

Risk Management Framework for ISP Network Operations Based on ISO 27005:2022 and FMEA

Jalu Tri Atmaja¹, Ghea Sekar Palupi²

^{1,2}*Universitas Negeri Surabaya, Surabaya, Indonesia*

jalu.22067@mhs.unesa.ac.id, gheapalupi@unesa.ac.id

ABSTRACT

This study designs information security risk management for network operations and monitoring at PT ABC using ISO/IEC 27005:2022 and FMEA. Asset identification was conducted across five categories (hardware, software, data & information, network & infrastructure, and human resources), with each risk assessed for its impact on the CIA triad and analyzed using Severity, Occurrence, and Detection parameters to generate Risk Priority Number (RPN). The findings identified 185 risk scenarios, with 11 priority risks ($RPN \geq 120$) requiring immediate treatment. The two highest risks (RPN 210) relate to IT asset inventory inaccuracies and unauthorized access to inventory data, dominated by the Data & Information category. Treatment recommendations emphasize mitigation through asset management, access control, preventive maintenance, and security awareness, along with risk transfer for DDoS and traffic overload.

Keyword: Risk Management, Information Security, ISO/IEC 27005:2022, FMEA.

Article Info:

Article history:

Received July 09, 2026

Revised August 31, 2026

Accepted September 29, 2026

Corresponding Author

Jalu Tri Atmaja

Universitas Negeri Surabaya, Surabaya, Indonesia

jalu.22067@mhs.unesa.ac.id

1. INTRODUCTION

The rapid expansion of digital activities in Indonesia has significantly increased societal and corporate dependence on internet services. According to a 2025 survey by the Indonesian Internet Service Providers Association (APJII), internet penetration in Indonesia has reached 80.66% of the total population. This massive growth has simultaneously amplified the potential threats and risks associated with information technology implementation [1].

PT ABC, a regional Internet Service Provider (ISP) operating in Bojonegoro, East Java, exemplifies this challenge. As an ISP, the company faces various risks that threaten service continuity and information security, including network infrastructure failures, DDoS attacks, hardware malfunctions, and customer data leakage. However, the company has never formally conducted risk management specifically related to information technology. Consequently, potential risks remain unidentified and undocumented. The involvement of third-party vendors in its business ecosystem further complicates risk management, particularly

regarding supply chain security and system interdependencies. Given these conditions, a systematic and structured risk management approach becomes essential [2] [3].

Based on these problems, this research aims to design an information security risk management framework for network operations and monitoring at a regional ISP in Indonesia using the ISO/IEC 27005:2022 framework integrated with the Failure Mode and Effect Analysis (FMEA) method. The research produces two key outputs: (1) a comprehensive risk assessment document identifying risk scenarios with priority ranking based on Risk Priority Number (RPN); (2) a risk treatment plan with specific control recommendations referencing ISO/IEC 27002:2022 for high-priority risks [4]. The contribution of this research is an integrated risk management model that combines ISO/IEC 27005:2022 guidance with quantitative FMEA assessment, specifically adapted to the operational characteristics of Indonesian ISPs.

The novelty of this research lies in the integration of ISO/IEC 27005:2022 and FMEA specifically applied to ISP network operations and monitoring, with CIA (Confidentiality, Integrity, Availability) assessment applied to each identified risk rather than merely to assets [5]. This approach enables more precise understanding of risk impacts on information security dimensions.

2. METHODS

This study is qualitative research, in which data collection was conducted through structured interviews and direct field observations of the research object [6] [7] [8]. The framework used as a reference for the implementation of this research is ISO/IEC 27005:2022 on information security risk management, which is combined with the FMEA method to translate the collected data into a quantitative risk assessment matrix. ISO/IEC 27005:2022 provides comprehensive guidance for managing information security risks, covering context establishment, risk identification, risk analysis, risk evaluation, risk treatment, and monitoring and review [9]. Failure Mode and Effect Analysis is a method used to identify potential failure modes, analyze their causes and consequences, and prioritize corrective actions through a scorecard-based assessment [10]. This study employs the following methodology:

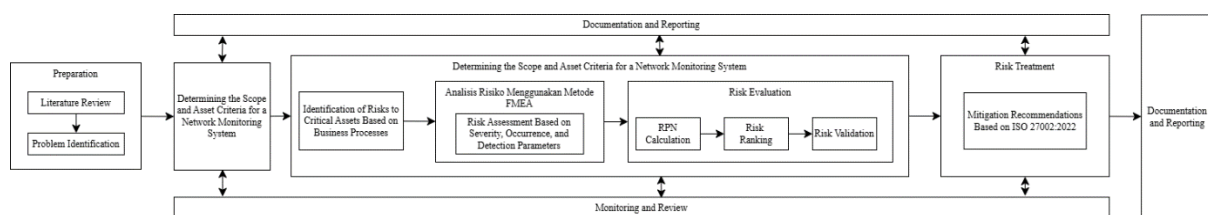


Figure 1. Flow of Research Methodology Using ISO 27005:2022 Integrated FMEA [5]

The integration of ISO/IEC 27005:2022 with FMEA offers a complementary approach: ISO 27005 defines the systematic process framework for risk management, while FMEA provides the quantitative technique for assessing each risk using three parameters; Severity (S), Occurrence (O), and Detection (D) to generate the Risk Priority Number (RPN). A key innovation in this integration is the application of CIA (*Confidentiality, Integrity, Availability*) assessment to each individual risk, rather than to assets alone, which ensures that the Severity score in FMEA accurately reflects the risk's specific impact on information security dimensions [10].

2.1 Asset and Risk Identification

Asset identification was performed using a systematic categorization framework adapted from the six-component information system model, comprising five categories relevant to the ISP operational context: hardware; software and supporting tools; data and information; network and infrastructure; and human resources [11]. Each asset was documented with its owner, operational function, and interdependencies with other assets.

Following asset identification, risk scenarios were developed by analyzing potential failure modes for each asset. For every failure mode, potential causes and their resulting impacts on business processes were identified. A single failure mode could have multiple potential causes, and each cause was treated as a distinct risk scenario to enable granular analysis [12]. This approach follows the ISO/IEC 27005:2022 requirement to identify risk sources, events, and their consequences systematically.

2.2 CIA-Based Impact Assessment

Each identified risk was evaluated for its potential impact on the three fundamental information security dimensions known as the CIA triad: Confidentiality (C), Integrity (I), and Availability (A). Rather than assessing CIA at the asset level, this research assesses how each specific risk impacts each dimension of the CIA triad. This approach enables more precise understanding of risk characteristics, as different risks affect information security dimensions differently. The assessment was conducted using a 1–3 ordinal scale adapted from Lai & Chin [5]: (1) low impact, indicating minor operational inconvenience with no significant business consequences; (2) moderate impact, indicating minor disruption to business activities without legal implications; and (3) high impact, indicating serious disruption to business continuity with potential legal consequences.

2.3 Risk Analysis Using FMEA

Risk analysis was conducted using the Failure Mode and Effect Analysis (FMEA) method, a proactive technique for identifying potential failure modes and prioritizing corrective actions through a scorecard-based assessment. Each risk scenario was evaluated using three parameters measured on a 1–10 scale [5]: (1) Severity (S) the magnitude of impact on business operations if the risk materializes, anchored to the CIA assessment; (2) Occurrence (O) the estimated frequency or probability of the risk occurring; and (3) Detection (D) the capability of existing controls to detect the risk before its impact manifests. The Risk Priority Number (RPN) was calculated using the formula $RPN = S \times O \times D$. Based on the calculated RPN values, risks were evaluated against established acceptance criteria: risks with $RPN \leq 50$ were considered acceptable; risks with $RPN 51–119$ required review and monitoring; and risks with $RPN \geq 120$ were designated as high-priority risks requiring immediate treatment [12].

3. RESULTS AND DISCUSSION

This section presents the result of information security risk analysis conducted PT ABC using ISO/IEC 27005:2022.

3.1 Critical Asset Identification

Based on the asset identification process, a total of 23 information technology assets were identified and categorized into five groups: hardware (6 assets), software and supporting tools (4 assets), data and information (6 assets), network and infrastructure (4 assets), and human resources (3 assets). From these assets, 185 risk scenarios were generated by analyzing potential failure modes, their causes, and their impacts on business processes. Table 1 presents the distribution of risks by asset category.

Table 1. Distribution of Risk by Asset Category

Asset Category	Number of Assets	Number of Risk
Hardware	6	50
Software & Support Tools	4	35
Data & Information	6	44
Network & Infrastructure	4	39
Human Resources	3	17
Total	23	185

The risk class (A, B, C) is determined based on the magnitude of the risk's potential effect on business processes [5]. Risks with critical impacts that could cause significant losses or complete service shutdown are classified as Class A. Risks with moderate impacts that could cause minor operational disruptions are classified as Class B. Risks with low impacts that result in inconvenience without affecting core functions are classified as Class C. The following is the data that was successfully identified

Table 2. Risk Classes Based on Business Impact

Risk Class	Business Impact Criteria	Number of Risk
Class A	Significant losses or complete service shutdown	127
Class B	Minor operational disruptions	24
Class C	Inconvenience, no core function disruption	34
Total		185

3.2 FMEA Analysis and Risk Priority Ranking

Using the FMEA method, each of the 185 risks was evaluated using three parameters: Severity (S), Occurrence (O), and Detection (D), measured on a 1–10 scale. Severity scores were anchored to the CIA-based risk classification: Class A risks received high Severity scores (8–10), Class B risks received moderate Severity scores (4–7), and Class C risks received low Severity scores (1–3). The Risk Priority Number (RPN) was calculated as $RPN = S \times O \times D$. Based on the established risk acceptance criteria ($RPN \leq 50$ = acceptable, RPN 51–119 = requires review, $RPN \geq 120$ = high priority), 11 risks were identified as high-priority requiring immediate treatment. Table 3 presents the ranking of these 11 priority risks.

Table 3. Risk Priority Ranking

Risk Code	Asset Category	Risk Description	C	I	A	Class	S	O	D	RPN	Strategy
R-144	Data & Information	IT asset inventory inaccuracies due to unintegrated recording system	1	3	1	B	6	7	5	210	Mitigate
R-145	Data & Information	Unauthorized access to IT asset inventory data	2	3	1	C	6	7	5	210	Mitigate

		containing critical infrastructure information									
R-092	Software & Tools	Website inaccessibility due to DDoS attacks exceeding protection capacity	2	2	3	B	9	6	3	162	Transfer
R-059	Hardware	Malware infection on PC Desktops due to low cybersecurity awareness	3	2	1	A	8	4	5	160	Mitigate
R-068	Software & Tools	Operating system failure due to unaddressed full disk capacity	2	3	3	A	8	5	4	160	Mitigate
R-093	Software & Tools	Server overload due to unapplied rate limiting on API endpoints	2	2	3	B	8	6	3	144	Transfer
R-141	Data & Information	IT asset inventory inaccuracies due to manual recording susceptible to errors	1	3	1	B	6	7	3	126	Mitigate
R-054	Hardware	PC Desktop hardware damage due to absence of predictive inspections	2	1	2	C	6	4	5	120	Mitigate
R-055	Hardware	PC Desktop hardware damage due to operational age exceeding limit	2	1	2	C	6	4	5	120	Mitigate
R-125	Data & Information	Loss of financial	3	3	1	A	8	5	3	120	Mitigate

		transaction historical data due to automated deletion without adequate notification									
R-146	Data & Information	Unauthorized access to IT asset data due to unenforced access policies	2	3	1	C	6	4	5	120	Mitigate

3.3 Risk Treatment Recommendations

Risk treatment recommendations for the eleven priority risks are dominated by mitigation strategies (9 out of 11 risks), including strengthening asset management through the integration of inventory tracking systems, implementing policy-based access controls on asset data files, strengthening retention policies and backups for financial transaction data, raising information security awareness among staff, and proactively scheduling hardware maintenance and replacement [2] [13] [14] [15]. For the two risks related to website service availability (R-092 and R-093), the recommended strategy is risk transfer through third-party DDoS protection services and a Content Delivery Network (CDN). All of these recommendations refer to the security controls in ISO/IEC 27002:2022, specifically in the domains of asset management, access control, operational security, and communication security.

CONCLUSION

This study successfully designed an information security risk management framework for a regional Indonesian ISP using ISO/IEC 27005:2022 and FMEA. From 23 identified assets, 185 risk scenarios were generated, with 11 priority risks ($RPN \geq 120$) requiring immediate treatment. The two highest risks ($RPN 210$) relate to IT asset inventory inaccuracies (R-144) and unauthorized access to inventory data (R-145), with the Data & Information category dominating 6 out of 11 priority risks. The theoretical contribution is the application of CIA assessment to each individual risk, enabling more precise impact analysis. Treatment recommendations emphasize mitigation strategies for procedural and managerial risks, and transfer strategies for DDoS and traffic overload risks. Further research is suggested to evaluate the effectiveness of implementing the risk treatment recommendations and to conduct periodic risk monitoring and reviews in accordance with the monitoring and review clauses of ISO/IEC 27005:2022.

ACKNOWLEDGEMENTS

The authors would like to express their sincere gratitude to PT ABC for its cooperation, data provision, and operational insights during this research. Appreciation is also extended to the Department of Information Systems, Faculty of Engineering, State University of Surabaya, for facilitating this research. The authors also thank the supervisor for her invaluable guidance, feedback, and support throughout the research process.

REFERENCES

- [1] APJII, “Highlight Survei Penetrasi Internet dan Segmentasi Pasar ISP APJII 2025,” 2025. [Daring]. Tersedia pada: <https://survei.apjii.or.id/survei>
- [2] I. M. M. Putra dan K. Mutijarsa, “Designing Information Security Risk Management on Bali Regional Police Command Center Based on ISO 27005,” dalam *2021 3rd East Indonesia Conference on Computer and Information Technology (EIconCIT)*, Surabaya, Indonesia: IEEE, Apr 2021, hlm. 14–19. doi: 10.1109/EIconCIT50028.2021.9431865.
- [3] A. S. Abbas dan S. A. Hameed Alazawi, “Network risk assessment in banking security based on ISO/IEC 27005,” dipresentasikan pada 6TH INTERNATIONAL CONFERENCE FOR PHYSICS AND ADVANCE COMPUTATION SCIENCES: ICPAS2024, Baghdad, Iraq, 2025, hlm. 030003. doi: 10.1063/5.0265276.
- [4] M. A. Aziman dan G. S. Palupi, “Information Security Risk Assessment Using ISO/IEC 27005:2018 in Internet Service Provider Company”.
- [5] M. H. Putri dan G. S. Palupi, “Information Technology Asset Risk Management for XYZ Digital Wallet Application with ISO 3100:2018 and FMEA,” 2025.
- [6] F. Kitsios, E. Chatzidimitriou, dan M. Kamariotou, “Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry,” *Sustainability*, vol. 14, no. 3, hlm. 1269, Jan 2022, doi: 10.3390/su14031269.
- [7] R. Maulana dan F. Mahardika, “ANALISIS RISIKO KEAMANAN PADA SISTEM E-LEARNING BERDASARKAN ISO 27005,” *J. Inform.*, vol. 2, no. 1, 2025.
- [8] A. Syaputra, “Penilaian IT Governance dalam Manajemen Risiko IT Menggunakan Metode Quantitative dan Qualitative Risk Analysis,” *J. Manaj. Inform. JAMIKA*, vol. 12, no. 1, hlm. 63–73, Apr 2022, doi: 10.34010/jamika.v12i1.6743.
- [9] “Information security, cybersecurity and privacy protection — Guidance on managing information security risks.” International Organization for Standardization, 2022.
- [10] A. C. Wicaksono, S. Prabowo, dan D. Oktaria, “Risk and Security Measurement Based on ISO 27001 Using FMEA Methodology Case Study: National Government Agency,” dalam *2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT)*, Bandung, Indonesia: IEEE, Nov 2022, hlm. 6–11. doi: 10.1109/ICoSEIT55604.2022.10029988.
- [11] D. E. R. Hidayatullah, R. Kunthi, dan R. Harwahyu, “Design and Analysis of Information Security Risk Management Based on ISO 27005: Case Study on Audit Management System (AMS) XYZ Internal Audit Department,” *Int. J. Electr. Comput. Biomed. Eng.*, vol. 2, no. 3, Sep 2024, doi: 10.62146/ijecbe.v2i3.81.

- [12] Bintang Rahmat Riadi, “Risk Management of Information Security in Inaportnet Using ISO/IEC 27005:2018,” *INOVTEK Polbeng - Seri Inform.*, vol. 10, no. 1, hlm. 225–236, Mar 2025, doi: 10.35314/pq4jhh89.
- [13] I. P. S. Syahindra, C. Hetty Primasari, dan A. Bagus Pradipta Iriantor, “EVALUASI RISIKO KEAMANAN INFORMASI DISKOMINFO PROVINSI XYZ MENGGUNAKAN INDEKS KAMI DAN ISO 27005 : 2011,” *J. Teknoinfo*, vol. 16, no. 2, hlm. 165, Jul 2022, doi: 10.33365/jti.v16i2.1246.
- [14] E. H. N. Safitri dan H. Kabetta, “Cyber-Risk Management Planning Using NIST CSF V1.1, ISO/IEC 27005:2018, and NIST SP 800-53 Revision 5 (A Study Case to ABC Organization),” dalam *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, Bogor, Indonesia: IEEE, Agu 2023, hlm. 332–338. doi: 10.1109/ICoCICs58778.2023.10277652.
- [15] N. K. D. Astini, Gusti Agung Ayu Putri, dan Dwi Putra Githa, “Information Technology Risk Analysis Using ISO 27005:2022 At Diskominfo Tabanan Regency,” *J. Ris. Inform.*, vol. 7, no. 4, hlm. 307–316, Sep 2025, doi: 10.34288/jri.v7i4.394.