JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9335
Hal 846-854
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Information Security Risk Analysis and Identification in the Tulang Bawang Data Portal Application Using the OCTAVE Allegro Method

Wahyu Aji Pulungan, Allwine*

Fakultas Matematika dan Ilmu Pengetahuan Alam, Program Studi Ilmu Komputer, Universitas Lampung, Bandar Lampung, Indonesia
Email: [1]wahyuaji@fmipa.unila.ac.id, [2*]allwine@fmipa.unila.ac.id
Email Penulis Korespondensi: allwine@fmipa.unila.ac.id
Submitted **12-11-2025;** Accepted **06-05-2026;** Published **30-06-2026**

Abstract

Information technology has become an essential component in supporting organizational and governmental operations. In line with the implementation of E-Government and the Satu Data Indonesia initiative, the Tulang Bawang Regency Government, through its Communications and Information Office (Diskominfo), developed the Tulang Bawang Data Portal to facilitate centralized data management. Despite its strategic role, the system is exposed to various information security risks that may threaten the confidentiality, integrity, and availability of data if not properly addressed. This study aims to systematically identify, assess, and prioritize information security risks within the Tulang Bawang Data Portal using the OCTAVE Allegro method. A qualitative risk assessment approach was employed, incorporating asset identification, threat analysis, impact evaluation, and risk prioritization based on defined risk measurement criteria. The findings indicate the presence of four significant risks, with Risk Relative Scores (RRS) ranging from 14 to 23. Notably, 75% of the identified risks are classified as high priority. The most critical risk is associated with database misuse, which poses a substantial threat to sensitive government data. To address these risks, several mitigation strategies are recommended, including the enhancement of access control mechanisms, periodic security audits, user awareness programs, and the establishment of comprehensive data governance policies. This study contributes to the field by providing a structured and practical risk assessment framework tailored to government-based data portal systems, thereby supporting more effective and informed decision-making in information security management.

Keywords: Data; Portal Data; Risk; Octave; Allegro

1. INTRODUCTION

Information technology has become a fundamental necessity and plays a crucial role in supporting the activities of organizations and institutions. To achieve their business objectives, organizations increasingly rely on information technology to enhance productivity, transform working methods, stimulate economic growth, and facilitate global knowledge sharing. Furthermore, the adoption of information and communication technology enables the automation of business processes and improves organizational communication efficiency. Information Technology Governance (ITG) in Indonesia is regulated under the Sistem Pemerintahan Berbasis Elektronik (SPBE) or Electronic-Based Government System (E-Government). E-Government refers to the implementation of government services utilizing information and communication technology to deliver services to users [1]. This initiative aligns with public governance reform efforts outlined in the Grand Design of Bureaucratic Reform 2010–2025, as stipulated in Presidential Regulation Number 81 of 2010 [2].The Department of Communication and Informatics (Diskominfo) functions as a Regional Apparatus Organization (Organisasi Perangkat Daerah/OPD) responsible for overseeing the implementation of information technology at both regional and central government levels [3]. According to [4], Diskominfo serves as the executing body for governmental affairs in communication and informatics, cryptography, and statistics, led by a Head of Department accountable to the Regent through the Regional Secretary.

In line with advancements in information technology within the governmental sector, the Tulang Bawang Regency Government has implemented the Portal Data Tulang Bawang to support SPBE and the Satu Data Indonesia program [5][6]. The Satu Data Indonesia policy, regulated under Presidential Regulation No. 39 of 2019 [7], aims to establish high-quality, integrated, and accessible data governance across government institutions. The Portal Data Tulang Bawang is designed to centralize sectoral data, enabling data sharing among Regional Apparatus Organizations and facilitating public access to government data [8]. This openness is essential, as data serves as a fundamental resource for identifying and addressing public issues [9]. The Portal Data system is a web-based application hosted on Diskominfo servers, enabling flexible access regardless of time and location. It allows OPDs to store, manage, and process sectoral data digitally, replacing previously fragmented and manual processes. The platform is managed collaboratively by the Regional Development Planning Agency (BAPPEDA), Diskominfo, and the Central Statistics Agency (BPS). All data published in the portal is categorized as public information, in compliance with Law Number 14 of 2008 on Public Information Disclosure [10]. Despite its advantages, the increasing reliance on digital systems introduces various information security risks. Information is a critical organizational asset, and its protection is essential to ensure business continuity. Information security risks arise from the interaction between assets, vulnerabilities, and threats [11]. As organizations transition toward digital environments, they face increasing exposure to cyber threats such as data breaches and unauthorized access, which may lead to misuse of sensitive information and institutional data [12].

In practice, information systems may not always function as intended, making risk identification a critical process in ensuring system reliability and security. Information security is defined by the protection of confidentiality, integrity,

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9335
Hal 846-854
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

and availability (CIA) of information [13]. Risk refers to the possibility of an undesirable event that may negatively impact organizational objectives, although it may also present opportunities under certain conditions [14].

Several previous studies have applied risk assessment frameworks such as OCTAVE, ISO 27005, and NIST to evaluate information security risks in organizational systems. These studies generally provide structured approaches for identifying and managing risks; however, many of them are not specifically tailored to government-based open data portals, which have unique characteristics such as high data accessibility, multi-stakeholder involvement, and regulatory compliance requirements. In particular, there is still limited research focusing on risk identification in regional government data portals within the context of SPBE implementation. Based on this gap, this study aims to identify and analyze information security risks in the Portal Data Tulang Bawang using the OCTAVE Allegro method. This method is selected due to its asset-focused approach and its suitability for evaluating information security risks in organizational contexts. The contribution of this research lies in providing a structured and context-specific risk assessment framework for government data portals, which can support decision-making processes and enhance information security management in the public sector.

2. RESEARCH METHODOLOGY

2.1 Research Framework

The research framework in this study is structured based on the eight steps of the OCTAVE Allegro method, which are grouped into four main phases. These steps are applied systematically to assess information security risks in the Tulang Bawang Data Portal. Figure 1 illustrates the research framework used in the study.

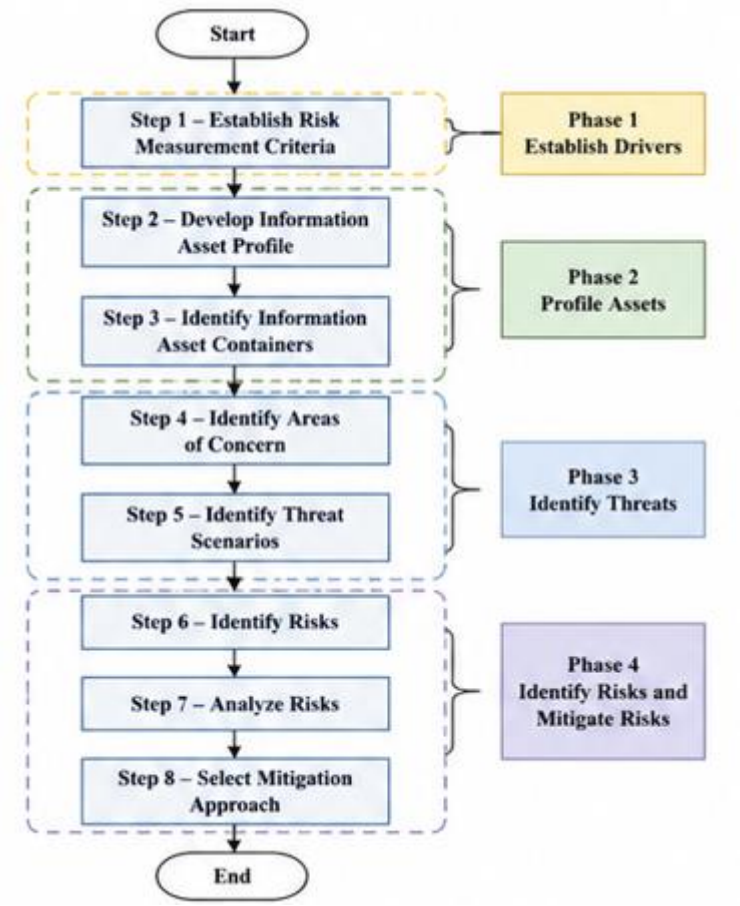

Figure 1. Research Framework based on the OCTAVE Allegro method

2.2 Research Design

This study employs a qualitative risk assessment approach using the OCTAVE Allegro method to identify, analyze, and mitigate information security risks. The method is selected due to its asset-focused perspective and its suitability for organizations with limited resources [18]–[20].

2.3 Research Object

The object of this research is the Tulang Bawang Data Portal, a web-based application developed by Diskominfo to centralize sectoral data from Regional Apparatus Organizations (OPDs) in support of SPBE and Satu Data Indonesia.

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9335
Hal 846-854
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

2.4 Data Collection Methods

Data were collected through:
1. Observation of system operations and infrastructure
2. Interviews with administrators and stakeholders (Diskominfo)
3. Documentation review of policies, system design, and regulations

2.5 OCTAVE Allegro Implementation

The OCTAVE Allegro method consists of eight steps grouped into four phases. Table 1 summarizes the steps and their application in this study.

Table 1. Application Of Octave Allegro In This Study

Phase	Step	Activity	Application in This Study
Phase 1 Establish Drivers	1	Establish risk measurement criteria	Define risk evaluation criteria based on organizational objectives and CIA (Confidentiality, Integrity, Availability).
Phase 2 Profile Assets	2	Develop information asset profile	Identify critical assets such as sectoral data, user data, applications, and infrastructure.
Phase 2 Profile Assets	3	Identify information asset containers	Identify where assets are stored, processed, and transmitted (databases, servers, networks, devices).
Phase 3 Identify Threats	4	Identify areas of concern	Identify security concerns and vulnerabilities in the system.
Phase 3 Identify Threats	5	Identify threat scenarios	Develop threat scenarios such as unauthorized access, data leakage, malware attack, and system disruption.
Phase 4 Identify Risks and Mitigate Risks	6	Identify risks	Formulate risks by combining assets, threats, and vulnerabilities.
Phase 4 Identify Risks and Mitigate Risks	7	Analyze risks	Evaluate and prioritize risks using the Risk Relative Score (RRS).
Phase 4 Identify Risks and Mitigate Risks	8	Select mitigation approach	Determine appropriate mitigation strategies for high-priority risks.

2.6 Risk Analysis Method

Risk analysis is performed using the Risk Relative Score (RRS) approach. Each identified risk is evaluated based on its potential impact on the organization's information security criteria. The RRS is calculated as follows:

$$RRS = \sum_{\{i=1\}}^{\{n\}} (W_i \times S_i) \quad (1)$$

Where:
Wi = Weight of impact criterion i
Si = Score of impact level for criterion i
n = Number of impact criteria

The following table 2 presents risk assessment criteria based on the aspects of Confidentiality, Integrity, and Availability, along with their respective weights to measure the level of impact on information security.

Table 2. Risk Impact Criteria And Weight

No.	Criterion	Description	Weight (Wi)
1	Confidentiality	Impact on unauthorized disclosure of information	0.4
2	Integrity	Impact on unauthorized modification or corruption of information	0.3
3	Availability	Impact on system/service unavailability	0.3

Table 3 presents the impact level scoring scale, which categorizes the severity of potential risks into Low, Medium, and High levels, along with their corresponding scores and descriptions to assess their effects on operational activities.

Table 3. Impact Level Scoring Scale

Score (Si)	Impact Level	Description
1	Low	Minimal impact; limited effect on operations
2	Medium	Moderate impact; noticeable effect on operations
3	High	Significant impact; critical effect on operations

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9335
Hal 846-854
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Table 4 presents the risk priority levels based on the Risk Rating Score (RRS), categorizing risks into Low, Medium, and High levels with corresponding priorities and recommended actions for mitigation.

Table 4. Risk Priority Level Based On RRS

RRS Range	Risk Level	Priority	Action
1–10	Low	3	Acceptable; monitor regularly
11–20	Medium	2	Planned mitigation required
21–30	High	1	Immediate mitigation required

2.7 Validity and Reliability

To ensure the validity of the findings, data triangulation is conducted by comparing results from observations, interviews, and documentation. The risk assessment process is reviewed by experts in information security from Diskominfo to ensure reliability and accuracy of the analysis.

3. RESULT AND DISCUSSION

This section presents the results of the OCTAVE Allegro implementation on the Portal Data Tulang Bawang system, followed by a comprehensive discussion that connects the findings with the research objectives and prior studies related to information security risk assessment in e-government systems.

3.1 Establish Risk Measurement Criteria

This section elaborates on the establishment of risk measurement criteria, which is crucial as it forms the foundational basis for consistently evaluating and prioritizing risks. It will detail how these criteria are defined, encompassing the parameters utilized to assess both the impact and likelihood of incidents, thereby providing a clear framework for subsequent risk analysis. Table 5 describes the impact on reputation and customer confidence.

Table 5. Reputation and Customer Confidence

Impact Area	Low	Medium	High
Reputation	OPD trust in Portal Data Application is little or not affected	OPD trust in Portal Data Application is affected	OPD trust in Portal Data Application is highly affected
User Loss	Use of Portal Data Application is optimal	Use of Portal Data Application is less then optimal	Use of Portal Data Application is not optimal

Table 6 explains productivity impact,

Table 6. Productivity

Impact Area	Low	Medium	High
Data Collective	Data input is done inconsistently	Data input is done consistently	Data input is done very consistently

Table 7 presents the priority ranking of impact areas. These criteria ensure a structured and consistent risk evaluation process.

Table 7. Impact Area Priority

Impact Area	Priority
Security	1
Productivity	2

3.2 Develop Information Asset Profile

This section presents the results of the information asset profiling stage. This process involved the identification and categorization of critical information assets related to the Portal Data Application. Each asset will be described in detail, including its strategic value to the organization, thereby providing a comprehensive understanding of what needs to be protected and why each asset is considered crucial.

Table 8 presents the OPD data asset profile

Table 8. OPD Data Asset Profile

Allegro Wordsheet 7	Critical Asset Profile
Critical Asset	OPD Data
Description	This asset contains OPD information such as name, username, password
Owner	Related OPD

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9335
Hal 846-854
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Security Requirements	Confidentiality	Only related OPDs and Portal Data Operators can change data
	Integrity	Data changes are made by related OPDs through IT operators
	Availability	These assets must be available for each OPD
Most Important Security Requirement		Integrity. The data must match, because if not the user cannot log into the application.

Table 9 shows the sectoral data asset profile. The findings indicate that OPD data and sectoral data are the most critical assets, where integrity and availability are the main security priorities.

Table 9. Sectoral Data Asset Profile

Allegro Wordsheet 7		Critical Asset Profile
Critical Asset		Sectoral Data
Description		This asset contains sectoral data belonging to each OPD
Owner		OPD Terkait
Security Requirements	Confidentiality	Only related OPDs and Portal Data Operators can change data
	Integrity	Data changes are made by related OPDs through IT operators
	Availability	These assets must be available for each OPD
Most Important Security Requirement		Availability. Data must be available because OPD must fill in the data

3.3 Identify Information Asset Containers

Containers refer to the physical or logical locations where information assets are stored, processed, or transmitted. The discussion will include details regarding the infrastructure, systems, or software that serve as receptacles for these information assets, as well as the potential vulnerabilities inherent in each container.

Table 10 illustrates the information asset risk environment map. The results show that assets are distributed across internal (servers, databases, devices) and external containers (internet), increasing exposure to vulnerabilities.

Table 10. Information Asset Risk Environment Map

Internal	
Container Description	**Owner**
Server	Diskominfo
Devices for Access	Each OPD
Database	Diskominfo
External	
Container Description	**Owner**
Internet Network	QNN

3.4 Identify Areas of Concern

Areas of concern are aspects within the Portal Data Application environment that require specific attention due to their potential for significant risk. This identification is based on concerns arising from the analysis of assets and containers, as well as discussions with relevant stakeholders. Table 11 presents the areas of concern. The results highlight data input errors, power outages, and database abuse as primary concerns.

Table 11. Areas of Concern

No.	Areas of Concern	Related Assets
1.	Data input error	Application
2.	Power Outage	Applicatioin, Server, Internet
3.	Database Abuse	Application, Server

3.5 Identify Threat Scenarios

A threat scenario is a narrative description detailing how a threat can exploit vulnerabilities and cause negative impacts on information assets. The discussion will encompass various identified scenarios, providing a clear overview of potential attacks or incidents that might occur within the Portal Data Application.

Table 8 presents Threat Scenario 1 using the OCTAVE Allegro Worksheet 9, which describes a risk to the Portal Data Application caused by data input errors by IT operators. This scenario highlights human error as the primary motive, with a medium probability due to its frequent occurrence, potentially resulting in incorrect or invalid data being stored and affecting data integrity.

Table 12. Threat Scenario 1

Allegro Worksheet 9	Information Asset Risk Worksheet

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9335
Hal 846-854
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Information Asset	Portal Data Application
Areas of Concern	Data input error
Actor	IT Operators of each OPD
Means	Errors in data input so that the data is invalid (wrong) or doesn't match the format
Motive	Human Error
Outcome	Incorrect data or error when saved
Security Requirements	OPD operator can manage data entry
Probability	Medium. Because human error often occurs

Table 13 presents Threat Scenario 2 using the OCTAVE Allegro Worksheet 9, which describes a risk to the application, server, and internet caused by power outages. This scenario identifies external factors related to the electricity provider as the main motive, with a low probability due to its rare occurrence, potentially resulting in temporary service disruption and inability to perform data input.

Table 13. Threat Scenario 2

Allegro Worksheet 9	Information Asset Risk Worksheet
Information Asset	Application, Server, Internet
Areas of Concern	Power Outage
Actor	Network Engineer and Administrator
Means	There is a power outage so that the server is down and the application cannot be accessed. Data input cannot be done
Motive	The electricity provider is carrying out routine or emergency power outages
Outcome	Cannot input data temporarily
Security Requirements	Provide UPS or Generator Set
Probability	Low. Rarely occurs

Table 14 presents Threat Scenario 3 using the OCTAVE Allegro Worksheet 9, which describes a risk to the application and server caused by database abuse or theft. This scenario involves both internal and external actors with malicious intent, driven by motives such as personal dissatisfaction or intent to harm the agency. With a high probability due to its vulnerability, this threat can lead to loss of trust and requires strong security measures, including system protection, continuous monitoring, and strict database control.

Table 14. Threat Scenario 3

Allegro Worksheet 9	Information Asset Risk Worksheet
Information Asset	Application, Server
Areas of Concern	Database abuse
Actor	Network Administrator, Perpetrator
Means	Database is misused or stolen
Motive	Dislike or want to bring down the agency
Outcome	Distrust
Security Requirements	Provide Security System Services and routine monitoring and control of database and applications
Probability	High. Vulnerable to occur

Table 15 presents Threat Scenario 4 using the OCTAVE Allegro Worksheet 9, which describes a risk to the Portal Data Application caused by the reluctance of OPD to use the system. This scenario highlights lack of awareness or concern as the main motive, with a high probability due to its susceptibility, potentially resulting in incomplete data entry. To address this, clear regulations, SOPs, and responsible operators are required to ensure proper system usage.

Table 15. Threat Scenario 4

Allegro Worksheet 9	Information Asset Risk Worksheet
Information Asset	Portal Data Application
Areas of Concern	OPD doesn't want to use the application
Actor	Related OPD
Means	There is lack of trust or indifference towards the use of the Portal Data Application by the related OPD
Motive	Not knowing or not caring
Outcome	OPD data is not filled in

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9335
Hal 846-854
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

Security Requirements	Related OPD operators who independently manage data filling. Rules such as SK and SOP for filing need to be provided
Probability	High. Because it is very susceptible to occur

3.6 Identify Risks

This section presents the specific results of risk identification. Based on the previously defined risk measurement criteria, asset profiles, containers, areas of concern, and threat scenarios, each risk will be clearly formulated. Every identified risk will be individually described, including the affected assets and their potential consequences.
Table 16 summarizes the identified threat scenarios and their corresponding consequences, providing a clear overview of potential impacts on system operations, data reliability, service availability, and organizational trust.

Table 16. Threat Scenarios and Consequences

No.	Threat Scenarios	Consequences
1.	Data input error	Re-input
2.	Power outage	All related assets cannot be used
3.	Database abuse	Can affect reputation and trust because it is not secure
4.	OPD doesn't want to use the application	Application is not used and data is not filled

Table 17 shows impact scoring. Database abuse and lack of system usage are identified as critical risks.

Table 137 Impact Area and Score

Impact Area	**Priority**	**Impact Score**		
		Low	**Medium**	**High**
Security	1	5	10	15
Productivity	2	4	8	12

3.7 Analyze Risks

This analysis involves evaluating the severity of each identified risk by considering its likelihood of occurrence and its potential impact. The discussion will cover how risk scores are calculated and how risk priorities are determined, offering both a quantitative and qualitative perspective on each threat.

Table 18 presents the risk analysis results by evaluating each area of concern based on its impact on security and productivity, along with the calculated Relative Risk Score (RRS) to determine the overall risk level and support appropriate mitigation decisions.

Table 18. Risk Analyzing

No.	**Areas of Concern**	**Risk**			
1.	Data Input Error	**Consequences**	OPD operators can manage data entry independently, so it must be done carefully.		
		Severity	**Impact Area**	**Impact Score**	**Score**
			Security	Medium	10
			Productivity	Low	4
		Relative Risk Score			14
2.	Power Outage	**Consequences**	Provide UPS or Generator Set.		
		Severity	**Impact Area**	**Impact Score**	**Score**
			Security	Medium	10
			Productivity	High	12
		Relative Risk Score			22
3.	Database Abuse	**Consequences**	Providing Security System Services and routine monitoring and control of databases and applications.		
		Severity	**Impact Area**	**Impact Score**	**Score**
			Security	High	15
			Productivity	Medium	8
		Relative Risk Score			23
4.	OPD doesn't want to use the application	**Consequences**	Related OPD operators who independently manage data filling. Rules such as SK and SOP for filing need to be provided.		
		Severity	**Impact Area**	**Impact Score**	**Score**
			Security	Low	5

JURIKOM (Jurnal Riset Komputer), Vol. 13 No. 3, Juni 2026
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v13i3.9335
Hal 846-854
https://ejurnal.stmik-budidarma.ac.id/index.php/jurikom

	Productivity	High	12
	Relative Risk Score		17

3.8 Select Mitigation Approach

Based on the results of the risk analysis, various proposed mitigation strategies for reducing or managing the identified risks will be presented. The discussion will include the justification for each chosen approach, whether it involves risk avoidance, transfer, mitigation, or acceptance, while considering its effectiveness and implementation feasibility.

Table 19 presents the risk reduction approach based on the Relative Risk Score (RRS), outlining appropriate treatment strategies such as mitigation, mitigation or suspension, and risk acceptance according to the severity of each identified risk.

Table 19. Risk Reduction Approach

Pool	Area of Concern	Mitigation Approach
30 - 45	-	Mitigation
16 - 29	1. Power Outage	Mitigation or suspension
	2. Database Abuse	
	3. OPD doesn't want to use the application	
0 - 15	Data Input Error	Accepted

3.9 Discussion

The results indicate that database abuse and power outages represent the highest risks to the Portal Data system. This aligns with previous studies mentioned in the Introduction filecite turn1file0, where information security risks in government systems are commonly associated with data breaches, unauthorized access, and system availability issues. However, this study identifies an additional critical risk, namely the reluctance of OPD users to utilize the system. This differs from many prior studies using OCTAVE, ISO 27005, or NIST frameworks, which tend to focus primarily on technical vulnerabilities rather than human and organizational factors. In terms of similarity, this study confirms that the core principles of information security—confidentiality, integrity, and availability (CIA)—remain central in risk assessment, as highlighted in previous research. Database abuse directly threatens confidentiality and integrity, while power outages affect system availability. In contrast, the inclusion of user adoption issues highlights the importance of socio-technical aspects in e-government systems, particularly in SPBE-based environments where multiple stakeholders are involved. These findings support the research objective of identifying and analyzing information security risks in the Portal Data Tulang Bawang system. The results demonstrate that effective risk management requires both technical solutions (such as security monitoring and backup infrastructure) and organizational strategies (such as SOP enforcement and user training).

4. CONCLUSION

The findings of this study demonstrate that the implementation of the application has achieved its primary objective of supporting more efficient and centralized data management across Regional Apparatus Organizations (OPDs). A strong relationship between application security and user productivity was identified, where higher levels of security contribute to increased user trust, comfort, and overall performance. The study also highlights several critical risk areas with varying levels of urgency based on their Relative Risk Score (RRS). Database misuse represents the highest risk (RRS 23), indicating the need for strict cybersecurity controls such as access management, encryption, and regular system audits to maintain data integrity and public trust. Power outages (RRS 22) pose a significant operational threat that can disrupt system availability and potentially lead to data loss, emphasizing the importance of reliable backup and recovery mechanisms. Meanwhile, resistance from OPDs in adopting the application (RRS 17) reflects a non-technical challenge that requires effective change management strategies, including training and user engagement, to ensure full participation. Although data input errors have a lower risk level (RRS 14), they remain important due to their potential to affect data accuracy and decision-making, thus necessitating proper validation systems and standardized procedures. Overall, the study identifies a high-risk level environment with multiple priority concerns and provides several key recommendations focused on strengthening security, improving system reliability, and enhancing user adoption to ensure sustainable and optimal use of the application.

REFERENCES

[1] Pemerintah Republik Indonesia, Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE), 2018.
[2] Pemerintah Republik Indonesia, Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia, 2019.
[3] Pemerintah Republik Indonesia, Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2023 tentang Interoperabilitas Data dalam SPBE dan Satu Data Indonesia, 2023.
[4] Pemerintah Republik Indonesia, Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, 2008.

[5] M. J. Islami, "Implementasi Satu Data Indonesia: Tantangan dan Critical Success Factors (CSFs)," Jurnal Komunika, vol. 10, no. 1, pp. 13–23, 2021.
[6] R. Maulidya and M. Rozikin, "Analisis Retrospektif Kebijakan Satu Data Indonesia," Dinamika: Jurnal Ilmiah Ilmu Administrasi Negara, vol. 9, no. 2, pp. 273–282, 2022.
[7] W. Sardjono and M. I. Cholik, "Information Systems Risk Analysis Using OCTAVE Allegro Method at Banking Sector," in Proc. 2018 Int. Conf. Information Management and Technology (ICIMTech), 2018, pp. 38–42.
[8] J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with OCTAVE Allegro at Educational Institution," Procedia Computer Science, vol. 135, pp. 202–213, 2018.
[9] G. Sitorus, R. Fauzi, and R. A. Nugraha, "Analisis Risiko Keamanan Informasi Menggunakan Metode OCTAVE Allegro pada Instansi Pemerintah," eProceedings of Engineering, vol. 7, no. 2, pp. 7003–7008, 2020.
[10] S. A. Grishaeva and V. I. Borzov, "Information Security Risk Management," in Proc. 2020 IEEE Int. Conf. Quality Management, Transport and Information Security, 2020, pp. 96–98.
[11] A. Setiawan, D. Prabowo, and R. Nugroho, "Information Security Risk Assessment Using OCTAVE Allegro in E-Government Systems," International Journal of Advanced Computer Science and Applications, vol. 12, no. 6, pp. 450–457, 2021.
[12] M. H. Kurniawan and T. D. Susanto, "Risk Analysis of E-Government Services Using OCTAVE Allegro Method," in Proc. 2021 Int. Conf. Informatics, Multimedia, Cyber and Information System (ICIMCIS), 2021, pp. 120–125.
[13] N. A. Rahman, F. H. Ahmad, and Z. M. Yusof, "Information Security Risk Assessment in Public Sector Using OCTAVE Allegro," Journal of Information Security and Applications, vol. 58, 2021.
[14] B. H. Prasetyo and A. N. Hidayanto, "Evaluation of Information Security Risk Management in Government Institutions," Procedia Computer Science, vol. 161, pp. 123–130, 2019.
[15] R. Khan, S. U. Khan, and M. Ilyas, "Systematic Review of Information Security Risk Assessment Methods," IEEE Access, vol. 7, pp. 107–124, 2019.
[16] ISO/IEC, ISO/IEC 27005:2018 Information Security Risk Management, 2018.
[17] A. Alshamrani, K. Alsubhi, and M. Alghamdi, "Cybersecurity Risk Assessment in Smart Government Systems," IEEE Access, vol. 9, pp. 123456–123470, 2021.
[18] D. Fitriansyah, E. Utami, and A. Nugroho, "Analisis Risiko Sistem Informasi Pemerintah Menggunakan Metode OCTAVE Allegro," Jurnal RESTI, vol. 5, no. 3, pp. 450–458, 2021.
[19] L. S. Devi and Y. Priyadi, "Information Security Risk Analysis on Public Service Applications," International Journal of Computer Applications, vol. 183, no. 20, pp. 15–22, 2022.
[20] F. A. Saputra and I. M. Sukarsa, "Risk Management Implementation in Government Information Systems: A Case Study," Telkomnika, vol. 21, no. 2, pp. 345–353, 2023.