



Information Security Risk Management Using ISO/IEC 27005 to Ensure the Continuity of Academic Services at UPN “Veteran” Yogyakarta

Juwairiah^{1*}, Herry Sofyan², Hari Prapcoyo³, Rivan Adi Pardana⁴,
Nauval Ghaina Mochamad Hanif⁵, Brigitta Chrishyandra⁶, Siti Fatimahtul Ughro⁷

^{1,2,3,4,5,6,7} Information Systems Study Program, Faculty of Industrial Engineering,
Universitas Pembangunan Nasional “Veteran” Yogyakarta, Indonesia

Received: September 8, 2026	Revised: September 18, 2026	Accepted: September 22, 2026	Online: October 7, 2026
-----------------------------	-----------------------------	------------------------------	-------------------------

Abstract

UPA TIK of UPN ‘Veteran’ Yogyakarta operates four interdependent academic systems: Bima for academic administration, Spada Wimaya for online learning, Sadewa for student activities and achievements, and Nakula for lecturer services. Service interruptions caused by DDoS traffic, malware, unstable power, and hardware failure motivated a structured risk assessment. This study applies ISO/IEC 27005:2022 to identify, analyze, evaluate, and treat information security risks using asset-based scenarios. Evidence was obtained from document review, interface observation, interviews with the Head of UPA TIK as the risk owner and key informant, and a confirmatory survey of users. The assessment identified 257 risk scenarios: for primary assets, there are 34 in Bima, 37 in Spada Wimaya, 58 in Sadewa, 76 in Nakula, and 52 in supporting assets. Likelihood and consequence were scored on harmonized five-level scales and mapped to a 5 × 5 matrix. Based on the risk assessment results for 257 risk scenarios, 11 are high, 72 are medium, 131 are low, and 32 are very low. Consequently, 83 risks must be prioritized for mitigation using ISO/IEC 27001:2022 Annex A controls. Critical recommendations include capacity management for peak registration, redundant processing facilities and maintained power support, continuous malware protection, stronger upload validation, data classification and encryption, longer log retention, and formal incident ticketing. The principal contribution is an integrated assessment of four systems that share infrastructure and governance, producing one comparable risk register, Statement of Applicability, and implementation-oriented treatment plan. Residual risk will be measured after the recommended controls are implemented.

Keywords *Academic Information Systems; Information Security; ISO/IEC 27005; Risk Assessment; Risk Treatment*

INTRODUCTION

Higher education increasingly depends on interconnected information systems for registration, learning, assessment, and student services. This dependence improves access but also makes academic continuity sensitive to failures in infrastructure, software, security controls, and human processes. Universities are attractive cyber targets because they combine open access, heterogeneous users, valuable personal data, and decentralized technology management (Cheng & Wang, 2022). Information security therefore requires the coordinated protection of confidentiality, integrity, and availability, supported by risk-based governance rather than isolated technical controls (ISO/IEC 27001, 2022).

In Indonesia, Government Regulation No. 71/2019, Ministry of Communication and Informatics Regulation No. 4/2016, and National Cyber and Crypto Agency Regulation No. 4/2021 reinforce electronic-system continuity and security (Ministry of Communication and Informatics of Indonesia, 2016; National Cyber and Crypto Agency of Indonesia, 2021). These instruments strengthen the institutional case for documented risk ownership, security controls, and periodic

Copyright Holder:

© Juwairiah, Herry, Hari, Rivan, Nauval, Brigitta, & Siti. (2026)
Corresponding author’s email: juwairiah@upnyk.ac.id

This Article is Licensed Under:



evaluation.

At UPN 'Veteran' Yogyakarta, UPA TIK manages four complementary systems. Bima supports registration, schedules, grades, and transcripts; Spada Wimaya provides online learning; Sadewa manages student activities and achievements; and Nakula supports lecturer services. The systems share infrastructure and governance, so a disruption in power, networks, servers, or common controls can affect several services. Recorded incidents include DDoS traffic during registration, Bima data loss associated with unstable voltage, malware in an outdated Moodle installation, repeated brute-force attempts, Sadewa interruptions during graduation periods, and Nakula downtime during grade submission.

A prior quality evaluation of an academic information system in the same institutional context also identified areas requiring improvement, but it did not provide an integrated information-security risk register for the four services (Adi et al., 2024). Despite these incidents, UPA TIK had not conducted a standard-based, integrated assessment of the four systems. Earlier studies of academic systems often assessed one application, applied a general enterprise-risk method, or stopped after risk classification without linking scenarios to implementation responsibilities (Leasa & Prassida, 2024; Setyaningrum & Maria, 2024; Sulaeman et al., 2023). This leaves limited guidance for institutions whose systems share assets and risk ownership.

This study addresses three questions: (1) what asset-threat-vulnerability scenarios affect the four systems; (2) which scenarios require treatment under a common likelihood, consequence, and acceptance model; and (3) which ISO/IEC 27001:2022 controls and actions should be prioritized? The study aims to produce a comparable cross-system risk register and treatment plan. Its novelty lies in applying ISO/IEC 27005:2022 simultaneously to four interdependent academic services under one risk owner, while linking scenario assessment to existing controls, a Statement of Applicability (SOA), and a Risk Treatment Action Plan (RTP). The scope is limited to the defined application roles and shared UPA TIK assets; control implementation and post-treatment residual-risk measurement are outside the current study.

LITERATURE REVIEW

ISO/IEC 27005:2022 is an international standard that provides guidance for information security risk management in accordance with the requirements of ISO/IEC 27001 (ISO/IEC 27005, 2022). The risk management process under this standard is cyclical and consists of several main stages as shown in Figure 1.

ISO/IEC 27005:2022 guides organizations in establishing context, identifying and analyzing risk, evaluating risk against acceptance criteria, selecting treatment, communicating with stakeholders, and monitoring outcomes. It supports ISO/IEC 27001 but does not prescribe one scoring formula; organizations must define scales appropriate to their context (ISO/IEC 27005, 2022). This flexibility enables local adaptation, but it may also reduce comparability and introduce expert judgment bias. Semi-quantitative scores should therefore be supported by explicit definitions, traceable evidence, validation by risk owners, and periodic review (Chandra et al., 2022).

Asset-based identification begins with information and business-process assets, then maps relevant threats and vulnerabilities. It was selected here because UPA TIK needed an auditable inventory and scenario register for operational control planning. An event-based approach is useful for strategic or ecosystem-wide scenarios, but it can obscure specific asset ownership and technical dependencies. The asset-based approach is more resource-intensive and can produce many scenarios; consolidation and prioritization are therefore necessary. NIST SP 800-30 similarly emphasizes threat sources, vulnerabilities, likelihood, impact, and uncertainty, supporting the need to document assumptions rather than treat scores as objective measurements (National Institute

of Standards and Technology, 2012).

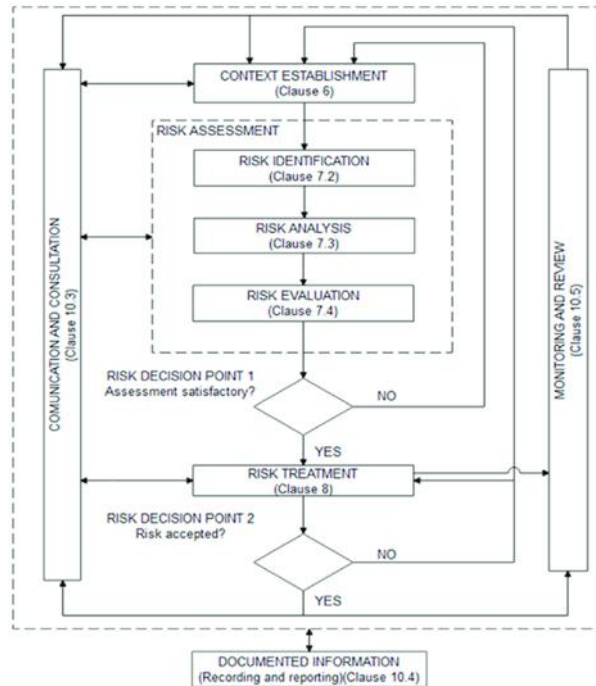
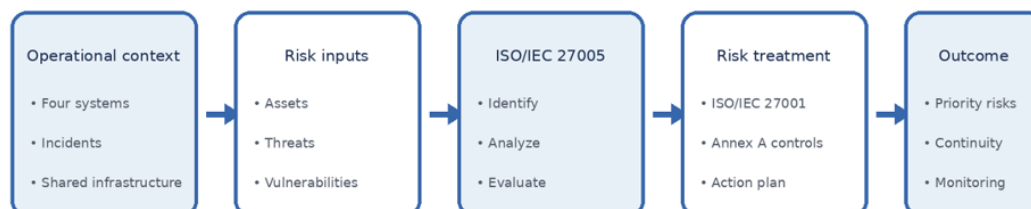


Figure 1. ISO/IEC 27005:2022 Information Security Risk Management Process

Prior studies demonstrate several alternatives. FMEA prioritizes failure modes but is less directly aligned with information-security control catalogs (Tutik et al., 2022; Ramayani, 2022). ISO 31000 offers general risk principles but lacks security-specific guidance (Setyaningrum & Maria, 2024). OCTAVE Allegro focuses on information assets and organizational impact (Astuti et al., 2023), whereas NIST SP 800-30 provides a detailed, threat-oriented assessment (Sulaeman et al., 2023). Recent research also stresses that effective cybersecurity in higher education combines governance, awareness, technical safeguards, and continuity planning (Cheng & Wang, 2022). ISO/IEC 27005:2022 was chosen because it integrates these risk-management activities with ISO/IEC 27001 controls and fits UPA TIK's need for an SOA and RTP.

Conceptual Framework



Communication, consultation, monitoring, and review operate across all stages

Figure 2. Conceptual framework of the study

RESEARCH METHOD

This study applies the information security risk management stages in accordance with ISO/IEC 27005:2022 to the four academic information systems managed by UPA TIK, UPN "Veteran" Yogyakarta, namely Bima, Spada Wimaya, Sadewa, and Nakula. Data were collected through literature study, interviews, direct observation of system interfaces, questionnaires to asset owners, and a study of inventory documents managed by UPA TIK. Context establishment for the four systems was carried out with the same risk owner, namely the Head of UPA TIK, so that the established consequence, likelihood, risk level, and risk acceptance criteria remained consistent, allowing the risk assessment results to be presented in an integrated manner.

Design, Scope, and Participants

A descriptive case-study design was used. The unit of analysis was UPA TIK, and the embedded cases were Bima, Spada Wimaya, Sadewa, and Nakula. Bima and Spada were assessed across the functions observed by the research team; Sadewa was limited to the Student Portal, Academic, Administration, and Student Affairs modules; and Nakula was limited to the Lecturer role. The team assessed shared hardware, software, networks, personnel, and locations once and referenced them across systems.

Participants were selected purposively because risk judgments required operational authority and system knowledge. The Head of UPA TIK served as risk owner and key informant for scope, assets, incidents, likelihood, consequences, existing controls, acceptance criteria, and recommended actions. Nine Sadewa student users completed a short confirmatory questionnaire about data-loss, re-entry, and data-accuracy experiences. The survey triangulated observed and interview findings; its small, non-probability sample was not used to estimate prevalence or test hypotheses.

Data Collection and Instrument Quality

Data were collected through: (1) a structured document review of asset inventories and available operational records; (2) direct observation of menus and functions, documented with screenshots; (3) semi-structured interviews organized around ISO/IEC 27005 context, incident, threat, vulnerability, and control domains; and (4) the Sadewa questionnaire, which contained factual experience items and optional clarification. Instrument content was mapped to ISO/IEC 27005:2022 and reviewed with the risk owner for relevance and terminology. Asset, threat, vulnerability, and scenario lists were cross-checked against observations, documents, and interviews. Because the questionnaire was descriptive and involved nine respondents, psychometric reliability statistics were not appropriate; this is reported as a limitation.

Risk Analysis and Evaluation

Primary assets were extracted from system functions; supporting assets were grouped as hardware, software, network, personnel, and location. Relevant threats and vulnerabilities were drawn from the ISO/IEC 27005 catalog and combined only when a credible pathway existed. Likelihood and consequence were scored from 1 to 5. Likelihood used the higher of historical frequency and estimated annual probability. Consequence used the highest impact across operations, academic processes, recovery effort, and regulatory exposure. The resulting pair was mapped to the matrix in Table 1. Low (L) and Very Low (VL) risks were accepted with monitoring; Medium (M) risks required improvement within 3-12 months; High (H) and Very High (VH) risks required treatment within three months. This harmonized model replaced the inconsistent three- and five-level scales used in earlier working assessments.

Table 1. Likelihood Criteria

Likelihood	Frequency	Probability
Almost Certain (5)	Occurs very frequently (>15 times per year)	Very high probability (>80% in one year)
Very Likely (4)	Occurs frequently (11–15 times per year)	High probability (60–79.9% in one year))
Likely (3)	Occurs quite frequently (6–10 times per year)	Quite high probability (40–59.9% in one year)
Rather Unlikely (2)	Occurs infrequently (2–5 times per year)	Small chance (20–39.9% in one year)
Unlikely (1)	Occurs very rarely (≤ 1 time per year)	Very small chance (<20% in one year)

Table 2. Consequence Criteria

Consequence	Operational	Academic Impact	Recovery Efforts	Regulations
Catastrophic (5)	Downtime >3 consecutive business days; entire service inaccessible	Data permanently lost/corrupted and unrecoverable; process restarted from the beginning.	The entire ICT team was mobilized; external vendors were required, and recovery took more than two working days.	Serious regulatory violation; potential for criminal or civil legal sanctions.
Critical (4)	Downtime of 1–3 business days; all services inaccessible.	Partial data loss/corruption; manual recovery takes >1 business day.	More than one ICT division involved; manual recovery takes 1–2 working days.	Violations of regulations result in formal administrative sanctions.
Serious (3)	Downtime 2 hours–1 business day	Data is not lost but temporarily inaccessible; recovery takes less than one business day.	One ICT division involved; manual technical intervention <1 working day.	A moderate violation results in a formal warning letter.
Significant (2)	Downtime of 15 minutes to 2 hours; service slowed or partially disrupted.	Data is not lost or corrupted; the process resumes immediately after the system recovers.	Handled by one technical staff member; procedural, <1 hour	Minor violations, resolved with a verbal reprimand
Minor (1)	Downtime <15 minutes or insignificant disruption	No impact on data; the process is running normally.	Automatic/self-recovery without technical personnel	No violation

Table 3 presents a 5×5 risk-level matrix that combines likelihood and consequence values

into one of five risk levels, ranging from Very Low (VL) to Very High (VH).

Table 3. Risk-Level Matrix

Likelihood / Consequence	Catastrophic 5	Critical 4	Serious 3	Significant 2	Minor 1
Almost Certain 5	VH	VH	H	H	M
Very Likely 4	VH	H	H	M	L
Likely 3	H	H	M	L	L
Rather Unlikely 2	M	M	L	L	VL
Unlikely 1	L	L	L	VL	VL

Qualitative Analysis, Validity, and Ethics

Interview and observation notes were coded into predefined domains: asset, threat, vulnerability, incident, existing control, control gap, and treatment owner. Evidence from at least two sources was sought for material findings; disagreements were resolved through follow-up clarification with the risk owner. An audit trail linked each scenario to its source and scoring rationale. To protect operational security, the paper reports representative controls and incidents but omits sensitive configurations and exploit details. Participation was voluntary, responses were reported in aggregate, and personally identifying survey data were not included in the analysis

FINDINGS AND DISCUSSION

Assets and Risk Scenarios

The assessment identified 111 primary assets and 30 shared supporting assets. Primary assets included data and business processes for each system, while supporting assets included hardware, software, network, personnel, and location. Mapping relevant assets, threats, and vulnerabilities generated 257 risk scenarios. The counts reflect differences in functional scope and asset granularity and should not be interpreted as direct measures of system insecurity.

Table 4. Aggregated asset and risk-scenario results

System	Assets	Risk scenarios	Share of scenarios
Primary Assets			
- Bima	14	34	13,2%
- Spada Wimaya	29	37	14,4%
- Sadewa	30	58	22,6%
- Nakula	38	76	29,6%
Supporting Assets	30	52	20,2%
Total	141	257	100%

Recurring threat groups included power and telecommunications loss, device or software failure, malware, abuse of access rights, human error, and service-provider failure. Recurrent vulnerabilities included single points of failure, delayed software updates, unnecessary services, limited security testing, unclear responsibility allocation, inadequate service agreements, and

unstable power. These patterns confirm that academic-service continuity depends on organizational and physical controls as well as application security. This aligns with Cheng and Wang's (2022) finding that higher-education cybersecurity requires an institution-wide strategy rather than a technology-only response.

Table 5. Example of Asset-Based Risk Scenarios per System

System	Code	Asset	Threat	Vulnerability	Risk Description
Bima	R-BM031	KRP Data	TT01- Device or System Failure	VN05 – Single Point of Failure; VS17 – Immature/New Software	KRP system failure during peak hours at the beginning of the registration period prevents thousands of students from enrolling in desired courses before capacity is reached
Sadewa	R-SD005	Student Profile and Academic Status Data	TT01- Device or System Failure	VN05- Single Point of Failure;	A single-server failure prevents all students from accessing the activity and achievement portal
Spada Wimaya	R-SW009	Learning Materials Data	TH25- Sending or distributing malware	VS16- Unnecessary services enabled	Document-based learning materials uploaded by lecturers contain malware because files are not scanned automatically during upload
Nakula	R-NK019	Student Final Project Data	Unnecessary services enabled	VS01- No or insufficient software testing, VS02- Well-known flaws in the software	Malware is distributed through malicious documents uploaded via the final-project upload feature, thereby infecting the system

Risk Analysis and Evaluation

Scenario-level likelihood and consequence were evaluated using the harmonized matrix. High-risk examples occurred across all systems: peak-period Bima failure, Sadewa single-server failure, malware in Spada uploads, and malicious Nakula uploads. Medium and Low examples demonstrate that the same matrix also distinguishes less urgent integrity and usability risks. The complete register includes the score and treatment status for every scenario. Table 6 provides the cross-system aggregation, which can be verified from the supplied registers.

Table 6. Representative Risk-Analysis Results

System/code	Risk Scenario	L	C	Level
Bima / R-BM023	KRP failure during peak registration prevents timely course enrollment	2	3	L
Sadewa / R-SD005	Single-server failure makes the student activity portal unavailable	3	5	H
Spada / R-SW005	Uploaded learning material distributes malware	2	3	L
Nakula / R-NK010	Loss of data values due to a backup system failure that went undetected and unreported in a timely manner.	2	4	M
Sadewa / R-SD027	Software defect misrepresents learning-outcome scores	1	3	L

Based on the risk evaluation conducted on 257 risk scenarios, the distribution of the number of risks by risk level is as follows:

Table 7. Summary of System Asset Risk Level Distribution

Assets Category	Risk Level				
	Very Low	Low	Medium	High	Very High
Primary Assets	32	116	45	1	–
Supporting Assets	–	15	27	10	–
Total	32	131	72	11	–

Risk evaluation prioritized Medium, High, and Very High scenarios for modification and retained Low and Very Low scenarios for periodic monitoring. This decision rule is deliberately more conservative than treating medium risk as immediately acceptable because academic deadlines create concentrated service demand. However, residual risk cannot yet be reported as an observed result: the proposed controls have not been fully implemented or tested. Each RTP item therefore specifies a target residual category and requires reassessment after implementation.

Risk Treatment and Existing-Control Gaps

All prioritized risks were assigned risk modification because the academic services could not reasonably be discontinued and contractual risk sharing was not yet available. Controls were selected from ISO/IEC 27001:2022 Annex A after reviewing existing safeguards. The SOA records applicability, justification, current status, and planned action; the RTP assigns an owner and timeframe. Table 8 summarizes the highest-priority lessons.

Existing controls included an Automatic Transfer Switch that changed to generator power in under ten seconds, a Web Application Firewall that blocked detected attacks, daily backups, and redundant cable routes. Important gaps remained: generator maintenance lacked a routine schedule; the UPS provided only about 20 minutes of support; some grade data were stored without encryption; formal data classification was absent; secure-code testing was basic; transaction logs were retained for only seven days; and internet connectivity depended on one provider. These findings show why control presence alone is insufficient: effectiveness, coverage, ownership, and continuity must also be evaluated.

Table 8. Representative treatment priorities and residual-risk verification

Risk Code	Risk Description	Recommended control and action	Verification after implementation
Bima	Peak-load and simultaneous-access failure	A.8.6 Capacity management: load testing, queueing or rate limiting, and peak-period monitoring	Repeat load test; rescore likelihood
Sadewa	Single server and unreliable backup power	A.7.11 Supporting utilities and A.8.14 redundancy: generator maintenance, failover, and recovery test	Failover and power-loss exercise; rescore impact
Spada	Outdated Moodle and unscanned uploads	A.8.7 malware protection and A.8.29 security testing: patch cycle, file validation, continuous scanning	Patch audit and upload test; rescore likelihood
Nakula	Intermittent antivirus and limited upload testing	A.8.7 and A.8.29: year-round protection and deeper pre-release security testing	Control log review and upload test; rescore likelihood

CONCLUSIONS

Applying ISO/IEC 27005:2022 across Bima, Spada Wimaya, Sadewa, and Nakula produced an integrated inventory of 111 primary assets, 30 shared supporting assets, and 257 asset-based scenarios. The harmonized 5×5 matrix provided a consistent basis for prioritization. Representative High risks involved peak-load failure, single points of failure, malware, and insecure file uploads. The treatment plan prioritizes capacity management, redundant processing and maintained utilities, continuous malware protection, stronger security testing, encryption and classification, longer log retention, and structured incident ticketing.

The theoretical contribution is a transparent application of asset-based ISO/IEC 27005 assessment to multiple academic systems with shared infrastructure and one risk owner. The practical contribution is an SOA and RTP that connect scenarios, existing controls, control gaps, responsible parties, implementation timeframes, and post-implementation verification. UPA TIK should first address cross-system dependencies and High or Very High risks, then reassess likelihood and consequence after controls operate for a defined period. Management should review the register at least annually and after major incidents, architectural changes, or regulatory updates.

LIMITATIONS & FURTHER RESEARCH

The study has five limitations. Methodologically, semi-quantitative scoring depends on expert judgment, and one key informant held both operational knowledge and risk-owner authority. The nine-person Sadewa survey was purposive and cannot represent all users. The scope included selected Sadewa modules and the Nakula Lecturer role, so other roles and external dependencies may include additional risks. Data limitations include incomplete historical incident and control-performance records, which constrained probability estimation and prevented statistical validation. ISO/IEC 27005 provides guidance rather than a fixed scoring method, so results depend on locally defined criteria and may not be directly comparable with other institutions. Finally, the assessment is time-bound: threats, assets, usage peaks, and controls change. Control implementation and observed residual-risk levels require longitudinal follow-up.

Future work should independently validate scenario scores with additional asset owners,

administrators, lecturers, and students; expand the scope to all roles and integrations; and maintain a centralized incident and control-evidence repository. After implementing the RTP, the same matrix should be used to measure residual risk and control effectiveness. Further studies could compare asset-based and event-based ISO/IEC 27005 identification, test inter-rater agreement, and examine whether shared-control improvements measurably reduce downtime and data-integrity incidents across the four systems.

REFERENCES

- Adi, N., Laudza, S., & Sofyan, H. (2024). Quality evaluation of academic information systems with ISO/IEC 25010 standards. *Telematika*, 21(2), 158–172. <https://doi.org/10.31515/telematika.v21i2.12406>
- Astuti, R. W., Putra, R. A., & Putra, I. S. (2023). Risk assessment of Academic Information System use using OCTAVE Allegro. *Journal of Computer and Information Systems Ampera*, 4(1), 1–10. <https://doi.org/10.51519/journalcisa.v4i1.337>
- Chandra, N. A., Ramli, K., Ratna, A. A. P., & Gunawan, T. S. (2022). Information security risk assessment using situational awareness frameworks and application tools. *Risks*, 10(8), 165. <https://doi.org/10.3390/risks10080165>
- Cheng, E. C. K., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, 13(4), 192. <https://doi.org/10.3390/info13040192>
- Government of Indonesia. (2003). *Law Number 20 of 2003 on the National Education System*.
- Government of Indonesia. (2019). *Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions*.
- ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. International Organization for Standardization.
- ISO/IEC 27005:2022. (2022). *Information security, cybersecurity and privacy protection—Guidance on managing information security risks*. International Organization for Standardization.
- Leasa, Z. V., & Prassida, G. F. (2024). Risk management of the XYZ University Academic Information System using ISO 27005:2018. *Jurnal Teknologi dan Sistem Informasi Bisnis*, 6(4), 649–656. <https://doi.org/10.47233/jteksis.v6i4.1459>
- Ministry of Communication and Informatics of Indonesia. (2016). *Regulation Number 4 of 2016 on Information Security Management Systems*.
- National Cyber and Crypto Agency of Indonesia. (2021). *Regulation Number 4 of 2021 on Risk Management and Electronic System Security*.
- National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments (NIST SP 800-30 Rev. 1)*. <https://doi.org/10.6028/NIST.SP.800-30r1>
- Ramayani, Y. (2022). Security risk management analysis of the Academic Information System using FMEA. *INOVTEK Polbeng—Seri Informatika*, 7(2), 279–288. <https://doi.org/10.35314/isi.v7i2.2631>
- Setyaningrum, N. N., & Maria, E. (2024). Application of ISO 31000:2018 to risk management in an Integrated School Information System. *JUKANTI*, 7(1), 31–44. <https://doi.org/10.37792/jukanti.v7i1.1164>
- Sulaeman, H., Utomo, H. P., & Suryana, A. I. (2023). Information security risk assessment of an Academic Information System using NIST SP 800-30. *Naratif*, 5(2), 1–10. <https://doi.org/10.53580/naratif.v5i2.254>
- Tutik, T., Mutiah, N., & Rusi, I. (2022). Information security risk analysis and management using FMEA and ISO/IEC 27001 controls. *Coding*, 10(2), 1–12. <https://doi.org/10.26418/coding.v10i02.55082>