Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 2, July 2023
https://doi.org/10.47709/cnahpc.v5i2.2524

Submitted : July 15, 2023
Accepted : July 16, 2023
Published : July 17, 2023

Risk Analysis of Information Security in Balikpapan International Airport Service Desk Plus (SDP) Using The Octave Allegro Method

Novi Indrayani[1)*], **Norma Amalia**[2)]
[1)2)]Faculty of Computer Science, Mulia University, Indonesia
[1)]novi.indrayani09@gmail.com, [2)]normaamalia@universitasmulia.ac.id

ABSTRACT

Indonesia, as a developing country, is not exempt from the advancements in information and communication technology. However, these advancements in information and communication technology can bring negative impacts, such as an increasing threat of misuse. SDP (Service Desk Plus) is a system that serves as a management tool for IT services, facilitating employees from various departments in requesting services and reporting ICT (Information Communication Technology) incidents. SDP has faced challenges or obstacles that have hindered its optimal use, such as IT services experiencing downtime, inaccessible ICT services, and SDP users frequently sharing usernames and passwords. Based on these threats, it is necessary to conduct a further analysis of information security risks regarding the security of implementing SDP centrally using the OCTAVE Allegro method. OCTAVE Allegro is a framework that utilizes the OCTAVE approach with a primary focus on information assets, designed to provide faster results without requiring in-depth knowledge of risk assessment. The results of this research identified three risks that can be mitigated, namely user data password errors with a relative risk score of 27, internet downtime with a relative risk score of 31, and file intrusion with a relative risk score of 38, considering the likelihood of threats occurring. Additionally, there is one accepted risk, which is the input error of incident data, with a relative risk score of 19.

Keywords: Analysis, Risk, Security, SDP (Service Desk Plus), OCTAVE Allegro

1. INTRODUCTION

Indonesia, as a developing country, is inevitably influenced by the advancements in information and communication technology. With its development, information and communication technology plays a significant role in various fields, providing convenience to its users. However, this progress can also bring negative impacts, particularly the increasing threat of information and communication technology misuse.

According to Whitman and Mattord (2010), information security is a form of protection for information and its essential elements, such as confidentiality, integrity, and availability. This applies to systems and hardware used to store and transmit information. Information security also helps minimize risks from various threats to assets, whether physical or network access-related.

SDP (Service Desk Plus) is a system that serves as a management tool for IT services, facilitating employees from all departments in requesting services and reporting ICT (Information Communication Technology) incidents. This system supports the central activities of the company, which may introduce certain risks. In the implementation of this centralized SDP system, Sultan Aji Muhammad Sulaiman Sepinggan International Airport branch acts as a client, which means that risks can arise due to network connections and interconnections. Previous issues have occurred, such as IT services experiencing downtime, inaccessible ICT services, and SDP users frequently sharing usernames and passwords. Given these threats, further research and risk analysis are necessary to evaluate the security of implementing SDP centrally using the OCTAVE Allegro method. The OCTAVE Allegro method is chosen because it allows for risk identification, risk analysis, risk assessment, and mitigation approaches.

2. LITERATURE REVIEW

Several studies have explored the application of the OCTAVE Allegro method in analyzing and managing information security risks within various organizational contexts. Abdullah, Isnainiyah, and Faried (2020) conducted a risk management analysis on an organizational website, highlighting the effectiveness of the OCTAVE Allegro

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 2, July 2023
https://doi.org/10.47709/cnahpc.v5i2.2524

Submitted : July 15, 2023
Accepted : July 16, 2023
Published : July 17, 2023

method in identifying and mitigating risks associated with website vulnerabilities and security breaches (Abdullah, Isnainiyah, & Faried, 2020). Similarly, Deva and Jayadi (2022) performed a risk and information security analysis in a system integrator company, emphasizing the importance of systematically assessing risks and implementing security measures (Deva & Jayadi, 2022). Additionally, Herdianto, Ramli, and Suryanto (2022) conducted a risk assessment of electronic archive services, demonstrating the applicability of the OCTAVE Allegro method in identifying vulnerabilities and ensuring the confidentiality, integrity, and availability of electronic archives (Herdianto, Ramli, & Suryanto, 2022).

The standardization of information security plays a crucial role in achieving effective security practices within organizations. Andersson, Hedström, and Karlsson (2022) conducted a structurational analysis, emphasizing the importance of standardization and highlighting the complexities involved in implementing standardized security measures (Andersson, Hedström, & Karlsson, 2022). This highlights the need for organizations to adopt standardized frameworks and practices to ensure consistent and robust information security.

The OCTAVE Allegro methodology has been introduced as an improved risk assessment process for information security. Caralli, Stevens, Young, and Wilson (2007) highlighted the benefits of the OCTAVE Allegro method in effectively identifying and prioritizing risks, providing organizations with a structured framework for risk assessment and mitigation (Caralli, Stevens, Young, & Wilson, 2007).

Several studies have applied the OCTAVE Allegro method to specific contexts. Legowo and Saputra (2019) conducted risk management of credit card payment gateways, highlighting the importance of the OCTAVE Allegro method in identifying and mitigating risks associated with secure transactions and customer information protection (Legowo & Saputra, 2019). Nastiti and Haryani (2022) performed a risk analysis of the information security in the e-gov Siskeudes system, showcasing the value of the OCTAVE Allegro method in ensuring the confidentiality, integrity, and availability of government information systems (Nastiti & Haryani, 2022).

Understanding related concepts and frameworks is essential in the context of information security and risk management. The International Standard (2013) provides comprehensive guidelines for information security management systems, serving as a reference for organizations seeking to establish effective security practices (International Standard, 2013). O'Brien (2005) introduced the concept of information systems, highlighting their significance in managing organizational data and processes (O'Brien, 2005). Oluwatosin (2014) explored the client-server model and its implications for information technology systems, considering the potential risks associated with data communication and exchange (Oluwatosin, 2014). Furthermore, Ramadhintia and Bisma2 (2021) emphasized the importance of proactive risk management strategies in educational institutions (Ramadhintia & Bisma2, 2021).

In summary, the literature review highlights the application of the OCTAVE Allegro method in risk management analysis within various organizational contexts. It emphasizes the importance of standardization in information security practices and explores relevant concepts and frameworks. These studies provide insights into the effective assessment and mitigation of information security risks using the OCTAVE Allegro method, enabling organizations to enhance their security measures and protect valuable assets.

3. METHOD

This research utilized a descriptive analysis method with a qualitative approach. The qualitative descriptive research approach was chosen to describe and depict the research findings based on data obtained from the objects under study. The data collection techniques employed in this research were as follows:

1. Direct Observation: Direct observation was conducted at Sultan Aji Muhammad Sulaiman Sepinggan Balikpapan International Airport to observe the implementation of SDP (Service Desk Plus).
2. Interviews: Interviews were conducted with the Airport Technology Officer and the Airport Safety Risk and Performance Management Department to obtain relevant data or information directly related to the assets and security of SDP (Service Desk Plus).
3. Literature Review: This involved reading, studying, and comprehending various sources, including books, e-books, journals, and previous research that were relevant to the researched problem.

The data analysis method used in this research was the OCTAVE Allegro method, which involved filling out worksheets according to the OCTAVE Allegro framework. OCTAVE Allegro is a framework that utilizes the OCTAVE approach with a primary focus on information assets, designed to yield faster results without requiring in-depth knowledge of risk assessment. All other assets important to the organization were identified and assessed within the

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 2, July 2023
https://doi.org/10.47709/cnahpc.v5i2.2524

Submitted : July 15, 2023
Accepted : July 16, 2023
Published : July 17, 2023

context of the connected information assets. In OCTAVE Allegro, all relevant information about the risks to information assets was captured using Allegro worksheets.

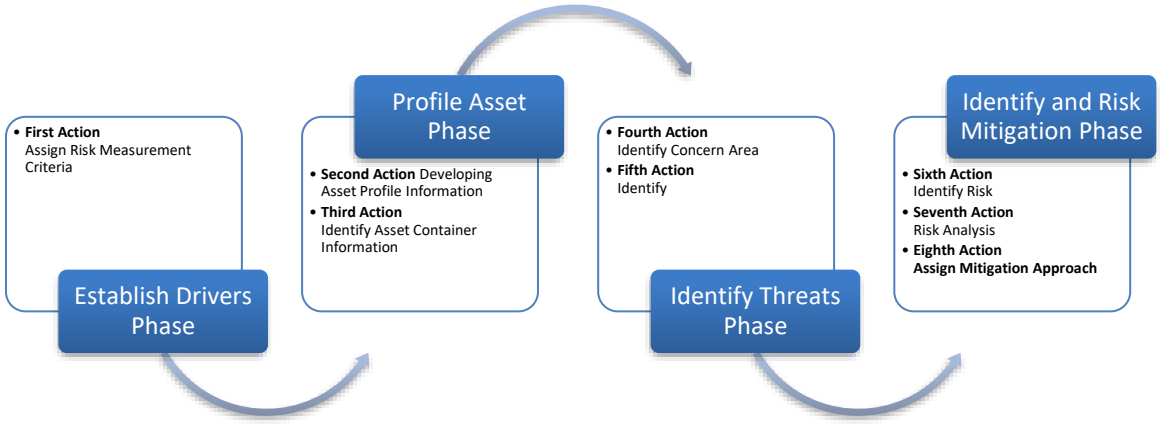

Fig. 1 Steps of OCTAVE Allegro Method

The OCTAVE Allegro method consists of four phases:

1. The first phase is establishing drivers, developing risk measurement criteria based on the organization's strategic goals, vision, and mission.
2. The second phase is creating an asset profile, determining important information assets for the organization's business continuity.
3. The third phase is identifying threats that could impact information assets and developing threat scenarios based on three platforms (technical, physical, people).
4. The fourth and final phase is identifying risks and determining mitigation approaches based on the identification results.

Within these four phases, there are eight steps in the OCTAVE Allegro method:

1. Establishing risk measurement criteria: The organization establishes consistent risk measurement criteria as a reference for risk assessment, recognizing the areas of significant impact.
2. Developing an information asset profile: This step ensures that assets are clearly and consistently described through the development of a profile, which represents the features, quality, characteristics, and unique value of the assets.
3. Identifying information asset containers: After determining the information asset profile, containers or holders of information assets are identified. These containers are the places where information assets are stored, transported, or processed, and can become vulnerable points and threats that put the information assets at risk.
4. Identifying areas of concern: This step involves brainstorming potential conditions or situations that could threaten organizational assets. These real-world scenarios are referred to as areas of concern.
5. Identifying threat scenarios: The identified areas of concern are expanded into more detailed threat scenarios.
6. Identifying risks: After creating detailed threat scenarios, the organization determines the consequences of these threat scenarios to complete the risk picture.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 2, July 2023
https://doi.org/10.47709/cnahpc.v5i2.2524

Submitted : July 15, 2023
Accepted : July 16, 2023
Published : July 17, 2023

7. Analyzing risks: This step involves qualitatively measuring the extent to which the organization is affected by threats by calculating risk scores for each information asset.
8. Selecting mitigation approaches: In the final step of the OCTAVE Allegro process, the researcher determines which identified risks require mitigation and develops mitigation strategies for those risks.

4. RESULT AND DISCUSSION

This section will discuss the steps taken in analyzing SDP (Service Desk Plus) using the OCTAVE Allegro method. The first step is establishing risk measurement criteria. By establishing risk measurement criteria, we can determine the impact areas on SDP (Service Desk Plus) based on the Allegro worksheet. In OCTAVE Allegro, there are five impact areas: anti-bribery management system, organizational strategic goals, human resources, occupational health and safety, and reputation, each with a low, medium, or high measurement value. Next, we prioritize the impact areas, giving the highest score to the most important areas and the lowest score to less important areas, as indicated in Table 1.

Table 1
Impact Area Priority

Allegro Worksheet 7	**Impact area prioritization worksheet**
Priority	Impact Areas
5	Anti-bribery management system
4	Organizational strategic goals
3	Human resources
2	Occupational health and safety
1	Reputation

It is essential to identify the assets that hold critical value within the system. These assets can be crucial for the effective functioning and security of SDP. The identification process involves evaluating various components and elements of SDP to determine their significance and impact on the overall system. The identified critical assets are then documented and presented in a tabular format, specifically in Table 2, to provide a clear overview of the assets that require special attention and protection within the SDP environment. This step ensures that appropriate measures can be taken to safeguard these critical assets and mitigate potential risks or vulnerabilities associated with them.

Table 2
Critical Asset Profile I

Allegro Worksheet 8	**Critical Information Asset Profile**
Critical Asset	Network Interconnection
Description	The network that connects client computers to access the SDP server at the head office through the internet.
Owner	PT. (Persero) Angkasa Pura I-SAMS

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 2, July 2023
https://doi.org/10.47709/cnahpc.v5i2.2524

Submitted : July 15, 2023
Accepted : July 16, 2023
Published : July 17, 2023

Security Requirements	
Confidentiality	Technician
Integrity	Technician
Availability	All staff
More Important Security Requirement	Availability

In the analysis of SDP, it is crucial to identify the containers or holders of information assets. These containers refer to the physical components, systems, or environments that store, transmit, or process the information within the SDP system. By identifying these containers, the analysis can focus on understanding the risks associated with the physical aspects of connectivity in the service request reporting process.

Table 3 serves as a visual representation or map that outlines the physical risk environment related to the connectivity process of service request reports in SDP. It provides a detailed overview of the physical elements, infrastructure, or network components that play a role in facilitating the connectivity of the service desk and the transmission of service requests within the system. This information helps in identifying potential vulnerabilities, points of failure, or security risks that may arise in the physical environment, such as network connectivity issues, hardware failures, or physical access breaches.

The purpose of including this table is to enhance the understanding of the physical risk landscape and enable effective risk assessment and mitigation strategies to be implemented within the SDP environment. By considering the physical aspects of connectivity, organizations can better identify and address potential risks that may impact the availability, integrity, and confidentiality of service request data in SDP.

Table 3
Information Asset Risk Environment Map (Physical)

Allegro Worksheet 9	**Information Asset Risk Environment Map (Physical)**
Firewall	PT. (Persero) Angkasa Pura I – SAMS Sepinggan
Router	PT. (Persero) Angkasa Pura I – SAMS Sepinggan

When analyzing the usage of SDP it is important to thoroughly review and evaluate each asset container identified earlier. This review helps identify specific areas that require attention or consideration due to their potential impact on the system's usage and overall performance.

By examining each asset container, such as network connections, databases, user interfaces, or communication channels, organizations can identify potential areas of concern. These areas may include vulnerabilities, points of failure, or specific aspects that require extra attention to ensure smooth and secure usage of the SDP system.

Table 4 serves as a comprehensive representation of the areas of concern specifically related to the usage of SDP. It provides a structured overview of the identified areas that require careful consideration, enabling organizations to prioritize their efforts and allocate appropriate resources for risk assessment and mitigation.

By identifying and addressing the areas of concern, organizations can proactively manage and mitigate potential risks, ensuring the effective and secure utilization of SDP. This contributes to enhancing the overall performance, reliability, and security of the system, resulting in improved service delivery and user satisfaction.

Table 4
Area of Concern

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 2, July 2023
https://doi.org/10.47709/cnahpc.v5i2.2524

Submitted : July 15, 2023
Accepted : July 16, 2023
Published : July 17, 2023

No	Area of Concern
1	Leaked user password data
2	Internet outage
3	Incorrect incident data input
4	File intrusion

In the identification of threat scenario step, scenarios that can affect the information assets for each identified asset container are created. This is done by identifying actors, means, motives, outcomes, and determining the probability of threat scenarios occurring.

The identification of threat scenarios is a critical aspect of the risk assessment process within the OCTAVE Allegro method. It involves creating scenarios that depict potential threats to the information assets within each asset container. These scenarios help in understanding the various actors or entities involved, the means they may employ, their motives or intentions, and the potential outcomes or impacts if the threat scenario unfolds.

By identifying and analyzing threat scenarios, organizations gain insights into the specific risks that their information assets may face. This allows them to better understand the potential vulnerabilities and plan appropriate mitigation strategies. The identification process also involves determining the probability of threat scenarios occurring, which helps prioritize risks and allocate resources effectively. Properties of threat, plays a crucial role in presenting a detailed overview of the identified threat scenarios. It outlines the specific properties or characteristics of each threat scenario, providing a comprehensive understanding of the nature of the threats. These properties may include information about the actors involved, the methods they might employ, the motives driving their actions, and the potential consequences or outcomes of the threat scenario. The information presented in table 5 assists organizations in developing a comprehensive understanding of the potential threats they may face. It allows for more accurate risk assessment, enabling organizations to implement targeted measures and controls to mitigate the identified threat scenarios. By addressing these threat scenarios proactively, organizations can enhance the security and resilience of their information assets within the SDP environment.

Table 5
Properties of Threat

No	Area of Concern	Threat of Properties	
1	Leaked user password data	Actor	Unknown
		Means	Login Attempts
		Motives	Unintentional
		Outcome	Modification
		Security requirements	Performing periodic clear history on user's PC
2	Internet outage	Actor	Unknown
		Means	Attempted internet access
		Motives	Unintentional
		Outcome	Interuption

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 2, July 2023
https://doi.org/10.47709/cnahpc.v5i2.2524

Submitted : July 15, 2023
Accepted : July 16, 2023
Published : July 17, 2023

		Security requirements	Backup service configuration
3	File intrusion	Actor	Unknown
		Means	Accidentally inputting file attachment
		Motives	Unintentional
		Outcome	Destruction
		Security requirements	Antivirus configuration

The identification of risks involves analyzing the potential consequences that may arise from the identified threat scenarios. In this context, the table 6 provides a comprehensive overview of the risks associated with specific threat scenarios.

The table highlights the interconnectedness between the identified threat scenarios and the potential consequences that may occur. Specifically, it emphasizes the risks that may arise if there is an internet outage, password leakage, or file intrusion. Each of these scenarios poses different risks to the security and integrity of the SDP system and its information assets.

By identifying and understanding these risks, organizations can effectively prioritize their mitigation efforts and implement appropriate controls to minimize the potential impact. This step allows for a proactive approach to risk management, ensuring that the necessary measures are in place to address and mitigate the identified risks.

The correlation between the threat scenarios and their associated consequences serves as a valuable reference for risk assessment and decision-making processes. It enables organizations to allocate resources and implement targeted risk mitigation strategies to safeguard the confidentiality, integrity, and availability of the SDP system and its information assets.

Table 6
Risk Identification

Threat Scenario	Consequence
Experiencing network damage, resulting in the unavailability of Service Desk Plus access.	Disruption of operational activities of ICT services, where any disruptions must be reported using the Service Desk Plus.
Experiencing leakage of user access passwords.	Disruption of incident reporting related to ICT services, resulting in unreliable or inaccurate reporting.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 2, July 2023
https://doi.org/10.47709/cnahpc.v5i2.2524

Submitted : July 15, 2023
Accepted : July 16, 2023
Published : July 17, 2023

Indication of file attachment intrusion with a virus.	Disruption of access to applications, leading to server downtime.

Risk analysis can identify risks and calculate risk outcomes by considering how to reduce the probability of failure and assessing the extent to which risk consequences affect the company. To obtain high, medium, and low impact values in the impact area, it is necessary to complete step 1 in activity 1, which includes the risk measurement criteria worksheet to determine the impact areas of risk. Additionally, in step 1 of activity 2, the prioritization of impact areas from high to low is determined.

Risk analysis is a crucial process in risk management that aims to identify and assess potential risks to an organization. It involves evaluating both the likelihood of failure and the potential impact of risks on the company. By conducting a thorough risk analysis, organizations can gain valuable insights into their risk landscape and make informed decisions to mitigate and manage risks effectively.

One important aspect of risk analysis is determining the impact areas, which refer to the different aspects or components of the organization that could be affected by risks. In this case, completing step 1 in activity 1 is crucial. This step involves using a risk measurement criteria worksheet to assess and determine the impact areas of the identified risks. The worksheet helps assign high, medium, or low impact values to each impact area based on the assessment criteria.

Furthermore, in step 1 of activity 2, the prioritization of impact areas is determined. This step involves assessing and ranking the impact areas based on their importance or significance to the organization. By prioritizing impact areas from high to low, organizations can focus their resources and efforts on addressing the most critical areas first, ensuring that risk mitigation measures are effectively implemented where they are most needed.

The combination of these steps and activities in risk analysis enables organizations to quantitatively and qualitatively assess risks, prioritize their actions, and allocate resources accordingly. This approach helps organizations make informed decisions in managing risks and minimizing their potential impact on the company's operations and objectives. Table 7 presents impact value based on the impact area.

Table 7
Impact Value

Impact Area	Impact Value
Anti-bribery management system	High
Organizational strategic goals	Medium
Human resources	Medium
Occupational health and safety	Low
Reputation	Low

Table 8 plays a significant role in the risk analysis process within the OCTAVE Allegro method. It presents the impact areas consistently identified from the initial steps, ensuring a comprehensive understanding of the areas affected by risks. These impact areas represent different aspects or components of the organization that could be impacted if risks materialize.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 2, July 2023
https://doi.org/10.47709/cnahpc.v5i2.2524

Submitted : July 15, 2023
Accepted : July 16, 2023
Published : July 17, 2023

The table also includes the prioritized ranking of impact areas. This ranking helps organizations determine the relative importance or significance of each impact area in relation to the others. By assigning a ranking to each impact area, organizations can prioritize their attention and allocate resources accordingly, focusing on the areas with the highest potential impact.

Table 8
Calculating Impact Area Score

Impact Area	Rank	Impact Value		
		Low (1)	Med (2)	High (3)
Anti-bribery management system	5	5	10	15
Organizational strategic goals	4	4	8	12
Human resources	3	3	6	9
Occupational health and safety	2	2	4	6
Reputation	1	1	2	3

To assess the risks associated with each impact area, the impact value is calculated. This value is derived by multiplying the prioritized ranking of the impact area with the predefined impact values, which are typically categorized as high, medium, or low. This calculation results in a numerical value that represents the level of impact associated with each area.

The impact values are then used for further risk analysis, mitigation planning, and control recommendations. Organizations can assess the risks by considering the impact values, alongside the probability of occurrence and other relevant factors. The analysis allows organizations to prioritize their mitigation efforts and implement appropriate control measures to address the identified risks effectively.

By utilizing the impact values and considering the recommended control measures, organizations can develop a comprehensive risk management strategy. This approach helps mitigate potential risks and ensure that appropriate measures are in place to minimize the impact on the organization's operations, assets, and objectives.

Once risks have been identified and their potential consequences understood, organizations need to determine the most effective strategies to mitigate these risks and minimize their impact. To prioritize risks for mitigation, organizations consider a variety of factors. These factors may include the severity of potential consequences, the likelihood of risks occurring, the value of the assets or systems at risk, and the overall risk tolerance of the organization. By establishing a prioritization framework, organizations can determine which risks require immediate attention and allocate resources accordingly. This enables them to focus their mitigation efforts on the most critical and impactful risks. Developing a mitigation strategy involves formulating specific actions and control measures to reduce the likelihood and impact of identified risks. This strategy takes into account the value of assets and the containers associated with those assets. Containers refer to the places where assets are stored, transported, or processed, and may include physical locations, databases, or networks. Table 9, which provides the Pool for categorizing risks, serves as a reference for organizing and classifying risks based on their risk scores. The risk scores help determine the severity and priority of each risk, allowing organizations to allocate resources and implement appropriate mitigation measures. By following a systematic approach to risk mitigation and using the Pool to categorize risks, organizations can effectively manage and reduce their exposure to potential threats. This helps protect their assets, ensure business continuity, and enhance overall information security.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 2, July 2023
https://doi.org/10.47709/cnahpc.v5i2.2524

Submitted : July 15, 2023
Accepted : July 16, 2023
Published : July 17, 2023

Table 9
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

Each identified risk will be provided with control recommendations based on the control annex of ISO 27001:2013, which serves as a reference for establishing and implementing risk handling measures for the containers and solutions involved. Table 10 presents the mitigation approach for the user data container in SDP (Service Desk Plus) that specifically addresses the risk of user password leakage. The table includes control recommendations from the ISO 27001:2013 annex and the corresponding solutions.

Table 10
Risk Mitigation

Risk Mitigation I		**Risk Mitigation II**	
Area of Concern	User password leakage	Area of Concern	Internet outage
Probability	Medium	Probability	Medium
Action	Mitigate	Action	Mitigate
Controls	**A.9.26** Removal or adjustment of access rights	Controls	**A.13.1.2** Security of network Services
	Conduct regular reviews and audits for all active and inactive users in the employee database		Redirect internet traffic from inactive sources to active sources on the router side
Risk Mitigation III		**Risk Mitigation IV**	
Area of Concern	File Intrusion	Area of Concern	Data Input Error
Probability	Medium	Probability	Low
Action	Mitigate	Action	Accept
Controls	**A.12.2.1** Controls against malware	Controls	**A.12.1.1** Documented operating procedures
	1. Perform regular antivirus updates on each user's PC. 2. Block all files containing viruses, both from the internet and the use of removable media.		1. Perform regular antivirus updates on each user's PC. 2. Block all files containing viruses, both from the internet and the use of removable media.

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 5, Number 2, July 2023
https://doi.org/10.47709/cnahpc.v5i2.2524

Submitted : July 15, 2023
Accepted : July 16, 2023
Published : July 17, 2023

The risk mitigation process yielded positive results by effectively reducing the identified risks and enhancing the overall security posture of the organization. Through the implementation of recommended control measures and the application of relevant solutions, the organization successfully mitigated potential vulnerabilities and threats. Regular updates of antivirus software on user PCs were carried out to minimize the risk of malware infections. Additionally, blocking files containing viruses from both internet sources and removable media contributed to preventing malicious content from infiltrating the organization's systems. These risk mitigation efforts have significantly improved the organization's ability to safeguard sensitive data, maintain operational continuity, and mitigate the potential impact of security incidents.

5. CONCLUSION

In conclusion, the research findings highlight the importance of risk assessment and mitigation in ensuring the security of SDP (Service Desk Plus) at Sultan Aji Muhammad Sulaiman Sepinggan International Airport. The analysis identified critical areas of impact and assets, enabling the implementation of targeted risk mitigation strategies. By addressing user data password errors, internet outages, and file infiltration risks, the organization has significantly reduced the potential for security incidents. Furthermore, the adoption of appropriate controls and measures, such as password policies, redundancy plans, and antivirus systems, has strengthened the overall security posture of SDP. These efforts contribute to the protection of sensitive information, the reliability of ICT services, and the establishment of trust among users and stakeholders. In light of these findings, it is recommended that the organization continue to prioritize information security and regularly review and update its risk mitigation strategies. This can involve conducting periodic risk assessments to identify emerging threats and vulnerabilities, implementing ongoing training programs to enhance user awareness and best practices, and staying up to date with industry standards and regulations. Additionally, fostering a culture of security and promoting proactive incident reporting can further enhance the organization's ability to detect and respond to potential risks promptly. By continuously improving its risk management practices, the organization can maintain a robust and resilient information security framework for SDP.

6. REFERENCES

Abdullah, K., Isnainiyah, I. N., & Faried, M. I. (2020). Risk Management Analysis on Organizational Website Using Octave Allegro Method. Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020, 201–206.

Andersson, A., Hedström, K., & Karlsson, F. (2022). "Standardizing information security – a structurational analysis." Information and Management, 59(3).

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.

Deva, B. S., & Jayadi, R. (2022). Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro. Jurnal Teknologi Dan Informasi (JATI), 12(27), 12.

Herdianto, R. A., Ramli, K., & Suryanto, Y. (2022). Risk Assessment of Electronic Archive Services using Octave Allegro Method (Case Study: SIKN JIKN). IOP Conference Series: Materials Science and Engineering, 1232(1), 012007.

International Standard. (2013). Information technology-Security techniques-Information securitymanagement systems-Requirements.

Legowo*, N., & Saputra, K. A. (2019). Risk Management of Credit Card Payment Gateway using Octave Allegro Methodology At Electronic Payment Provider Institution. International Journal of Recent Technology and Engineering (IJRTE), 8(4), 11831–11838.

Nastiti, F. E., & Haryani, P. (2022). Analisis Risiko Keamanan Informasi E- gov Siskeudes menggunakan metode OCTAVE Allegro.

O'brien, M. (2005). Introduction to Information System.

Oluwatosin, H. S. (2014). Client-Server Model. IOSR Journal of Computer Engineering, 16(1), 57–71.

Ramadhintia, R., & Bisma2, R. (2021). Perencanaan Mitigasi Risiko Menggunakan Metode OCTAVE Allegro pada SMA Semen Gresik. JEISBI, 02.

Whitman, M. E. (2011). Principles of Information Security Fourth Edition.

* Corresponding author