Journal of Emerging Information Systems and Business Intelligence
ISSN: 2774-3993
Journal homepage: https://ejournal.unesa.ac.id/index.php/JEISBI/

Information Security Risk Assessment Using ISO/IEC 27005:2018 in Internet Service Provider Company

Muhammad Atho'ullah Aziman[1], Ghea Sekar Palupi[2]
[1,2]*Universitas Negeri Surabaya, Surabaya, Indonesia*
muhammadathoullah.21039@mhs.unesa.ac.id, *gheapalupi@unesa.ac.id*

ABSTRACT

Information security is a critical concern for Internet Service Provider companies due to their high dependency on information systems and customer data. PT XYZ has not yet conducted a formal information security risk analysis, despite its plan to prepare for ISO/IEC 27001 certification. This study aims to assess information security risks at PT XYZ using the ISO/IEC 27005:2018 framework and to formulate appropriate risk mitigation recommendations. This research adopts a qualitative descriptive approach with a case study method. Data were collected through literature studies, interviews, and direct observations of information assets, business processes, and existing security controls at PT XYZ. The risk analysis process includes context establishment, identification of critical assets based on confidentiality, integrity, and availability principles, identification of threats and vulnerabilities, risk analysis using likelihood and impact parameters, risk evaluation, and the development of risk treatment plans. The results indicate that out of 27 identified information assets, 24 assets are classified as critical. Several identified risks are categorized as high and very high, which may significantly affect the continuity of the company's core services, including internet connectivity, web hosting, and Domain Name System services. Based on these findings, risk mitigation recommendations are proposed with reference to ISO/IEC 27002:2022 security controls. This study is expected to support PT XYZ in strengthening its information security posture and to serve as an initial step toward achieving ISO/IEC 27001 certification.

Keyword: Information Security, Information System, Internet Service Provider, ISO/IEC 27001, ISO/IEC 27005:2018, Risk Management.

Article Info:
Article history:
Received December 16, 2025
Revised January 23, 2026
Accepted February 19, 2026

Corresponding Author
Muhammad Atho'ullah Aziman
Universitas Negeri Surabaya, Surabaya, Indonesia
muhammadathoullah.21039@mhs.unesa.ac.id

1. INTRODUCTION

In the rapidly evolving digital era, information security has become a fundamental element for maintaining organizational operational continuity and institutional reputation. This condition is particularly critical for information technology service providers such as *Internet Service Providers* (ISPs), which operate complex network infrastructures and manage large volumes of sensitive customer data [1]. As digital gatekeepers, ISPs are responsible for monitoring network traffic, ensuring service availability, and protecting users from cyber threats, including *Distributed Denial of Service* (DDoS) attacks and email spoofing that can severely disrupt essential services [2].

Despite the growing importance of information security, many organizations still experience difficulties in implementing comprehensive *information security risk management*. Limited understanding of potential risks often results in increased system vulnerabilities, while resource constraints hinder the effective deployment of security controls [3]. These challenges are further amplified in ISP environments, where rapid growth in bandwidth usage and service demand can elevate exposure to network failures and security incidents if not accompanied by proportional risk management measures [4]. Consequently, inadequate risk governance may threaten service continuity, regulatory compliance, and customer trust.

Several studies have emphasized the importance of standardized frameworks in managing information security risks. Research on the adoption of *ISO/IEC 27001* highlights its effectiveness in establishing structured *information security management systems* across various sectors [5]. Further analysis of ISO/IEC 27001 implementation demonstrates that systematic risk identification and control selection are essential to align security practices with organizational objectives [6]. In addition, recent studies indicate that integrating international security standards with national data protection regulations can enhance organizational compliance and resilience against cyber threats [7].

To address these challenges, this study adopts the *ISO/IEC 27005:2018* framework as a structured approach for information security risk management. The framework provides systematic stages, including context establishment, asset identification, threat and vulnerability analysis, risk evaluation, and risk treatment planning [8]. This approach enables organizations to assess risks based on the *Confidentiality, Integrity, and Availability* (CIA) Triad, ensuring that critical information assets are prioritized according to their potential impact on business operations [9]. The flexibility of *ISO/IEC 27005* allows it to be effectively applied in ISP environments, particularly for critical services such as internet connectivity, cloud infrastructure, and *Domain Name System* (DNS) operations [10].

This research contributes by applying a comprehensive *information security risk management* assessment using *ISO/IEC 27005:2018* within an ISP context that has not previously implemented formal risk analysis. Unlike prior studies that focus primarily on general security control adoption, this study emphasizes asset criticality assessment and risk prioritization tailored to core ISP services. The findings are expected to provide practical recommendations that support *ISO/IEC 27001* certification readiness while offering a replicable model for other ISPs seeking to strengthen sustainable information security governance.

2. METHODS

This study employs a qualitative descriptive research design with a case study approach, focusing on information security risk management at PT XYZ as an *Internet Service Provider* (ISP). The case study approach enables an in-depth understanding of real organizational conditions and provides contextual insights into information security risks arising from daily operational activities [11]. The scope of this research is limited to critical information assets that support PT XYZ's core services, namely internet connectivity, web hosting, and *Domain Name System* (DNS). This limitation ensures that the risk analysis concentrates on assets with a direct impact on service continuity and customer trust [12].

Data collection was conducted through literature review, semi-structured interviews, and direct observation. The literature review was carried out to establish a theoretical foundation related to information security risk management and the application of international standards [13]. Semi-structured interviews involved IT management and technical personnel to identify information assets, threats, vulnerabilities, and existing security controls within PT XYZ. Direct

observation was used to validate interview findings and to ensure consistency between documented controls and actual security practices in the operational environment.

Data analysis followed the ISO/IEC 27005:2018 risk management framework, which consists of context establishment, asset identification, threat and vulnerability identification, risk analysis, risk evaluation, and risk treatment planning. Asset identification was performed using the CIA Triad approach Confidentiality, Integrity, and Availability to systematically assess asset criticality [14]. This structured and iterative methodology enables systematic identification and prioritization of information security risks while maintaining alignment with organizational objectives and regulatory requirements. Furthermore, this approach supports continuous improvement in information security management and facilitates organizational readiness for ISO/IEC 27001 certification [15].

3. RESULTS AND DISCUSSION

This section presents the results of the information security risk analysis conducted at PT XYZ using the ISO/IEC 27005:2018 framework. The findings are systematically organized into sub-sections to clearly describe the asset criticality assessment, risk identification and distribution, and the discussion of high-priority risks along with their implications for information security management.

3.1 Asset Identification and Criticality Assessment

Asset identification was conducted through structured interviews and direct observations of PT XYZ's operational environment, focusing on systems supporting core Internet Service Provider (ISP) services, including internet connectivity, web hosting, and Domain Name System (DNS). A total of 30 information technology assets were identified and evaluated using the Confidentiality, Integrity, and Availability (CIA) Triad.

Each asset was scored on a scale of 1–5 for each CIA component, and the average score was used to determine asset criticality. Assets with an average CIA score greater than 3.00 were classified as critical. The assessment results show that 24 assets were categorized as critical, covering six asset categories: hardware, software, data and information, network and infrastructure, human resources, and physical facilities.

The distribution of critical assets across asset categories is summarized in Table 1 and Table 2, which highlights the prioritization of assets based on their CIA evaluation. The results indicate that network and infrastructure assets, as well as data-related assets, exhibit the highest criticality scores. This finding emphasizes their strategic importance in supporting PT XYZ's service continuity and compliance with information security regulations. Disruptions to these assets could directly affect customer services and organizational reputation.

Table 1. Asset Category Code

Asset Code	Asset Category
K1	Hardware
K2	Software
K3	Data and Information
K4	Network and Infrastructure
K5	Human Resources
K6	Physical Facilities

Table 2. Asset Code

Asset Category Code	Asset Code	IT Asset	CIA Triad Score
K1	A1	Border Router	4.3
	A2	Distribution Router	3.3
	A3	Border Switch	4.3
	A4	Distribution Switch	3.3
	A5	Uninterruptible Power Supply (UPS)	4.0
	A6	Security Access Control System	3.3
	A7	Server	4.3
K2	A8	Odoo ERP System	3.7
	A9	cPanel	4.0
	A10	RADIUS Server	4.3
	A11	System Monitoring Application	3.3
K3	A12	Customer Data	4.3
	A13	Financial Data	4.0
	A14	Corporate Email	4.3
K4	A15	Global Internet Connectivity	4.3
	A16	Wireless Network	4.3
	A17	Fiber Optic Network	4.3
K5	A18	System Administrator	3.3
	A19	Host Master	3.3
	A20	Field Engineer	3.3
	A21	Network Engineer	3.3
	A22	Technical Support	3.7
K6	A23	Head Office	4.0
	A24	Network Operation Center (NOC)	5.0

3.2 Risk Identification and Risk Evaluation

Following the identification of critical assets, a comprehensive risk analysis was conducted by identifying potential threats and vulnerabilities associated with each asset. Risk values were calculated by multiplying likelihood and impact scores in accordance with the ISO/IEC 27005:2018 methodology.

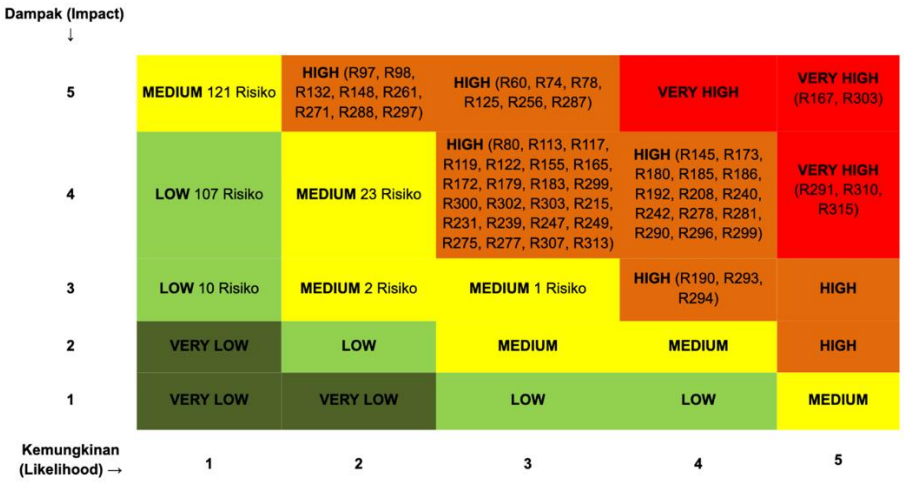

Figure 1. Information Security Risk Matrix of PT XYZ

The analysis resulted in the identification of 318 information security risks. The distribution of risk levels indicates that 5 risks (1.6%) fall into the *very high* category, 48 risks (15.0%) into *high*, 147 risks (45.4%) into *medium*, and 118 risks (38.0%) into *low*. Although the majority of risks are categorized as medium and low, the presence of high and very high risks demonstrates

the existence of significant vulnerabilities that require immediate management attention. The overall risk profile of PT XYZ is visualized in Figure 1, which presents the risk matrix illustrating the relationship between likelihood and impact.

The concentration of risks within the medium to high likelihood and impact ranges highlights potential threats to business continuity, particularly in relation to service availability and data protection. These findings underline the importance of implementing structured and prioritized risk treatment strategies.

Table 3. High and very high risk

Asset Code	Risk Code	Threat	Vulnerability	L	I	Risk
A2	R60	Prolonged Power Outage	Absence of secure shutdown procedures	3	5	15 (High)
A6	R74	Insider Unauthorized Access (Insider Threat)	Lack of access monitoring and auditing	3	5	15 (High)
A6	R78	Forced Entry Attack	Poor quality of physical security hardware	3	5	15 (High)
A6	R80	Tailgating / Piggybacking	Lack of employee security awareness	3	4	12 (High)
A7	R97	Physical Threat	Inadequate disaster protection	2	5	10 (High)
A7	R98	Physical Threat	Use of conventional air conditioning systems	2	5	10 (High)
A8	R113	Bugs or Vulnerabilities in Custom Code	Inadequate testing processes	3	4	12 (High)
A8	R117	Data Input Errors (Human Error)	Non-intuitive user interface	3	4	12 (High)
A8	R119	Data Input Errors (Human Error)	Lack of user training	3	4	12 (High)
A8	R122	Access Rights Misconfiguration	No periodic access review	3	4	12 (High)
A8	R125	Brute Force Attack on Login Page	Two-Factor Authentication (2FA) not implemented	3	5	15 (High)
A9	R132	Security Patching Delay	Manual and unscheduled patching process	2	5	10 (High)
A10	R145	Inadequate Logging	Logs are not centralized	4	4	16 (High)
A11	R148	Monitoring Console Hijacking	Two-Factor Authentication (2FA) not implemented	2	5	10 (High)
A12	R155	Log and Metric Data Manipulation	Data integrity is not guaranteed	3	4	12 (High)
A12	R165	Malware Attack (Ransomware, Spyware)	Inadequate security software	3	4	12 (High)
A12	R167	Human Error & Negligence	Lack of regular security awareness training	5	5	25 (Very High)
A12	R172	System Failure & Disaster	No off-site backup available	3	4	12 (High)
A12	R173	Compliance & Regulatory Violation	Lack of understanding of regulations	4	4	16 (High)

Asset Code	Risk Code	Threat	Vulnerability	L	I	Risk
A13	R179	Human Error in Financial Processes	Overly manual financial processes	3	4	12 (High)
A13	R180	Human Error in Financial Processes	Poor inter-department communication	4	4	16 (High)
A13	R183	Financial Report Manipulation	Lack of independent oversight	3	4	12 (High)
A13	R185	Physical Theft of Financial Documents & Devices	No encryption on finance staff devices	4	4	16 (High)
A13	R186	Physical Theft of Financial Documents & Devices	Lack of regular security awareness training	4	4	16 (High)
A14	R190	Email Account Takeover (ATO)	Multi-Factor Authentication (MFA) not enforced	4	3	12 (High)
A14	R192	Data Leakage via Email	No Data Loss Prevention (DLP) solution	4	4	16 (High)
A15	R208	Signal Jamming / Interference	Use of congested frequency channels	4	4	16 (High)
A15	R215	Rogue Access Point	Lack of user awareness and education	3	4	12 (High)
A17	R231	Physical Tampering or Theft	Unsecured passive infrastructure	3	4	12 (High)
A18	R239	Critical Update Negligence	No centralized patch management	3	4	12 (High)
A18	R240	Critical Update Negligence	Delayed updates by staff	4	4	16 (High)
A18	R242	Critical Update Negligence	Lack of asset and software inventory	4	4	16 (High)
A18	R247	Abuse of Customer Account Access	Overly permissive access policies	3	4	12 (High)
A18	R249	Social Engineering by “Customers”	Lack of regular security training	3	4	12 (High)
A18	R256	Physical Infrastructure Sabotage (Field)	Inadequate physical access supervision	3	5	15 (High)
A18	R261	Theft of Company Property and Materials	No asset tagging implemented	2	5	10 (High)
A21	R271	Firewall & ACL Misconfiguration	Lack of periodic firewall rule audits	2	5	10 (High)
A21	R275	Inadequate Capacity Planning	Poor inter-department communication	3	4	12 (High)
A22	R277	Social Engineering	Lack of regular security awareness training	3	4	12 (High)
A22	R278	Incorrect Information or Diagnosis	Incomplete knowledge base	4	4	16 (High)
A22	R281	Customer Data Handling Errors	Insecure workspace policies	4	4	16 (High)

Asset Code	Risk Code	Threat	Vulnerability	L	I	Risk
A23	R287	Fire	Insufficient fire extinguishing equipment	3	5	15 (High)
A23	R288	Fire	Lack of staff preparedness	2	5	10 (High)
A23	R290	Unauthorized Physical Access	Insecure access points	4	4	16 (High)
A23	R291	Unauthorized Physical Access	Weak visitor supervision procedures	5	4	20 (Very High)
A23	R293	Human Negligence	Lack of clear policies	4	3	12 (High)
A23	R294	Human Negligence	Lack of training and awareness	4	3	12 (High)
A24	R297	Total Power Supply Failure (Total Blackout)	Dependence on building generator	2	5	10 (High)
A24	R303	Fire	Water-based fire suppression system	5	5	25 (Very High)
A24	R307	Water Leakage	No water leakage sensors	3	4	12 (High)
A24	R310	Earthquake	Absence of seismic bracing	5	4	20 (Very High)
A24	R313	Unauthorized Physical Access (Bypassing Controls)	CCTV not actively monitored	3	4	12 (High)
A24	R315	Internal or External Sabotage	Lack of access activity logging	4	5	20 (Very High)

3.3 Risk Treatment Plan

Further analysis reveals that high and very high risks primarily originate from three key areas: physical security weaknesses, human resource factors, and technical control limitations. Physical security risks are mainly associated with inadequate fire protection systems and insufficient access control mechanisms in critical facilities such as the Network Operation Center (NOC). These weaknesses increase the likelihood of asset damage and unauthorized physical access, which could result in service disruption.

Human-related risks are predominantly linked to limited security awareness and the absence of regular information security training programs. Insufficient awareness among employees increases the probability of human error, credential misuse, and social engineering attacks, which are commonly reported as major contributors to security incidents in ISP environments.

In addition, technical vulnerabilities such as the absence of multi-factor authentication (MFA) and the lack of centralized patch management significantly elevate the risk of unauthorized access and system compromise. These conditions indicate that existing security controls at PT XYZ are not yet fully aligned with current best practices in information security risk management.

Based on these findings, a risk treatment plan was developed focusing on 53 risks classified as high and very high. The proposed mitigation measures reference relevant controls from SNI ISO/IEC 27002:2022, providing practical guidance for strengthening organizational, technical, and physical security controls. This approach supports PT XYZ's strategic objective of enhancing its information security posture and serves as an essential preparatory step toward ISO/IEC 27001 certification.

Table 4. Control & Mitigation Recommendations

Risk Code	Recommended Control (ISO/IEC 27002:2022)
R167	6.3 Information security awareness, education, and training
R291	7.2 Physical security perimeter
R303	7.7 Protection against physical and environmental threats
R310	7.7 Protection against physical and environmental threats
R315	7.3 Securing offices, rooms, and facilities
R60	8.9 Configuration management
R74	8.16 Monitoring activities
R78	7.2 Physical security perimeter
R80	6.3 Information security awareness, education, and training
R97	7.7 Protection against physical and environmental threats
R98	7.7 Protection against physical and environmental threats
R113	8.29 Security testing in development and acceptance
R117	8.29 Security testing in development and acceptance
R119	6.3 Information security awareness, education, and training
R122	5.18 Access rights review
R126	8.5 Secure authentication
R133	8.8 Management of technical vulnerabilities
R145	8.15 Logging
R148	8.5 Secure authentication
R155	8.15 Logging
R165	8.7 Protection against malware
R172	8.13 Information backup
R173	5.31 Legal, statutory, regulatory, and contractual requirements
R179	8.10 Information protection
R180	5.22 Monitoring, review, and change management of supplier services
R183	5.25 Independent review of information security
R185	8.10 Information protection
R186	6.3 Information security awareness, education, and training
R190	8.5 Secure authentication
R192	8.12 Data leakage prevention
R208	8.22 Network services security
R215	8.21 Security of network services
R231	7.9 Security of equipment and assets
R239	8.8 Management of technical vulnerabilities
R240	8.8 Management of technical vulnerabilities
R242	5.9 Inventory of information and other associated assets
R247	8.2 Privileged access rights
R249	6.3 Information security awareness, education, and training
R256	7.9 Security of equipment and assets
R261	5.9 Inventory of information and other associated assets
R271	8.9 Configuration management
R275	8.6 Capacity management
R277	6.3 Information security awareness, education, and training
R278	5.9 Inventory of information and other associated assets
R281	7.6 Office and facility security
R287	7.7 Protection against physical and environmental threats
R288	5.24 Information security incident management planning and preparation
R290	7.3 Securing offices, rooms, and facilities
R293	5.1 Policies for information security
R294	6.3 Information security awareness, education, and training
R297	7.11 Supporting utilities
R307	7.7 Protection against physical and environmental threats
R313	7.4 Physical security monitoring

CONCLUSION

This study has successfully addressed the formulated research questions by systematically analyzing information security risks at PT XYZ using the ISO/IEC 27005:2018 framework. The research findings demonstrate that the asset identification process identified 24 critical information technology assets supporting PT XYZ's core services, classified into six categories: hardware, software, data and information, network and infrastructure, human resources, and physical facilities. Risk analysis results revealed a total of 318 identified information security risks, with 5 risks (1.6%) fall into the *very high* category, 48 risks (15.0%) into *high*, 147 risks (45.4%) into *medium*, and 118 risks (38.0%) into *low*, indicating that a significant portion of risks requires managerial attention and structured mitigation. The results further show that the most significant contributors to high and very high risks originate from physical security weaknesses, insufficient security awareness and training among human resources, and the absence of essential technical controls, such as multi-factor authentication and centralized patch management. Based on these findings, this research proposes a risk treatment plan focusing on 53 high and very high risks, providing mitigation recommendations aligned with SNI ISO/IEC 27002:2022 controls. Theoretically, this study contributes to the body of knowledge on information security risk management by demonstrating the applicability of ISO/IEC 27005:2018 in the ISP sector and by integrating risk assessment results with updated security control standards. Practically, the findings offer PT XYZ a structured reference for strengthening its information security posture and supporting preparation for ISO/IEC 27001 certification. Future research may extend this study by incorporating quantitative risk valuation, comparative analysis with other risk management frameworks, or longitudinal assessments to evaluate the effectiveness of implemented controls over time.

ACKNOWLEDGEMENTS

The author is deeply grateful to PT XYZ for granting permission, providing access to data and facilities, and supporting this research, as well as to the management and IT staff for their cooperation during interviews and observations. Furthermore, appreciation is extended to colleagues and peers for their discussions and motivation, and to family members for their continuous moral support throughout the completion of this study.

REFERENCES

[1] CyberDB, *"The Essential Role of ISPs in Cybersecurity,"* CyberDB, 2024.

[2] M. Ghasabi and M. Deypir, "Using optimized statistical distances to confront distributed denial of service attacks in software defined networks," *Intelligent Data Analysis*, vol. 25, no. 1, pp. 155–176, 2021, doi: 10.3233/IDA-194796.

[3] Hoshmand and Ratnawati, *"Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity,"* in Proc. AICOMS, 2023.

[4] S. A. Arnomo and Y. Yulia, "Clustering the potential bandwidth upgrade of FTTH broadband subscribers," *ILKOM Jurnal Ilmiah*, vol. 13, no. 1, pp. 51–57, 2021, doi: 10.33096/ilkom.v13i1.805.51-57.

[5] M. Mirtsch, J. Kinne, and K. Blind, "Exploring the adoption of the international information security management system standard ISO/IEC 27001: A web mining-based analysis," *IEEE Transactions on Engineering Management*, vol. 68, no. 1, pp. 87–100, 2021, doi: 10.1109/TEM.2020.2977815.

[6] C. Sunitha and R. Ranjana, "Analysis of ISO/IEC 27001:2013 Information security management system in an organization," *International Journal of Research Publication and*

Reviews, vol. 4, no. 10, pp. 3316–3329, 2023, doi: 10.55248/gengpi.4.1023.102841.

[7] A. A. Nugraha and A. H. Nasyuha, "Integrating ISO 27001 and Indonesia's personal data protection law for data protection requirement model," *Journal of Information Systems and Informatics*, vol. 6, no. 2, pp. 1052–1069, 2024, doi: 10.51519/journalisi.v6i2.754.

[8] B. Bonnie, *"The ISO 27005 Approach to Information Security Risk Management,"* Secureframe, 2021.

[9] Isnaini *et al.*, *"Analisis Risiko Keamanan Informasi Menggunakan ISO 27005:2019 pada Aplikasi Sistem Pelayanan Desa,"* Jurnal Eksplora Informatika, 2023.

[10] Mastan, *"Seputar Kelompok ISO 27000 — Information Security Management System (ISMS),"* Masyarakat Standarisasi Indonesia, 2022.

[11] D. Fatih and R. F. Aji, *"Evaluasi keamanan informasi menggunakan ISO/IEC 27001: Studi kasus PT XYZ,"* J-Sakti (Jurnal Sains Komputer dan Informatika), vol. 8, no. 1, p. 72, 2024, doi: 10.30645/j-sakti.v8i1.767.

[12] A. Leasa and R. Pressida, *"Manajemen Risiko pada Sistem Informasi Akademik Universitas XYZ menggunakan ISO 27005:2018,"* JTEKSIS, 2024.

[13] S. Meitarice, L. Febyana, A. Fitriansyah, R. Kurniawan, and R. A. Nugroho, *"Risk management analysis of information security in an academic information system at a public university in Indonesia: Implementation of ISO/IEC 27005:2018 and ISO/IEC 27001:2013 security controls,"* Journal of Information Technology and Cyber Security, vol. 2, no. 2, pp. 58–75, 2024, doi: 10.30996/jitcs.12099.

[14] R. M. Rasyid and R. F. Aji, *"Perancangan manajemen risiko keamanan informasi menggunakan SNI ISO/IEC 27005: Studi kasus Integrated School Management System milik PT XYZ,"* JURASIK (Jurnal Riset Sistem Informasi dan Teknik Informatika), vol. 10, no. 1, p. 226, 2025, doi: 10.30645/jurasik.v10i1.866.

[15] A. Wahyuningtyas, N. M. I. M. Mandenni, and M. A. Pasirulloh, *"Analisis dan manajemen risiko keamanan aset teknologi informasi menggunakan metode OCTAVE dan FMEA berbasis ISO 27001:2022,"* Neptunus: Jurnal Ilmu Komputer dan Teknologi Informasi, vol. 3, no. 2, pp. 65–76, 2025, doi: 10.61132/neptunus.v3i2.796.