

Preparation of Information Security Risk Management Based on Iso / IEC 27001: 2022 at Diskominfo West Java Province

Ginanjar Nugraha^{*1}, Ina Siti Nurhasanah²,
Idi Sumardi³, Yuda Prasetya Nugraha⁴

^{1,2,3} Universitas Al Ghifari

Corresponding Author: ^{*1}ginz@stmikjabar.ac.id,
²inast.nurhasanah@gmail.com.

Article Information:

Received: January 14, 2025, Accepted: January 20, 2025, Published: January 22, 2025

Abstract

Information security and awareness of the dangers of information leakage are the most important things in information technology, especially information that is classified and has strategic value. Information security risk management is an approach organizations use to identify, distribute, measure, and manage risks related to information security, which, if left unchecked, can paralyze existing business process activities in the organization. In carrying out its business processes, the West Java Province Diskominfo still has risk problems, namely that information security incidents often disrupt institutional business processes, where some incidents can be handled directly (reactively) in the field. However, several other incidents require planning and time. There are quite a few solutions, and there is no proper supervision and planning in managing data and information security, so Information Security Risk Management based on ISO/IEC 27001:2022 is needed. The results of this research show that there are forty-one information security risks in the West Java Province Diskominfo, and recommendations have been given for each risk in accordance with the ISO/IEC 27001:2022 standard.

Keywords— Information Security, Information Security Risk Management, ISO 27001:2022

1. Introduction

Technological advances are positively utilized in the process of governance. The utilization of technological advances is to improve the efficiency, effectiveness, transparency and accountability of public services through electronic-based government services in accordance with Presidential Regulation No. 95/2018 on Electronic-Based Government Systems (Budiarto, 2017).

Through the application of technology in the governance process, the government can optimize the development of advances in information technology in the bureaucratic process by forming a network of integrated management systems and work processes (Mahardika, 2017). This causes government agencies to work in an integrated manner, making it easier and simpler to access government information and public services so that the public and other stakeholders can optimally utilize government information and public services through various websites and public service applications to attract investment, provide information and improve public

services. The negative impact caused by the large number of public service applications creates vulnerabilities in information and communication system transactions (Matondang et al., 2018).

Information security and vigilance against the danger of information leakage are the most important things in the use of information technology, especially classified and strategic information (Wijaya et al., 2024). Any information must be guaranteed security and confidentiality from all threats such as access, use, disclosure, interference, modification or destruction from unauthorized parties. So whatever form of information is used, whether stored or disseminated, it must always be protected.

In line with the increasing amount of information presented by the government as part of the service, the greater the challenge to information security (Wijaya & Senen, 2024) (Indonesia, 2023). Information security concerns confidentiality, integrity, and availability. All parties, especially policy-making officials, must understand the importance of information security and realize all potential vulnerabilities in information and communication system transactions, one of which can identify existing risks. risks can occur by managing staff who have insufficient competence, can also occur for losses that are closely related to single events that are not expected but have the potential to have a serious impact if the risk actually occurs, for example internal and external fraud, system failure, and natural disasters. From these risks, it is necessary to manage good information security risk management.

Information security risk management itself is an approach used by organizations to identify, evaluate, measure, and manage risks related to information security which if left unchecked can paralyze business process activities in the organization (Syahindra et al., 2022). In the International Standard Organization (ISO) 27001 document which is an international standard for information security management, it is used by many organizations as requirements and best practices that organizations must comply with to ensure that their information security management system (ISMS) is effective in protecting sensitive and important data and information. ISO 27001 is designed to help organizations identify, evaluate, manage and mitigate information security risks (Fajri & Harwahu, 2024). ISO 27001 promotes a risk-based approach to information security management. Organizations should identify information security risks, evaluate their impact and probability, and take appropriate action to mitigate them. The advantage of ISO 27001 is that it promotes a risk-based approach in information security management that helps organizations better identify and manage risks, which in turn can reduce potential losses and impacts (Fajri & Harwahu, 2024).

The West Java Provincial Government, in this case the Communication and Informatics Office of West Java Province, is a government agency that has the main task in accordance with West Java Governor Regulation Number 60 of 2017 concerning Tasks, Functions, Details of Unit Tasks and Work Procedures of the Communication and Informatics Office of the Regional Government of West Java Province, namely carrying out regional government affairs in the field of communication and informatics, including E-Government, Informatics Applications, Public Information and communication, coding and information security and statistics, which are the authority of the Provincial Region, carrying out deconcentration tasks and carrying out assistance tasks in accordance with their fields of duty, based on statutory provisions. In accordance with its duties, the Diskominfo of West Java Province is required to carry out good and sustainable information security governance so as to avoid information security incidents. Poor management of information security governance can have an impact on the low quality

of service so that it can affect the reputation of the Diskominfo of West Java Province and cause risks that can be detrimental.

In carrying out its business processes, Diskominfo of West Java Province still has risk problems, namely the frequent occurrence of information security incidents that cause disruption to the institution's business processes where some incidents that occur can be resolved directly (reactive) in the field, but some other incidents require planning and a lot of time to solve them and there is no proper supervision and planning in managing data and information security (Rilyani et al., 2015).

There are several problems after the researchers conducted an initial survey of the problems in the field: Diskominfo West Java Province faces increasing information security threats, both from external cyber attacks and internal weaknesses. This can have an impact on the confidentiality, integrity and availability of public information that is managed. Risk Management The information security risk management process has not been structured in accordance with international standards, potentially leading to inefficiencies in risk identification, mitigation and control. Compliance with ISO/IEC 27001:2022: With the update of the ISO/IEC 27001 standard to version 2022, there is an urgent need to align information security risk management with the latest principles to remain relevant and effective in facing modern challenges. Gaps in Human Resources Capacity and Technology There are still gaps between the technology needs and skills of human resources and the standards required by ISO/IEC 27001:2022, which may hinder the optimal implementation of information security management systems. Impact on Public Services: Information security risks that are not managed properly can affect the quality of public services, especially in the context of transparency and accountability of information that the public needs.

Based on the background, this research is discussed and focused on the preparation of "Information Security Risk Management Based on ISO 27001: 2022 at Diskominfo West Java Province".

2. Literature Review

2.1 Standard ISO/IEC 27001:2022

The ISO/IEC 27001:2022 update introduced several significant changes compared to previous versions, mainly to address evolving cybersecurity challenges and enhance digital trust. One of the key updates is the restructuring of Annex A, in line with the revised ISO/IEC 27002:2022, which reflects a more streamlined and comprehensive set of security controls (Vinet & Zhedanov, 2011a). This restructuring includes the introduction of eleven new security controls, primarily addressing the protection of cloud computing services, which have become increasingly important to businesses (Malatji, 2023). The update also emphasized the integration of the standard with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, particularly enhancing the Protect Function, which maintains a high-frequency distribution of security controls similar to the 2013 version (Malatji, 2023). Furthermore, implementation of the updated standard has shown practical improvements in information security management systems (ISMS), such as improved confidentiality, integrity, and availability controls, leading to a significant reduction in security incidents (Chavez et al., 2024). These improvements make ISO/IEC 27001:2022 a more robust framework for organizations aiming to protect their information assets in a rapidly changing digital landscape (Chavez et al., 2024).

The relevance of information security standards in government agencies is underscored by the increasing threats to sensitive data, which require a strong legal and technical framework to protect state and commercial secrets. Legal provisions play an important role in building the foundations of information security, as highlighted by Seydvalieva, who emphasizes the need for legislative measures and international cooperation to protect government data(Seydvalieva, 2024). The implementation of standards such as ISO 27001 is essential in identifying vulnerabilities and ensuring compliance with security protocols, as demonstrated in educational institutions where these standards help reduce risk and improve data security(Ahmedi & Ibrahimi, 2024).

2.2 Implementation in Government Organizations

Adopting ISO/IEC 27001 in the government sector presents several challenges and barriers, as highlighted by various studies. One significant challenge is the immature communication between management and the information security landscape, which complicates risk assessment activities. This issue is particularly noted in the implementation of standards in Malaysian government agencies, where effective communication is critical to aligning security objectives with organizational goals (Awang et al., 2016). In addition, the integration of national regulations with international standards can be complex, as seen in the case of the Pedro Moncayo Cantonal Property Registry in Ecuador. This integration is necessary to ensure that public data security is maintained at a high standard, but requires careful coordination and adaptation of existing legal frameworks(Tintin & Hidalgo, 2023). Furthermore, the implementation process itself demands a shift from subjective perceptions of security to an objective understanding of security needs, which can be a cultural and operational hurdle for public institutions(Carvalho & Marques, 2019). Despite these challenges, successful implementation, as demonstrated by the Property Registry, can lead to significant improvements in data security and trust in public data management(Tintin & Hidalgo, 2023). However, achieving such success requires a commitment to continuous improvement and adaptation of security controls, as well as fostering a culture of security awareness within the organization(Carvalho & Marques, 2019).

2.3 Information Security Risk Management

The information security risk management process according to ISO/IEC 27001 involves a systematic approach to identify, assess and mitigate risks to ensure the confidentiality, integrity and availability of information. This process begins with the establishment of an Information Security Management System (ISMS), which is central to ISO/IEC 27001 and provides a framework for securely managing sensitive information(Vinet & Zhedanov, 2011b). The implementation plan for an ISMS includes a methodological cycle with phases and activities designed to facilitate the entire process, ensuring compliance and operational continuity(Hernandez et al., 2024). Risk management under ISO/IEC 27001 involves identifying potential risks, assessing their impact and likelihood, and implementing appropriate controls to mitigate them. For example, a study using the Failure Mode and Effect Analysis (FMEA) methodology identified and prioritized risks based on their severity, leading to targeted mitigation strategies(Wicaksono et al., 2022). The process also involves continuous monitoring and review to adapt to evolving threats, as demonstrated by a government agency's risk management efforts that identified 15 risks and 50 threats, with 42% categorized as moderate impact. In addition, ISO/IEC 27001 encourages a security-first culture within the organization, promoting awareness and best practices across departments(Folorunso et al.,

2024). Despite challenges such as resource constraints and the need for continuous updates, the adoption of ISO/IEC 27001 improves the organization's cybersecurity posture and aligns with regulatory compliance requirements(Folorunso et al., 2024). Overall, the risk management process under ISO/IEC 27001 is integral to developing a proactive cybersecurity strategy, ensuring the organization is resilient to information security threats.

2.4. Diskominfo West Java Province

Diskominfo, or the Office of Communication and Information Technology, plays an important role in managing information security at the provincial level by implementing comprehensive IT governance and cybersecurity measures. Diskominfo's responsibilities include ensuring accountability, reliability, and trustworthiness of information within the institution, which are critical for effective information security governance(Fahmi Rifai et al., 2023). In addition, Diskominfo is tasked with securing web servers against vulnerabilities and potential attacks, such as cross-site scripting, by using tools such as OWASP scanners to provide recommendations for improving web server security(Wijayanto et al., 2020). Effective IT governance is also a key responsibility, as demonstrated by the use of frameworks such as COBIT 4.1 and COBIT 2019 to assess and improve IT governance maturity levels, ensuring that IT resources are managed efficiently and risks are mitigated(Ringga, 2022). In addition, Diskominfo contributes to building cybersecurity resilience by establishing a Computer Security Incident Response Team (CSIRT) to manage cyber risks, analyze threats, and develop countermeasures, thereby increasing the overall cyber awareness and resilience of the provincial government(Patrick et al., 2018). This responsibility highlights Diskominfo's integral role in safeguarding information and ensuring the continuity of government operations in the face of evolving cyber threats.

2.5 Research Gaps

In researching the literature on Discominfo West Java and ISO/IEC 27001:2022, several research gaps emerged, particularly in the context of operational excellence and information security management. A systematic literature review by Kovilage et al. highlighted a lack of focus on the impact of operational and dynamic capabilities on operational excellence, as well as shortcomings in theoretical frameworks to explain this phenomenon across different industry sectors and geographical regions(Kovilage et al., 2022). This gap is pertinent to Discominfo West Java, as understanding these capabilities can improve the implementation of ISO/IEC 27001:2022, which is critical for information security management. Furthermore, Holt's exploration of online black markets underscores the need for further research into the social dynamics and practices of market participants, which can inform the development of more robust security measures under ISO/IEC 27001:2022(Holt, 2017). Lastly, Sin and Jusoh emphasize the importance of systematically identifying and prioritizing research gaps, which is critical to advancing the understanding and application of ISO/IEC 27001:2022 in diverse organizational settings(Sin & Jusoh, 2019). Collectively, these insights point to the need for more comprehensive research in the integration of operational excellence and information security standards, particularly in the context of Discominfo West Java.

3. Research Methods

The method used uses a measurement framework based on ISO / IEC 27005: 2022. The ISO 27005:2022 method used includes 4 (four) parts, namely risk identification, risk analysis, risk

evaluation, and risk treatment (Supradono, 2009) which are explained using the diagram 1 below:

Problem Identification: The first step of this research is to identify problems in the Communication and Informatics Office of West Java Province by conducting observations and interviews. **Literature Study:** A Literature Study is a method of collecting data by collecting documents, books, or other reference media that support solving research problems, which are then studied in order to find a solution to the problem. Data will be collected through interviews with SMK managers of work units at the Diskominfo of West Java Province as respondents of this study. The questions for the interview are as follows Table 1:

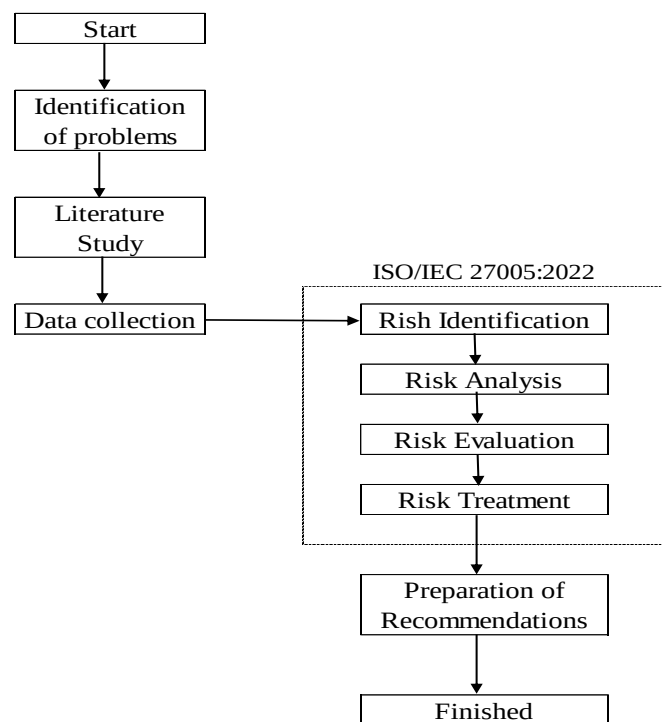


Figure 1. Methodology Diagram

Table 1 Question List

No.	Question	Control ISO/IEC 27001:2022
1.	What are the information assets that are important to the organization? How are these assets identified and categorized?	Clause 8.1 (Operational planning and control), Annex A.8.1 (Asset inventory)
2.	What are the main threats faced by information assets in organizations?	Clause 6.1.2 (Information security risk assessment)
3.	Is there a process in place to assess the impact in the event of a breach of these information assets?	Annex A.8.1 (Asset inventory), Clause 6.1.2 (Information security risk assessment)

No.	Question	Control ISO/IEC 27001:2022
4.	What controls have been implemented to reduce information security risks?	Clause 6.1.3 (Handling information security risks), Annex A.12.1 (Operational procedures and responsibilities)
5.	How does the organization identify and evaluate vulnerabilities that could be exploited by the threat?	Klausul 6.1 (Tindakan untuk mengatasi risiko dan peluang)
6.	What controls have been planned to reduce information security risks?	Clause 6.1.3 (Handling information security risks), Annex A.12.1 (Operational procedures and responsibilities)
7.	How is the effectiveness of these controls monitored and measured?	Clause 9.1 (Monitoring, measurement, analysis and evaluation), Annex A.12.1 (Operational procedures and responsibilities)

2.1. Risk Identification

The preparation of Information Security Risk Management based on ISO/IEC 27001 at Diskominfo, West Java Province, involves a comprehensive approach to risk identification, which is an essential component of an Information Security Management System (ISMS). The ISO/IEC 27001 standard provides a structured framework for implementing an ISMS, emphasizing the need for a thorough risk assessment process that includes risk identification, analysis, and evaluation. Risk identification, as highlighted in the literature, has traditionally been asset-centric, which can be complex and subjective, relying heavily on the expertise of information security practitioners. However, innovative methodologies propose to move away from this approach by incorporating Risk Indicators, which allow for a more objective and scientific analysis, thus increasing stakeholder confidence. In practice, risk identification involves documenting potential risks and their causes, as demonstrated in a study conducted at a private university in Surabaya, which faced incidents such as hacking, underlining the importance of preventive, detective and corrective security measures. In addition, the integration of ISO/IEC 27001 with local regulations, such as Indonesia's Personal Data Protection Law, can provide a strong framework for data protection, aligning international standards with local legal requirements (Nugraha & Nasyuha, 2024). This integration is crucial for organizations like Diskominfo to ensure comprehensive data protection and compliance with global and local mandates. Overall, the risk identification process at Diskominfo should leverage these insights to build a resilient information security posture that addresses both technical and regulatory challenges.

2.2. Risk Analysis

The preparation of information security risk management based on ISO/IEC 27001 involves a structured approach to identify, analyze and mitigate risks associated with information systems. Implementing an Information Security Management System (ISMS) according to ISO 27001 requires a comprehensive plan that includes a series of stages and activities to ensure the confidentiality, integrity, and availability of information, as demonstrated in a case study of a higher education institution (Hernandez et al., 2024). The process starts with setting the context, followed by risk identification, analysis, evaluation, and maintenance, as outlined in a study of a telecommunications company using ISO 27005, which supports the requirements of ISO 27001 (Jaya Putra et al., 2020). Failure Mode and Effect Analysis (FMEA) methodology is another approach used to assess risks, resulting in a Risk Priority Number to prioritize risks

Published by:

from highest to lowest, as applied in a national government agency(Wicaksono et al., 2022). This method helps in categorizing risks into high, medium, and low levels, which are then mitigated using the ISO 27002 standard(Wicaksono et al., 2022). In addition, recommendation PN-ISO/IEC 27005:2014-01 provides a qualitative method for evaluating IT risks, focusing on threats that can damage telecommunication systems and information resources. Collectively, these methodologies and standards provide a robust framework for managing information security risks, ensuring that organizations can effectively protect their information assets.

2.3. Risk Evaluation

The preparation of information security risk management based on ISO/IEC 27001 involves a systematic approach to identifying, evaluating, and mitigating risks associated with information technology assets. The ISO 27001 standard provides a framework for establishing, implementing, maintaining and continuously improving an information security management system (ISMS). A key component of this process is risk evaluation, which can be done effectively using methodologies such as Failure Mode and Effects Analysis (FMEA). These methods assist in determining the Risk Priority Number (RPN) to prioritize risks from highest to lowest, as demonstrated in a case study of a national government agency where 14 risk classifications were identified, with varying levels of risk that were then mitigated using the ISO 27002:201 standard(Wicaksono et al., 2022). In the telecommunications sector, ISO 27005 complements ISO 27001 by providing guidelines for risk management, emphasizing the importance of selecting appropriate control objectives to support the ISMS. This involves establishing context, risk identification, analysis, evaluation, and treatment, resulting in prioritized impact scenarios and controller objectives(Jaya Putra et al., 2020). In addition, the implementation of ISO 27001 in academic environments, such as at Surabaya State University, has shown a positive impact on data security by addressing cyber threats and physical risks, thus improving the integrity and protection of sensitive information(Intan Mafiana et al., 2023). Overall, continuous risk evaluation and the implementation of appropriate controls are essential to maintaining a robust information security management system in various sectors.

Risk Evaluation, which is determining which risks require treatment and how to prioritize the treatment carried out at this stage, namely defining existing controls to reduce the impact and possibility of risks that have been running in accordance with the ISO / IEC 27001: 2022 standard which is evidenced in filling out the form as follows:

Likelihood Criteria

2.3.1 Likelihood Criteria

Likelihood criteria are criteria for defining, determining or measuring objectively or subjectively the likelihood of threats to assets which are expressed qualitatively as follows (West Java Governor Regulation Number 6 of 2023).

Table 2. Likelihood Criteria

Level	Frequency of Occurrence
Very Low (1)	Threat occurs once > 5 years
Low (2)	The threat may occur once over 2 to 5 years
Intermediate (3)	The threat may occur once in 1-2 years
Height (4)	Threats may occur several times a year
Very High (5)	Threats occur almost every day/month

Published by:

2.3.2 Impact Criteria

Impact Criteria (Impact or Consequences) specify the degree or cost that the West Java Provincial Diskominfo must bear in the event of an incident or attack on information assets, quantified as follows: (West Java Governor Regulation Number 6 of 2023).

Table 3. Impact Criteria

Level	Financial Impact	Operational Impact	Quality Impact/Month	Reputation Impact
Not Significant (1)	Causing a loss of funds of less than Rp. 10,000,000,-	Disrupts system function (less than 5 hours)	Number of complaints less than 5	There is negative news but it does not result in a decrease in trust
Small (2)	Causes a loss of funds of Rp. 10,000,000 to Rp. 50,000,000	Disrupts system function (5 hours to 1 day)	Number of complaints 5 to 10	There is negative news that can affect performance and policies.
Intermediate (3)	Causing a loss of funds of more than Rp. 50,000,000,- to Rp. 200,000,000,-	Disrupting system function (more than 1 day to 7 days)	Number of complaints more than 10 to 20	There is negative news that reduces stakeholder trust
Big (4)	Causing a loss of funds of more than Rp. 200,000,000,- to Rp. 1,000,000,000,-	Disrupting system function (more than 7 days to 1 month)	Number of complaints more than 20 to 30	Deterioration/losses of stakeholder trust
Very Big (5)	Causing a loss of funds of more than Rp. 1,000,000,000,-	Causes disruption to system function (more than 1 month)	Number of complaints more than 30	Giving rise to legal claims

2.3.3 The Risk Value

The risk value is the level of risk determined based on the value (criteria) of impact and the value (criteria) of probability expressed quantitatively as follows: (West Java Governor Regulation Number 6 of 2023).

Table 4. The Risk Value

Likelihood	Impact (<i>Impact/Consequences</i>)				
	Not Significant (1)	Small (2)	Intermediate (3)	Big (4)	Very Big (5)
Very Low (1)	Low (1)	Low (2)	Low (3)	Low (4)	Intermediate (5)

Low (2)	Low (2)	Low (4)	Intermediate (6)	Intermediate (8)	Intermediate (10)
Intermediate (3)	Low (3)	Intermediate (6)	Intermediate (9)	Height (12)	Height (15)
Height (4)	Low (4)	Intermediate (8)	Height (12)	Very High (16)	Very High (20)
Very High (5)	Intermediate (5)	Intermediate (10)	Height (15)	Very High (20)	Extreme (25)

2.4. Risk Treatment

Information Security Risk Management (ISRM) based on ISO/IEC 27001 is a structured approach to managing risks associated with information systems, ensuring the confidentiality, integrity, and availability of information. The ISO/IEC 27001:2022 standard provides a comprehensive framework for ISRM, emphasizing the identification, evaluation, and treatment of risks to reduce potential threats to information security (Paksoy, 2023). The process begins with setting the context, followed by risk identification, analysis, evaluation, and treatment, as outlined in ISO 27005, which complements ISO 27001 by providing detailed guidance on the risk management process (Jaya Putra et al., 2020). The integration of the ISO/IEC 27005:2018 and NIST SP 800-30 frameworks further enhances risk assessment and management, especially in sectors such as insurance, where vulnerabilities exist (Putra & Soewito, 2023). Effective ISRM involves continuous monitoring and improvement, with organizations required to adapt their security measures to evolving threats and technological advances (Hernandez et al., 2024). Despite the availability of these standards, many organizations still face challenges in implementing adequate security measures, underscoring the need for comprehensive risk management strategies and software tools to facilitate compliance and reporting (Paksoy, 2023). The implementation of ISRM in various sectors, such as telecommunications and higher education, demonstrates the importance of a customized risk control program that aligns with organizational objectives and the specific requirements of ISO 27001 (Jaya Putra et al., 2020) (Hernandez et al., 2024). Risk Treatment is a stage to select options that can reduce or eliminate the impact and possibility of risk occurrence (Supristiowadi & Sucahyo, 2018).

2.5. Drafting Recommendations

The preparation of recommendations for preparing information security risk management based on ISO/IEC 27001 involves a comprehensive approach that integrates various methodologies and frameworks to ensure robust security measures. The implementation of an Information Security Management System (ISMS) based on ISO/IEC 27001:2013, as demonstrated in higher education institutions, involves a structured methodological cycle that includes phases and activities designed to facilitate the entire implementation process, ensuring process and continuity (Hernandez et al., 2024). This approach is essential for linking personnel to compliance with standards and raising awareness about the importance of information security. In addition, the integration of frameworks such as NIST CSF 2.0 and CIS Control v8 with ISO/IEC 27001:2022 provides a synthesis of key components such as risk management processes, security policy implementation, and incident response planning, which are essential for developing comprehensive information security measures (Tanjung et al., 2024). In the university context, the rapid development of information technology requires managing information security through standardized risk-based documents, including policy documents,

procedure guidelines, and work instructions to address emerging threats (Fitriani, 2022). Furthermore, in clinical laboratories, risk assessment using ISO/IEC 27001 involves the identification, analysis and evaluation of risks to ensure effective information security controls, highlighting the need for vigilance in the use of information systems (Susanto et al., (2023)). These studies collectively underscore the importance of a multi-faceted approach to information security risk management, emphasizing the need for continuous improvement and adaptation to technological advances.

Preparation of Recommendations is the last stage of this research. The aim is to provide recommendations for the resolution of known risks based on the ISO / IEC 27001: 2022 standard so that later the existing risks can be properly mitigated.

2.6 Previous Research

Table 5. Previous Research

No.	Authors	Conclusion	Difference from Research Title	Similarity with Research Title
1	Syahindra et al., 2022	Evaluation of information security at the XYZ Province Diskominfo using KAMI Index and ISO/IEC 27005:2011 showed that the institution had not optimally implemented information security risk management, leading to internal and external incidents.	Focuses on evaluating information security risks using ISO/IEC 27005:2011 at XYZ Province Diskominfo.	Discusses information security risk management at government institutions (Diskominfo) with the ISO/IEC 27001 approach.
2	Alberto & Karyati, 2023	The design of an Information Security Management System (ISMS) based on ISO 27001:2022 at the Tangerang Selatan Diskominfo Data Center showed that the institution lacked a structured ISMS, necessitating appropriate ISMS design.	Case study on the Tangerang Selatan Diskominfo Data Center focusing on ISMS design.	Utilizes ISO 27001:2022 standards in designing information security management at government institutions.
3	Khamil, 2022	The readiness level evaluation of information security at the Gianyar Regency Diskominfo using KAMI Index 4.2 and ISO/IEC 27001:2013 resulted in a "Not Eligible" status to meet ISO/IEC 27001 standards, necessitating improvement recommendations.	Conducted at Gianyar Regency Diskominfo using KAMI Index 4.2 and ISO/IEC 27001:2013.	Evaluates information security readiness at government institutions with ISO/IEC 27001 standards.

4	Yuze et al., 2016	The analysis of the Information Security Management System (ISMS) at the Directorate of Higher Education Information Systems using ISO/IEC 27001:2013 highlighted the need for maturity level improvements and a recommended system model using Data Flow Diagram.	Focuses on an educational institution (Directorate of Higher Education Information Systems) and ISO/IEC 27001:2013 analysis.	Uses ISO/IEC 27001 standards for information security management analysis.
5	Asriyar & Manurung, 2016	The application of information security risk management based on ISO/IEC 27001:2013 at PT. XYBASE Indonesia proved effective in reducing vulnerability levels by 30%.	Case study on a private company (PT. XYBASE Indonesia) focusing on risk management application.	Employs ISO/IEC 27001:2013 in information security risk management.

4. Results and Discussion

Researchers explained the description of the object of research, namely Diskominfo West Java Province, starting from the data collection process and analyzing information security risks from the results of data collection. The results of data collection that the author has carried out during the preparation of this research are as follows:

Determination of Context

From the results of interviews that have been conducted referring to the main tasks and functions at the Diskominfo of West Java Province, the scope of SMKI at the Diskominfo of West Java Province is obtained as follows:

1. Network and data center services
2. Government administration application services
3. General application services
4. Information security services
5. Data and information services
6. Internal facilities and infrastructure services
7. Public information and communication services

Identifikasi Aset

Assets that have been identified in the existing services at Diskominfo of West Java Province are:

1. Information assets in the form of both print and electronic
2. Software assets in the form of applications, systems and development tools
3. Hardware and software infrastructure assets
4. Assets of supporting facilities and infrastructure (utility)
5. Human resource assets and third parties

3.1. Risk Identification

From the interviews that have been conducted with resource persons, the information security risks that exist in the Diskominfo of West Java Province can be identified as follows:

From the results of risk identification that has been carried out, there are 41 (forty-one) information security risks consisting of 16 (sixteen) information risks (print / electronic), 13 (thirteen) software risks (applications, S / W systems, development tools), 5 (five) hardware and network infrastructure risks, 3 (three) risks of facilities and supporting facilities (utility) and 4 (four) risks of human resources and third parties that can be identified and spread across 7 (seven) work units at Diskominfo West Java Province.

The risk identification process in preparing Information Security Risk Management at Diskominfo, West Java Province, based on ISO/IEC 27001, involves a comprehensive approach to understanding and mitigating potential threats to information systems. The study by Kanka Wiemas N.G. and Jarot S. Suroso highlighted the identification of 15 risks and 50 threats, with 42% of these risks categorized as having a moderate impact, emphasizing the importance of a structured risk management process to maintain information confidentiality. Similarly, research conducted at SMAN 12 Bandung showed the implementation of ISO 27001:2013, where the risk assessment revealed a risk opportunity of 45% and a risk severity of 47%, indicating the need for continuous monitoring and improvement through the PDCA cycle to enhance the Information Security Management System (ISMS) (Pamungkas et al., 2024). In a clinical laboratory setting, Eddy Susanto et al. identified 35 significant risks within the Busdev&IT Department, underscoring the need for vigilant information security practices to protect sensitive data (Susanto et al., 2023). Furthermore, a study at XYZ Institute using the FMEA method identified various levels of risk, including 4 high-risk threats, which require targeted security measures to ensure operational continuity (Kusnandar et al., 2024). Finally, Jevelin and Ahmad Faza's evaluation of a private contractor's ISMS maturity highlighted the challenges of meeting the ISO 27001 standard, reinforcing the need for a robust security framework and continuous improvement to achieve certification (Jevelin & Faza, 2023). Collectively, these studies illustrate the critical role of risk identification and management in maintaining information security in various sectors, guided by the principles of ISO/IEC 27001.

3.2. Risk Analysis

From the risks identified above, the next step is to analyze the identified security risks based on the likelihood described in table 2 likelihood criteria and their impact based on table 3 impact criteria so that the risk value is obtained as a result of multiplying the likelihood value and impact value so that the risk category described in table 4 risk value is obtained. For example, there is an application repository risk with a likelihood value of 4 with a frequency of threat events that may occur several times a year and an impact value of 4 with a quality impact per month the number of complaints is more than 20 to 30 so that the risk value is 16 with a very high category. The risks that have been analyzed are described in the following table:

From the results of risk identification that has been carried out, there are 41 (forty-one) information security risks consisting of 16 (sixteen) information risks (print / electronic), 13 (thirteen) software risks (applications, S / W systems, development tools), 5 (five) hardware and network infrastructure risks, 3 (three) risks of facilities and supporting facilities (utility) and 4 (four) risks of human resources and third parties that can be identified and spread across 7 (seven) work units at the Diskominfo of West Java Province.

Published by:

Risk analysis to prepare for information security risk management based on ISO/IEC 27001 at Diskominfo, West Java Province, involves understanding the current state of information security and identifying potential risks and threats. The implementation of ISO/IEC 27001:2022 in government agencies in Indonesia revealed 15 risks and 50 threats, with 42% of these risks having a moderate impact, highlighting the importance of risk management in maintaining information confidentiality and security. Similarly, the implementation of ISO/IEC 27001:2013 in educational institutions, such as SMAN 12 Bandung, showed a high level of compliance with security procedures, reaching an implementation rate of 81.43%, which underscores the effectiveness of a structured risk management framework in improving information security (Pamungkas et al., 2024). In a clinical laboratory, the use of the ISO/IEC 27001 standard identified significant risks, especially in the Busdev&IT Department, which required increased vigilance and effective risk control measures to secure sensitive information (Susanto et al., 2023). In addition, the use of Fuzzy FMEA based on ISO/IEC 27001:2013 in another study identified 13 very high priority risks, indicating the need for improved documentation and compliance with security policies to increase public trust (Kusnandar et al., 2024). Finally, a gap analysis at Madiun City Diskominfo showed 71% readiness for ISO/IEC 27001:2013 certification, with significant improvements needed in planning to fully meet the requirements of the standard. These findings collectively emphasize the critical role of ISO/IEC 27001 in systematically managing information security risks and improving organizational readiness and resilience to potential threats.

3.3. Risk Evaluation

The evaluation of information security risk management at Diskominfo, West Java Province, based on ISO/IEC 27001, involved a comprehensive assessment of the current Information Security Management System (ISMS) and alignment with ISO standards. This research highlights the importance of robust data security measures, as demonstrated by the evaluation of a private contractor's ISMS, which revealed a maturity level below the ISO 27001 benchmark, emphasizing the need for improvement through the PDCA cycle (Jevelin & Faza, 2023). Similarly, the implementation of ISO 27001:2013 in educational environments, such as SMAN 12 Bandung, showed a high level of compliance with the standard, with a risk rating of 49% and control implementation at 100%, indicating effective risk management practices (Pamungkas et al., 2024). In a government agency, the risk management process identified 15 risks and 50 threats, with 42% of risks having a moderate impact, underscoring the need for ongoing risk mitigation strategies. In a clinical laboratory, an information security risk assessment revealed significant vulnerabilities, particularly in the Busdev&IT Department, requiring increased vigilance and risk control measures (Susanto et al., 2023). Furthermore, the use of the FMEA method at XYZ Institution identified varying levels of risk, highlighting the need for focused attention on high-risk threats to ensure information security (Kusnandar et al., 2024). Collectively, these studies underscore the important role of ISO/IEC 27001 in guiding risk evaluation and management, ensuring that organizations such as Diskominfo can effectively protect their information systems against potential threats.

From the results of the risk evaluation that has been carried out, a risk evaluation is carried out by identifying the controls that have been carried out and re-evaluating the impact criteria and the possibility arising from these risks which can be seen in the following table: From the results of the risk evaluation that has been carried out based on existing control, there is still 1 (one) risk with a high category and 15 (fifteen) risks with a medium category.

3.4. Risk Treatment

The implementation of ISO/IEC 27001 for information security risk management at Diskominfo, West Java Province, involves a comprehensive approach to identifying, assessing and mitigating risks associated with information systems. The study by Kanka Wiemas N.G. and Jarot S. Suroso highlighted the identification of 15 risks and 50 threats, with 42% of these risks categorized as having moderate impact, emphasizing the need for effective risk mitigation strategies (Wiemas N.G. & Suroso, 2024). In the same vein, a study conducted at SMAN 12 Bandung showed the implementation of ISO 27001:2013, where risk opportunity and severity were found to be around 45% and 47% respectively, with a high implementation rate of 81.43% for ISMS procedures, indicating a robust risk management framework (Pamungkas et al., 2024). Furthermore, a study at XYZ Institution using the FMEA method identified various levels of risk, including 4 high-risk threats, underscoring the importance of prioritizing information security to ensure operational continuity (Kusnandar et al., 2024). In addition, a study of a clinical laboratory in Jakarta revealed significant risks within the Busdev&IT Department, requiring increased vigilance and control measures to secure sensitive information (Susanto et al., 2023). Finally, a study of the XYZ Population Office using a fuzzy FMEA approach identified 13 very high priority risks, indicating the need for increased compliance with the ISO/IEC 27001:2013 standard to improve information security and public trust (Kusnandar et al., 2024). Collectively, these studies underscore the critical role of ISO/IEC 27001 in structuring an effective risk management process, highlighting the need for continuous evaluation and adaptation of security measures to address evolving threats.

From the results of the risk evaluation stage, it is obtained that the risk status is still in the middle to upper category. At this risk, it is required to have risk treatment for each risk. The risk treatment that has been prepared is as follows: From the results of the risk treatment that has been planned, there is 1 (one) risk with a medium category and 40 (forty) have a low category.

3.5. Drafting Recommendations

The development of recommendations for information security risk management based on ISO/IEC 27001 at Diskominfo, West Java Province, can draw valuable insights from various studies on the implementation and evaluation of the ISO 27001 standard. The evaluation of an Information Security Management System (ISMS) for ISO 27001 certification highlights the importance of the PDCA (Plan, Do, Check, Act) cycle in achieving compliance, although it also shows the need for improvement to fully meet the certification requirements (Jevelin & Faza, 2023). In the education sector, the implementation of ISO 27001:2013 in a web-based application showed a high level of compliance, with 81.43% of procedures effectively implemented, suggesting that a structured approach to risk management can significantly improve ISMS maturity (Pamungkas et al., 2024). In addition, integrating ISO 27001 with local regulations, such as Indonesia's Personal Data Protection Law, can provide a comprehensive framework that aligns international standards with local legal requirements, thus improving data protection strategies (Nugraha & Nasyuha, 2024). In government agencies, the risk management process based on ISO/IEC 27001:2022 has identified many risks and threats, with most categorized as medium impact, underscoring the need for continuous risk assessment and mitigation (Wiemas N. G. & Suroso, 2024). Finally, the maturity level of information security controls in academic settings, as measured by the ISO 27001 System Security Engineering Capability Maturity Model, suggests that adherence to standardized procedures can lead to

stable and secure information systems (Nurbojatmiko et al., 2024). These findings collectively suggest that Diskominfo should adopt a comprehensive risk management strategy that incorporates the PDCA cycle, aligns with local regulations, and continuously assesses and mitigates risks to improve their ISMS maturity and compliance with the ISO/IEC 27001 standard.

At this stage, the author will provide recommendations for all risks that have been identified referring to the ISO/IEC 27001: 2022 annex. The recommendations that have been prepared for the existing risks at the Diskominfo of West Java Province are as follows:

By implementing the above recommendations, it is expected that the organization can increase resilience to security threats, ensure compliance with international standards, and protect information assets from potential losses. The author encourages the implementation and continuous monitoring of the suggested policies and procedures to create a safe and secure working environment. Periodic evaluation and policy adjustments will also support adaptation to changing technologies and evolving threats, ensuring that information security remains a top priority in every aspect of operations.

5. Conclusion

The implementation of ISO/IEC 27001 for information security risk management at Diskominfo of West Java Province is a strategic step to improve data protection and align with international standards. The integration of ISO/IEC 27001:2022 with Indonesia's Personal Data Protection Law provides a comprehensive framework that addresses international and local regulatory requirements, emphasizing a risk-based approach and data subject rights. This is particularly important for Diskominfo, as current systems, such as employee attendance applications, face challenges in data processing efficiency and security, which can be mitigated by adopting a structured information security management system (ISMS). The experience of other institutions, such as IT Telkom Purwokerto, highlights the importance of a detailed risk management plan that includes asset identification, risk assessment, and business impact analysis, all of which are integral parts of ISO 27001 compliance. By adopting these practices, Diskominfo can effectively manage information security risks, ensuring the confidentiality, integrity and availability of its data assets, thereby improving its operational efficiency and confidence in public services.

Based on the results of the identification of information security risks that have been carried out at the Diskominfo of West Java Province, there are five assets/processes/services that can affect the failure of the running business process. The five assets/processes/services are information (print/electronic), software (applications, systems, development tools), hardware and network infrastructure, facilities and supporting facilities (utility) and human resources and third parties. These risk sources have risks that can affect the organization's operational processes, including the source of information risk (print / electronic) has sixteen risks, namely synchronization of SMKI policies and other policies, internal and external IT audit results, IT security incident reporting, official email, application repository, application development, main PPID, social media accounts, micro data services (podes, susenas, sakernas), exempted data, LAN cable labeling documentation and internal office network topology mapping, IP DHCP, data center documentation, network documentation, IT access issuance documents and source code. Furthermore, the source of software risk (applications, systems, development tools) has thirteen risks, namely information security support applications, use of open source applications, encryption, application architecture design, authentication, SSRF, web

Published by:

defacement, malware, application management, personal data, cloud services, division of workspace environment for application development and device assets and portable computers. Then the source of hardware and network infrastructure risk has five information security risks, namely office access, internet and intranet network infrastructure for data centers, network security devices, jabar cloud servers and public cloud servers. Furthermore, the source of risk for facilities and supporting facilities (utility) has three risks, namely the Work Unit Workspace, precision air conditioner and data center generator. Furthermore, the source of risk for human resources and third parties has four information security risks, namely the condition of human resources and the condition of concern for information security, contractual agreements with goods / services providers, the number of information security human resources and the condition of human resources and the condition of concern for information security.

From the risks that have been successfully identified, risk control is carried out to minimize the risk categories that have been analyzed. At the stage of risk without control (inherent risk) there are two risks with extreme categories, nine risks with very high categories, sixteen risks with high categories, eleven risks with medium categories and three risks with low categories. Then identification is carried out based on existing controls that have been carried out so that the current risk after existing control has one risk in the high category and fifteen risks in the medium category. Thus, the risk control that has been implemented by the Diskominfo of West Java Province is quite effective in reducing the risk category.

The information security risk mitigation plan that will be carried out by Diskominfo West Java Province to continue to reduce one risk with a high category and fifteen risks with a medium category refers to the clauses and annexes in ISO / IEC 27001:2022, namely providing account misuse information to the user's alternative email and to the employee's work unit email, socializing awareness of email usage to all employees and work units, adjusting repository service SOPs, adding special repository accounts for third parties, developing information service business processes through the PPID website, developing information service features on the PPID website to make it more interactive, making SK / SP regarding the person in charge of managing social media accounts, checking the history of changes in computer network cable labeling and computer topology mapping, periodic review of user access to data center documentation, periodic review of user access to network documentation, reviewing remote access rights, implementation of secure bridging system for private data exchange, environment separation, different domain names and public IP selection for staging and production environments, periodic QA code review to ensure no hardcoded credentials or configurations in application source code, database separation for staging and production, use of different accounts for staging and production, periodic user testing before the application is uploaded from the staging environment to production, installation/extend antivirus licenses on all computer/laptop devices, add a layer of security with a web application firewall to prevent massive attacks and with specific targets, perform document labeling, periodic monitoring of pacs, periodic heating of generators and propose additional employees.

Based on the results of the analysis that has been carried out, the advice that can be given to the Diskominfo of West Java Province regarding information security risk management is that the Diskominfo of West Java Province can implement the risk mitigation recommendations that have been prepared based on ISO / IEC 27001: 2022 and monitor the risk controls that have been made to continue to be implemented and the risk mitigation plan that has been

planned to be realized in accordance with the agreed targets and can evaluate information security risks regularly to ensure that the services provided by the Diskominfo of West Java Province can run optimally and optimally.

The shortcomings in this study are the need for more detailed risk identification of applications developed by Diskominfo of West Java Province so that each application developed has its own list of risks along with mitigation steps for each application. So that the advice that can be given by researchers for further research is that it is hoped that research related to information security risk management can be an option for conducting research carried out, especially for information security risk management for applications.

To prepare for ISO/IEC 27001-based information security risk management at the Diskominfo of West Java Province, it is important to follow a structured approach that integrates international standards and local regulatory requirements. Implementing an Information Security Management System (ISMS) based on ISO/IEC 27001:2013 involves a series of phases, including risk identification, analysis and evaluation, as demonstrated in the clinical laboratory study, which identified 35 significant risks that require treatment based on risk appetite. A gap analysis, similar to the one conducted at Madiun City Diskominfo, can be instrumental in assessing current readiness and identifying areas that need improvement, such as planning, which has the lowest percentage of readiness. In addition, integrating ISO/IEC 27001 with Indonesia's Personal Data Protection Law can provide a strong framework for data protection, ensuring compliance with international standards and local legal requirements. The experience of Central Java Province Bapenda highlights the importance of asset identification and risk mitigation using controls from NIST and ISO-IEC 27001:2013, which can be customized to effectively manage high-risk assets. Finally, a comprehensive implementation plan, such as the one developed for the IUB university institution, can facilitate the process by scheduling activities and raising awareness among personnel on the importance of information security, ensuring the ISMS is fully operational within the set timeline. This multi-faceted approach will help the Diskominfo of West Java Province achieve effective information security risk management and ISO/IEC 27001 certification.

6. References

- Ahmedi, B., & Ibrahim, A. (2024). Mastering information security through standard implementation. *International Journal of Informatics and Communication Technology*, 13(3), 428–435. <https://doi.org/10.11591/ijict.v13i3.pp428-435>
- Budiarto, R. (2017). Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode FMEA dan ISO 27001 pada Organisasi XYZ. *CESS (Journal of Computer Engineering System and Science)*, 2(2), 48–58. <https://doi.org/https://doi.org/10.24114/cess.v2i2.6264>
- Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. *Iberian Conference on Information Systems and Technologies, CISTI*, 2019-June. <https://doi.org/10.23919/CISTI.2019.8760870>
- Chavez, S., Anahue, J., & Ticona, W. (2024). Implementation of an ISMS Based on ISO/IEC 27001:2022 to Improve Information Security in the Internet Services Sector. *Proceedings of the 14th International Conference on Cloud Computing, Data Science and Engineering, Confluence 2024*, 184–189. <https://doi.org/10.1109/Confluence60223.2024.10463392>
- Fahmi Rifai, Jazman, M., Angraini, A., & Megawati, M. (2023). Design of Application Information

- Security Self-Assessment Using Vba and Msxml2.Xmlhttp Case Study: Diskominfo Kabupaten Kampar. *Jurnal Teknik Informatika (Jutif)*, 4(6), 1523–1534. <https://doi.org/10.52436/1.jutif.2023.4.6.1033>
- Fajri, K. S. Al, & Harwahu, R. (2024). Information Security Management System Assessment Model by Integrating ISO 27002 and 27004. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, 4(2), 498–506. <https://doi.org/10.57152/malcom.v4i2.1245>
- Fitriani, L. D. (2022). Risk Risk Assessment and Development of Access Control Information Security Governance Based on ISO/IEC 27001:2013 At XYZ University. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, 9(2), 891–907. <https://doi.org/10.35957/jatisi.v9i2.1643>
- Folorunso, A., Mohammed, V., Wada, I., & Samuel, B. (2024). *The impact of ISO security standards on enhancing cybersecurity posture in organizations*.
- Hernandez, L., Pranolo, A., & Wibawa, A. P. (2024). Implementation plan of the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis. Case study: Higher education institution. *Transactions on Energy Systems and Engineering Applications*, 5(2). <https://doi.org/10.32397/tesea.vol5.n2.635>
- Holt, T. J. (2017). Identifying gaps in the research literature on illicit markets on-line. *Global Crime*, 18(1), 1–10. <https://doi.org/10.1080/17440572.2016.1235821>
- Indonesia, G. of. (2023). *Peraturan Gubernur Jawa Barat Nomor 6 Tahun 2023 Tentang Pedoman Pengelolaan Risiko Di Lingkungan Pemerintah Daerah Provinsi Jawa Barat* (p. 100).
- Intan Mafiana, A., Hanum, L., Ilmi, H. M., & Febriliani, S. (2023). Implementasi Manajemen Keamanan Informasi Berbasis Iso 27001 Pada Sistem Informasi Akademik. *Journal of Digital Business and Innovation Management*, 2(2), 139–163. <https://doi.org/10.26740/jdbim.v2i2.57580>
- Jaya Putra, S., Nur Gunawan, M., Falach Sobri, A., Muslimin, J. M., Amilin, & Saepudin, D. (2020). Information Security Risk Management Analysis Using ISO 27005: 2011 for the Telecommunication Company. *2020 8th International Conference on Cyber and IT Service Management, CITSM 2020*. <https://doi.org/10.1109/CITSM50537.2020.9268845>
- Jvelin, J., & Faza, A. (2023). Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification. *Journal of Information Systems and Informatics*, 5(4), 1240–1256. <https://doi.org/10.51519/journalisi.v5i4.572>
- Kovilage, M. P., Yapa, S. T. W. S., & Hewagamage, C. (2022). Research Areas, Gaps and Future Research Directions of Operational Excellence: A Systematic Literature Review. *South Asian Journal of Business Insights*, 2(1), 3–32. <https://doi.org/10.4038/sajbi.v2i1.31>
- Kusnandar, A., Rochim, A. F., & Gunawan, V. (2024). *Pengukuran Tingkat Risiko dan Keamanan Informasi Menggunakan Metode FMEA Berbasis ISO / IEC 27001 pada Instansi XYZ untuk Keamanan Sistem Informasi*. 04. <https://doi.org/10.21456/vol14iss4pp375-384>
- Mahardika, F. (2017). Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang). *Jurnal Informatika: Jurnal Pengembangan IT*, 2(2), 1–8. <https://doi.org/10.30591/jpit.v2i2.484>
- Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *2023 International Conference on Cyber Management and Engineering, CyMaEn 2023*, 117–122. <https://doi.org/10.1109/CyMaEn57228.2023.10051114>
- Matondang, N., Isnainiyah, I. N., & Muliawatic, A. (2018). Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 2(1), 282–287. <https://doi.org/10.29207/resti.v2i1.96>

- Nugraha, A. A., & Nasyuha, A. H. (2024). Integrating ISO 27001 and Indonesia's Personal Data Protection Law for Data Protection Requirement Model. *Journal of Information Systems and Informatics*, 6(2), 1052–1069. <https://doi.org/10.51519/journalisi.v6i2.754>
- Nurbojatmiko, Aini, Q., Wasiqi, N. C., Alfajri, M. F., Ulinnuha, Z., Purwati, Y. K., Ayu, I. K., & Yasmin, N. A. (2024). Risk Assessment Maturity Level of Academic Information System Using Iso 27001 System Security Engineering-Capability Maturity Model. *Journal of Applied Engineering and Technological Science*, 5(2), 941–954. <https://doi.org/10.37385/jaets.v5i2.2971>
- Paksoy, A. A. M. P. M. (2023). Of azerbaijan high technical educational institutions azərbaycan ali texniki məktəblərinin xəbərləri. *Proceedings of Azerbaijan High Technical Educational Institutions*, 27(04). <https://doi.org/10.36962/PAHTEI>
- Pamungkas, A. C., Hulu, W. S., & Samihardjo, R. (2024). Information Security Risk Management Web-Based Final Semester Summative Assessment Application Using ISO 27001:2013. *Journal of Information Systems and Informatics*, 6(1), 349–362. <https://doi.org/10.51519/journalisi.v6i1.668>
- Patrick, H., van Niekerk, B., & Fields, Z. (2018). *Developing Cybersecurity Resilience in the Provincial Government*. 336–363. <https://doi.org/10.4018/978-1-5225-4763-1.ch012>
- Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *International Journal of Advanced Computer Science and Applications*, 14(4), 625–633. <https://doi.org/10.14569/IJACSA.2023.0140468>
- Rilyani, A. N., Firdaus, Y., & Jatmiko, D. D. (2015). Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000. *E-Proceeding of Engineering*, 2(2), 6201–6208. <https://doi.org/https://doi.org/10.35957/jatisi.v8i4.1082>
- Ringga, M. (2022). Analysis of Information Technology Governance at the Office of Communication and Information (Diskominfo) using the Cobit 4.1 Method. *Journal of Computer Scine and Information Technology*, 111–118. <https://doi.org/10.35134/jcsitech.v8i4.48>
- Seydvalieva, A. R. (2024). Legal provision of information security of state institutions. *Upravlenie Kachestvom (Quality Management)*, 7, 34–41. <https://doi.org/10.33920/pro-01-2407-05>
- Sin, K. Y., & Jusoh, M. S. (2019). Identifying and Prioritizing Research Gaps in Studies related to Total Quality Management on Competitive Advantage in Malaysian Hotel Industries. *International Journal of Academic Research in Business and Social Sciences*, 9(5). <https://doi.org/10.6007/ijarbss/v9-i5/5875>
- Supradono, B. (2009). Manajemen Risiko Keamanan Informasi dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation). *Media Elektrika*, 2(1), 4–8.
- Supristiowadi, E., & Sucahyo, Y. G. (2018). Manajemen Risiko Keamanan Informasi pada Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI) Kementerian Keuangan. *Indonesian Treasury Review Jurnal Perbendaharaan Keuangan Negara Dan Kebijakan Publik*, 3(1), 23–33. <https://doi.org/10.33105/itrev.v3i1.20>
- Susanto, E., Legowo, N., & Ady Prabowo, B. (2023). Assessing Information Security Risks in Clinical Laboratory in Accordance With ISO/IEC 27001 Standard. *Journal of Indonesian Applied Economics*, 11(2), 206–216. <https://doi.org/10.21776/ub.jiae.2023.011.02.8>
- Syahindra, I. P. S., Hetty Primasari, C., & Bagas Pradipta Iriantor, A. (2022). Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi Xyz Menggunakan Indeks Kami Dan Iso 27005 : 2011. *Jurnal Teknoinfo*, 16(2), 165. <https://doi.org/10.33365/jti.v16i2.1246>
- Tanjung, D. F., Dwi Nurhayati, O., & Wibowo, A. (2024). Design Information Security in Electronic-

- Based Government Systems Using NIST CSF 2.0, ISO/IEC 27001: 2022 and CIS Control. *International Journal of Innovative Science and Research Technology (IJISRT)*, 523–530. <https://doi.org/10.38124/ijisrt/ijisrt24jun1212>
- Tintin, R., & Hidalgo, M. (2023). Could an ISMS Model (ISO/IEC 27001:2013 Standard) Implementation Really Protect Public Data? *2023 9th International Conference on EDemocracy and EGovernment, ICEDEG 2023*. <https://doi.org/10.1109/ICEDEG58167.2023.10122109>
- Vinet, L., & Zhedanov, A. (2011a). A “missing” family of classical orthogonal polynomials. *Journal of Physics A: Mathematical and Theoretical*, 44(8), 1–14. <https://doi.org/10.1088/1751-8113/44/8/085201>
- Vinet, L., & Zhedanov, A. (2011b). A “missing” family of classical orthogonal polynomials. *Journal of Physics A: Mathematical and Theoretical*, 44(8), 2582–2595. <https://doi.org/10.1088/1751-8113/44/8/085201>
- Wicaksono, A. C., Prabowo, S., & Oktaria, D. (2022). Risk and Security Measurement Based on ISO 27001 Using FMEA Methodology Case Study: National Government Agency. *2022 1st International Conference on Software Engineering and Information Technology, ICoSEIT 2022*, 6–11. <https://doi.org/10.1109/ICoSEIT55604.2022.10029988>
- Wiemas N. G., K., & Suroso, J. S. (2024). Analysis of Risk Management Information System Applications Using Iso/Iec 27001:2022. *Syntax Literate ; Jurnal Ilmiah Indonesia*, 7(11), 18372–18391. <https://doi.org/10.36418/syntax-literate.v7i11.15426>
- Wijaya, F., & Senen, S. H. (2024). Strategic Human Resource Management in Social Enterprises : A Systematic Review of Practices and Challenges. *Journal of Social Entrepreneurship Theory and Practice (JSETP)*, 3(2). <https://doi.org/https://doi.org/10.31098/jsetp.v3i2.2821>
- Wijaya, F., Waspada, I., & Sari, M. (2024). A Systematic Literature Review of Investment Strategies in Perfect Capital Markets : Insights from the PRISMA Framework. *International Journal of Entrepreneurship and Sustainability Studies (IJEASS)*, 4(2). <https://doi.org/https://doi.org/10.31098/ijeass.v4i2.2813>
- Wijayanto, A., Utami, E., & Prasetyo, A. B. (2020). Analysis of Vulnerability Webserver Office Management of Information and Documentation Diskominfo using OWASP Scanner. *2020 2nd International Conference on Cybernetics and Intelligent System, ICORIS 2020*. <https://doi.org/10.1109/ICORIS50180.2020.9320833>

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/4.0/>)

