on productivity in the Village Information System: dampak produktivitas bervariasi dari rendah hingga tinggi. Low impact occurs if the system functions properly without interfering with admin tasks, so productivity remains stable. The Medium Impact shows that disruptions in the system affect productivity that do not significantly change working hours, for example through a less drastic decrease in efficiency. High impact occurs when a system outage causes a significant decrease in productivity, interferes with other tasks, and forces admins to work overtime, which requires mitigation strategies to restore the system and reduce disruption.
4. Health and Safety impact areas in Village Information Systems: In all Low, Medium, and High categories, risks associated with information systems do not affect the health or safety of the individuals involved. This is because the impact of information systems is more technical and administrative, with no direct impact on physical or mental conditions. However, it is important to ensure that risks that are not related to health and safety are managed properly to maintain a safe work environment.

5. Areas of impact of fines in the Village Information System: the impact of fines and legal sanctions can vary from low to high. Low impact means that no fines are applied, while Medium impacts involve fines for minor violations such as the dissemination of misinformation. High Impact involves large fines or heavy sanctions for serious offenses such as vandalism or illegal access, which can incur heavy financial and reputational burdens. For a legal sanction, Low impact means no legal action, a Medium impact involves minor offenses with administrative sanctions, and a High impact involves serious offenses with severe sanctions, such as imprisonment or a large fine. Mitigation strategies focus on preventing violations and over-handling must be implemented to reduce the risk of fines and sanctions.

Next, Activity 2 is to determine the priority scale. This priority determines the value of the company's impact area from highest to lowest [21]. The score uses a scale of 1-5, where scale 1 indicates the lowest priority and scale 5 indicates the highest priority. Table 1 shows the determination of the score.

Table 1. Impact Area Prioritization

Allegro Worksheet 7	**IMPACT AREAS PRIORITIZATION WORKSHEET**
Priority Score	**Impact Areas**
5	User Reputation and Trust
4	Financial
3	Productivity
2	Safety and Health
1	Fines and Legal Sanctions

The results of Table 1 explain that:

1. Reputation and user trust (Score 5): has the highest priority because user reputation and trust affect the sustainability and long-term success of the Village Information System. Damage to these areas can result in a widespread loss of trust, which has a direct impact on the participation and effectiveness of the system.
2. Financial (Score 4): being the second priority, with risks that include large costs for recovery, technology updates, or routine maintenance such as system security. Financial problems can affect the budget and the continuity of the system's operations.
3. Productivity (Score 3): this is the third priority because system disruptions can hinder access to information reduce productivity and interfere with working hours. Declining productivity can hinder village administrative and operational functions.
4. Health and Safety (Score 2): although risks to health and safety are rare in the context of village information systems, this area is still important to ensure that the system does not pose health or safety concerns for staff and users.
5. Legal Fines and Sanctions (Score 1): has the lowest priority although it is important for compliance with applicable laws and standards. The impact is often more modest than the impact on reputation, finances, and productivity, but it still needs to be considered to avoid breaking the law.

4.2 Step 2. Develop Information Asset Profile

Step 2 is the identification of the collection of information assets. The second activity focuses on the results of business process identification and documenting the results of identification [22]. This will help identify all points where information assets may be vulnerable to unauthorized access, alteration, loss, or damage, as well as tampering. More details can be found in Table 2.

Table 2. Critical Information Asset Profile

<table>
<tr><td><b>Allegro Worksheet 8</b></td><td colspan="3"><b>CRITICAL INFORMATION ASSET PROFILE</b></td></tr>
<tr><td><b>(1) Critical Asset</b>
What are critical information assets?</td><td><b>(2) Rationale for Selection</b>
Why are these information assets important in organizations?</td><td colspan="2"><b>(3) Description</b>
What is the description of the information asset?</td></tr>
<tr><td>Population data</td><td>Population data is a systematic recording of the population of an area and ensures that development is carried out truly to meet the needs of the community.</td><td colspan="2">Population data contains information on education, occupation, religion, gender, blood type, age group, country color, analysis, marriage, and family relationships.</td></tr>
<tr><td colspan="4"><b>(4) Owner(s)</b>
Who owns the information asset?</td></tr>
<tr><td colspan="4">Imogiri Village, Bantul, Yogyakarta</td></tr>
<tr><td colspan="4"><b>(5) Security Requirements</b>
What are the security needs for information assets?</td></tr>
<tr><td>Confidentiality</td><td colspan="3">Only authorized or access-authorized personnel can input or delete information assets.</td></tr>
<tr><td>Integrity</td><td colspan="3">Only authorized personnel can modify such information assets</td></tr>
<tr><td>Availability</td><td colspan="3">The asset must be available every hour, day/week, week/year.</td></tr>
<tr><td>Other</td><td colspan="3">Assets aforementioned have specific regulatory compliance protection requirements
.</td></tr>
<tr><td colspan="4"><b>(6) Most Important Security Requirement</b>
What are the most important security needs for those information assets?</td></tr>
<tr><td>Confidentiality</td><td>Integrity √</td><td>Availability</td><td>Other</td></tr>
</table>

The results of Table 2 explain that critical information assets are Population Data Information, which contains important data about the population of an area and is the basis for accurate development planning. Asit was chosen because of the importance of ensuring that development policies are based on the right demographic data. This information includes education, occupation, religion, gender, blood type, age, citizen status, marital status, and family relationships, which is useful for analysis and decision-making. This asset is owned by Imogiri Village, Bantul, Yogyakarta, and is managed with three main security needs: Confidentiality, Integrity, and Availability. Only authorized personnel access, modify, or delete data, ensuring its confidentiality and integrity.

4.3 Step 3: Identify Information Asset Containers

Step three is to identify the information asset container. Information asset containers have 3 types, namely Technical Containers, Physical Containers, and People Containers [20]. The step of identifying information asset containers is carried out through the interview stage. The identification process in Technical Containers includes both external and internal sides. On the internal side are servers, network devices, computer devices, and applications, while on the external side is an internet network. At the Physical Container identification stage, there is no separation of the external and internal sides because the information asset is already in the form of data. For the identification of People Containers, there are external and internal sides. On the internal side, there are district admins and Bantul communication and informatics office admins, while on the external side, there are institutional partners.

4.4 Step 4: Identify Areas of Concern

The fourth step is a statement of possible situations and conditions that could threaten information assets. From the results of the interviews that have been conducted, there are only 2 containers that are included in the area of concern, namely the Technical Container (TC) and the People Container (PC). TC includes a variety of technological devices and infrastructures used to store and process information, while PC involves individuals or groups that have access to information assets. This identification is crucial because each container has different potential threats. The following are the results of the identification of information asset containers that have been encoded respectively, such as Technical Container (TC) and People Container (PC). Each identification can be viewed in detail in Table 3.

Table 3. Area of concern

No	Area of Concern	Code	Requirements Security
Technical Container			
1	Server downtime is caused by many aspects such as network aspects or data center aspects	TC-1	1. Availability
2	Dissemination of online gambling links into the SID Kalurahan website	TC-2	1. Integrity 2. Confidentiality
3	Problems with the power supply that cause the server to stop	TC-3	1. Availability
4	Full Storage	TC-4	1. Availability
People Container			
5	The risk of data disclosure comes from human error	PC-1	1. Integrity 2. Confidentiality

4.5 Step 5: Identify Threat Scenarios

The fifth step is to describe the threat, including considering probability. Since a company or organization has more specific operations, this will help determine the situation. The identification process refers to the "Appendix C-Threats Scenarios Questionnaire 1-3". This questionnaire is divided into 3, namely technical containers, physical containers, and people containers. In the Technical Container questionnaire, 2 threats have occurred, namely interference from dangerous codes and natural disasters. The Physical Container questionnaire was not given because there were no identified physical containers in the Imogiri Village Empowered Village Information System. Meanwhile, in the people container questionnaire, some threats occur due to inadvertent ness that results in the disclosure of information assets to unauthorized people.

By describing threats in detail, organizations can more easily identify potential risks and establish appropriate mitigation measures. This process also includes an assessment of the likelihood of such a threat, thus providing a clearer picture of the level of urgency of each threat. Defining threats based on specific container types helps organizations focus on areas that need more attention, so resources can be allocated more effectively to protect critical information assets. By doing so, organizations can develop a more comprehensive and proactive security strategy. As a result, an organization's ability to respond to security incidents will be significantly improved.

4.6 Step 6: Identify Risks

The sixth step is the preparation of threat scenarios that have been identified. Identification is carried out based on threat scenarios according to the list of areas of the concert, and in this step, a relative score will be calculated. The relative score will be calculated by shifting the priority score contained in Step 1. High (n = 3), medium (n = 2), and low (n = 1) risk levels. Each threat scenario will be analyzed to determine its level of risk. The results of this analysis will be the basis for prioritizing mitigation actions. The score calculation method for each impact area is as follows [17]:

1. If the first impact area is entered at a low-risk level, it is diverted with the number 1, so the formula becomes (nPriority x nL=1).
2. If the first impact area is at the medium risk level, it is diverted with the number 2, so the formula becomes (nPriority x nL=2).
3. If the first impact area is entered at a high-risk level, it is diverted with the number 3, so the formula becomes (nPriority x nL=3).

Once the score is obtained, the next step is to determine the necessary mitigation measures. Mitigation measures should be designed to mitigate risk according to the threat scenarios that have been identified, with special attention to areas with high-risk scores. This step is important to ensure that all risks that have been identified are properly addressed. Periodic evaluations are also needed to assess the effectiveness of the mitigation measures that have been implemented. Score identification results from each area can be seen in Table 4.

Table 4. Area of concern

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

4.7 Step 7: Analyze Risks

The seventh step is the stage of total risk analysis from the results of steps 4, 5, and 6 by reviewing the calculation of the relative risk value. This calculation process aims to analyze risks and determine the right strategy for dealing with risks. Each activity at this stage refers to the information asset risk worksheet to obtain an optimal strategy [23]. The results of the risk analysis are obtained by calculating the score of each impact area that has been identified. Furthermore, an analysis of the number of risk points across all areas of concern is carried out, which comes from identifying previous threats through a profiling process. Thus, each risk is prioritized based on its risk area using Allegro Worksheet 10 [25]. The relevant risk areas can be seen in Table 5.

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

Code	Area of Concern	Reputation and Trust	Financial	Productivity	Safety and Health	Fines and Penalties	Risk Score	Probability	Mitigation Approach
TC-1	Server downtime is caused by many aspects such as network aspects or data center aspects	High (15)	Low (4)	High (9)	Low (2)	Low (1)	34	Medium	Mitigate
TC-2	Dissemination of online gambling links into the SID Kalurahan website	High (15)	Low (4)	High (9)	Low (2)	Medium (2)	32	High	Mitigate
TC-3	Problems with the power supply that cause the server to stop	Medium (10)	Low (4)	Medium (6)	Low (2)	Low (1)	23	Low	Accept
TC-4	Full Storage	Medium (10)	Medium (8)	High (9)	Low (2)	Low (1)	30	Medium	Mitigate
PC-1	The risk of data disclosure comes from human error	High (15)	Low (4)	High (9)	Low (2)	Medium (2)	32	High	Mitigate

The next stage is to group the number of threats in each category to facilitate mitigation, as seen in Table 6.

Table 6. Gruping Number of Threats

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

The results of Table 6 show the grouping of the number of threats, so it can be seen that Technical Containers have more threat risk with the number of 4. Meanwhile, the People Container only has 1 threat risk.

4.8 Step 8: Select Mitigation Approach

The eighth and final step in the OCTAVE Allegro method combines a qualitative description of the probability of risk with the priority of risk impact based on organizational criteria. At this stage, mitigation approaches are chosen by grouping each area of concern based on the relative scores that have been identified [24]. The mitigation plan aims to reduce threat risks based on areas of concern, and the results can be seen in Table 7.

Table 7. Grouping based on the Mitigation Approach

Mitigation

Mitigation Approach	Code	Area of Concern	Recommendation
Mitigate	TC-1	Server downtime is caused by many aspects such as network aspects or data center aspects	Regular Maintenance: Schedule regular checks on routers, switches, and firewalls to ensure all devices are functioning optimally and that there are no connection issues that could potentially cause the server to go down. IT Training: Train your IT team regularly to ensure they can handle network and data center issues quickly and effectively.

	TC-2	Dissemination of online gambling links into the SID Kalurahan website	Security Testing: Conduct periodic inspections to identify security loopholes that can be exploited for online gambling link insertion. Routine Backups: Create Schedule regular backups for website data, so that in the event of a compromise, the site can be immediately restored to a secure version.
	TC-4	Full Storage	Storage Monitoring: Use monitoring tools to monitor storage capacity usage in real-time, so that it can be anticipated immediately before it reaches its maximum limit. Capacity Increase: When capacity is near, increase storage to keep running uninterrupted.
	PC-1	The risk of data disclosure comes from human error	Training and Education: Conduct regular training for those in charge of data security in the district, or provide easy-to-access video guides. User Activity Monitoring: Use tools such as monitoring tools or observe IT to monitor user activity, so that errors or data misuse can be addressed before they cause bigger problems.
Accept	TC-3	Problems with the power supply that cause the server to stop	Use of UPS or ESS: Install an Uninterruptible Power Supply (UPS) or Energy Storage System (ESS) that can provide backup power during a power outage or when the generator is damaged. Make sure this system is strong enough to maintain the server during an outage until power is restored.

5. CONCLUSION

Risk assessment of Empowered Village Information System services in Imogiri District is carried out based on steps by the OCTAVE Allegro method. The risk assessment process begins by establishing risk measurement criteria and determining the priority of each impact area. The next step is to identify crucial information assets and create profiles for each of them. After that, container information assets such as technical containers, physical containers, and people containers are identified, and each container's area of concern (area of concert) is assigned. Next, risks are identified and analyzed by determining severity, then mitigation approaches are selected based on risk values and probabilities. Finally, mitigation strategy recommendations are drawn up for each identified area of concern. The results of research on the Imogiri Kalurahan Empowered Village Information System obtained mitigation approaches, namely 4 areas of concern with a mitigate approach, and 1 area of concern with an accept approach. A relatively high-risk score is found in Technical Containers with a score of 32 in the area of concern related to server down, which affects many aspects such as network aspects or data center aspects. While the risk value is relatively low in the Technical Container with a total score of 21 in the area of concern related to problems in the electricity supply that cause the server to stop. It is recommended to regularly hold workshops or internal training for staff related to information risk management. This training aims to increase staff's understanding of risk mitigation and effective measures, as well as become a forum for various experiences and best practices to face future information security challenges.

6. REFERENCES

[1] Budarsa, N. (2022). Information Security Risk Analysis Using Octave Allegro Method and Analytical Hierarchy Process at the Buleleng Regency Government Data Center. 7, 13–15.

[2] Isnaeni, S., &; Herzanita, A. (2022). Risk Management Analysis On Box Girder Cast-In Situ Work Study Case Case Halim Station Jakarta-Bandung High-Speed Railway. Artesian Journal, 2(2), 175–184.

[3] Zulfia, A., Ruskan, E. L., &; Son, P. (2021). Risk Assessment of Information Assets with the Octave Allegro Method: ICT Case Study Faculty of Computer Science, Sriwijaya University. Joins (Journal of Information System), 6(1), 40–47. https://doi.org/10.33633/joins.v6i1.4088.

[4] Muka, W., &; Wibowo, M. A. (2021). Application of Risk Management in Property Development Process. Journal of Settlements, ,(1),31.https://doi.org/10.31815/jp.2021.16.31-40

[5] Armadyana, R., Yasirandi, R., &; Makky, M. Al. (2023). Information Security Risk Analysis and Assessment using Octave Allegro (Case Study: PT . XYZ). 10(3), 3690–3703.

[6] Hidayatulloh, N. W., Dellia, P., Informatics, P., Education, F. I., &; Madura, U. T. (2023). 1,2 1 , 2. 15(2), 3330–3342.

[7] Dwi Lestari, I., Samsugi, S., &; Abidin, Z. (2020). Design a mobile-based part-time job information system in the Bandar Lampung area. Telefortech: Journal of Telematics and Information Technology, 1(1), 18–21. https://doi.org/10.33365/tft.v1i1.649

[8] Agustino, R., Widodo, Y. B., Wiyatno, A., &; Saputro, M. I. (2020). Research and Community Service Information System at Mohammad Husni Thamrin University. Journal of SainTek Nets, 2(1), 1–12. https://doi.org/10.31599/jaring-saintek.v2i1.61

[9] Sulistyowati, F., Tyas, H. S., Dibyorini, M. C. R., & Puspitasari, C. (2021). Utilization of Village Information System (SID) to Realize Smart Village in Kalurahan Panggungharjo, Sewon, Bantul, DI Yogyakarta. Journal of Science and Technology-Kom (Journal of Communication Science and Technology), 23(1), 213–226.

[10] Saputra, R. R., Ambarwati, A., &; Setiawan, E. (2020). Information Technology Risk Management Using Octave Allegro at Pt.Hd. Journal of Science, Technology and Industry, 17(1), 1. https://doi.org/10.24014/sitekin.v16i2.7457

[11] Hamzah, R. F., Jaya, I. D., &; Putri, U. M. (2020). E-LKP Information System Security Risk Analysis with Octave Method at State Universities X. Jusifo, 6(1), 55–65. https://doi.org/10.19109/jusifo.v6i1.5880

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

[13] A, R. R., &; Bisma, R. (2021). Risk Mitigation Planning Using the Octave Allegro Method at SMA Semen Gresik. 02(02), 17–23.

[14] Agustin, R. A., Nengsih, W., Muslim, I., &; Zulvi, M. S. (2023). ISSN Print: 2085-1588 ISSN Online: 2355-4614 Website-Based Cement Distribution Information System with E-Supply Chain Management Approach ISSN Print: 2085-1588 ISSN Online: 2355-4614 Supported by advances in the world of information technology in the present, ba. 15(2), 3315–3329.

[15] Yoewono, J. O., &; Prasetyo, A. H. (2022). Risk Management Design and Process at Pt Surya Selaras Cita. Journal of Estuary Economics and Business, 6(1), 56. https://doi.org/10.24912/jmieb.v6i1.12207

[16] Nurul, S., Shynta Anggrainy, & Siska Aprelyani. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). Jurnal Ekonomi Manajemen Sistem Informasi, 3(5), 564–573. https://doi.org/10.31933/jemsi.v3i5.992

[17] Diahapsari, A., & Riadi, I. (2022). Analysis Risk Assessment on Hospital Management Information System using Octave Allegro Framework. International Journal of Computer Applications, 184(24), 27–34. https://doi.org/10.5120/ijca2022922286

[18] Ramjanati, P., Wijaya, F. K., &; Muarie, M. S. (2021). Information Security Risk Assessment Using Octave Allegro: A Case Study in Higher Education. Jusifo (Journal of Information Systems), 7(1), 10–20. https://doi.org/10.19109/jusifo.v7i1.5870

[19] Ningsih, N. F., & Riadi, I. (2021). Risk Assessment Analysis on Library Information System using Octave Allegro Framework. International Journal of Computer Applications, 183(28), 6–13. https://doi.org/10.5120/ijca2021921620

[20] Kartika, N. C., & Riadi, I. (2023). Analysis of Risk Management on Dapodik System Services using Octave Allegro Framework. International Journal of Computer Applications, 185(11), 37–44. https://doi.org/10.5120/ijca2023922759

[21] Deva, B. S., &; Jayadi, R. (2022). Risk Analysis and Information Security in a System Integrator Company Using the Octave Allegro Method. Journal of Technology and Information, 12(2), 106–117. https://doi.org/10.34010/jati.v12i2.6829

[22] Anggraini, E., & Riadi, I. (2021). Analysis of Risk Assessment on Electronic Services using Octave Allegro Framework. International Journal of Computer Applications, 183(5), 26–32. https://doi.org/10.5120/ijca2021921273

[23] Naibaho, B. S. G., &; Tjahjadi, D. (2022). Information System Risk Management Study Using Octave Allegro Method. Justice: Scientific Journal of Informatics Engineering and Information Systems, 11(1), 131. https://doi.org/10.35889/jutisi.v11i1.758

[24] Afrininda, R. R. (2021). Risk Management Analysis of Online Exam Applications with the Octave Allegro Method in Educational Institutions. Justindo (Indonesian Journal of Information Systems and Technology), 6(2), 62–73. https://doi.org/10.32528/justindo.v6i2.4546

[25] Tristania, S. D. P, & Riadi, I. (2022). Analysis of Risk Management on Learning Management System using Octave Allegro Framework. International Journal of Computer Applications 184(34), 37-44. 10.5120/ijca2023922759