JIEM : JOURNAL INFORMATIC, EDUCATION AND MANAGEMENT
Vol 8 No 2 (2026): March - August 2026, pp. 416~424
ISSN: 2716-0696, DOI: 10.61992/jiem.v8i2.383

ISMS GOVERNANCE IMPROVEMENT STRATEGY BASED ON ISO/IEC 27001:2022 IN THE UNIVERSITY INFORMATION TECHNOLOGY UNIT

Siti Kholijah [1*]

[1] Universitas Islam Negeri Jurai Siwo Lampung

Article Info

Article history:
Received May 15, 2026
Revised June 6, 2026
Accepted June 11, 2026

Keywords:
ISMS, ISO/IEC 27001:2022, Higher Education, Information Security Governance, Gap Analysis.

ABSTRACT

This study evaluates the implementation of an ISO/IEC 27001:2022-based Information Security Management System (ISMS) in an information technology unit at a university. The method used is quantitative descriptive with Gap Analysis, through observation, documentation study, and a compliance questionnaire for 93 Annex A controls. The results show that ISMS implementation is at a moderate level with a medium compliance category. Most controls have been implemented according to SOPs (40% with a score of 3), but there are still obstacles in the form of uneven control implementation (16% with a score of 0) and a lack of formal documentation (14% with a score of 1). The effectiveness of ISMS is influenced by management support, documentation standardization, and a culture of information security awareness. This study recommends improving documentation, strengthening internal audits, and preparing for international certification through an ISMS development roadmap to strengthen the university's information security resilience against cyber threats.

Corresponding Author:
Siti Kholijah | Universitas Islam Negeri Jurai Siwo Lampung
Email: siti.kholijah@uinjusila.ac.id

BACKGROUND

In the midst of a massive wave of digital transformation , according to Sholikhatin et al. (2018) universities have evolved into a very complex data -based ecosystem . Hisyam & Rojabi (2025) stated that as an institution that manages volumes of information including personal data of academics , intellectual property research results , to financial assets , the Information Technology (IT) Unit plays a major role as a guarantor of the continuity of operations and the reputation of the institution . Meanwhile, according to Ramadhanty (2024) in line with dependence on digital infrastructure , the risk of cyber threats is also growing to be greater and more organized , which can potentially paralyze educational services at any time .

Hendayun & Zulianto (2019) stated that conventional information security governance , which tends to be reactive, is now considered inadequate in facing the dynamics of modern cyber threats . Therefore , the adoption of international standards has become a strategic urgency for higher education institutions . Damanik et al. (2023) in their previous research stated that ISO/IEC 27001:2022 is present as the latest version that improves the Information Security

Management System (ISMS) framework . Meanwhile, according to Izzani et al. (2026) this standard places a stronger emphasis on security controls that are adaptive to the latest technological trends , such as cloud service risk mitigation and strengthening data privacy protection .

The implementation of ISO/IEC 27001 for IT Units in higher education presents unique challenges , especially in aligning strict technical compliance with an academic culture that upholds information transparency , as stated in Bakri & Irmayana 's (2017) research . Pia Suci Lestari et al. (2025) stated that the inability to manage information risks not only has implications for data leaks , but can also undermine stakeholder trust and lead to legal violations , especially after the ratification of personal data protection regulations at the national level , this is also in line with the opinion of Mustaqillah & Aziz (2025) .

This article aims to examine the strategy for strengthening ISO/IEC 27001 -based ISMS governance in higher education IT units . According to Laily & Siahaan (2023), through gap analysis and mapping of the latest security controls , higher education institutions are expected to build a resilient and adaptive information security foundation . This effort is not merely a matter of compliance , but a crucial step in supporting the academic vision amidst the complexity of global cyber threats , this is in line with the opinion of Goeritno & Hendrawan (2016) .

Unlike previous studies that generally focused on evaluating the level of compliance with ISO/IEC 27001, this study not only conducted a gap analysis based on the 93 controls of Annex A of ISO/IEC 27001:2022, but also identified factors that influence the effectiveness of ISMS implementation in higher education environments and developed a roadmap for improving information security governance that is integrated with the operational needs of the university's Information Technology Unit. Thus, this study provides a practical contribution in the form of implementable recommendations that can be used as a basis for the sustainable development of ISMS.

THEORETICAL STUDY

According to Basuki et al. (2026) , the implementation of an information security management system has become a significant concern due to the increasing cybersecurity threats in various organizational sectors, including higher education institutions. Previous research by Setiawan & Wardhani (2026) shows that information security is not only influenced by the sophistication of the technology used, but also by the governance, policies, and behavior of human resources involved in managing information systems. Therefore, a managerial approach through the implementation of international standards is seen as a strategic solution in controlling information security risks comprehensively , this is in line with the opinion of Suprayitno (2026) .

Research by Siregar & Mardiah (2025) states that the implementation of ISO/IEC 27001:2022 in the Information Technology Unit of higher education aims to improve information security governance systematically and sustainably. Information security does not only focus on technical aspects, but also includes organizational management in protecting important assets and data. Meanwhile, according to Izzani et al. (2026) ISO/IEC 27001:2022 is an international standard that provides an ISMS framework with a simpler and more targeted control structure through four main categories, namely organizational, people, physical, and technological, so

that information security implementation can be tailored to organizational needs more effectively.

According to Rahman et al. (2024) ISO 27001: 2022 is an update of the previous version that adapts to modern information security needs. In this version, Annex A consists of 93 controls grouped into four main categories : Organizational Controls , People Controls , Physical Controls , and Technological Controls . The new structure is designed to improve the effectiveness of implementing information security controls that are more adaptive to the development of digital technology and contemporary cyber threats . Known as a risk assessment standard that involves a risk identification process where each existing risk must be well recognized, then the risk impact is analyzed and ways to mitigate the risk are evaluated. Budiarto (2017) states that the ISO 27001 framework involves a process of communication and consultation as well as monitoring and review for the risk management process. Damanik et al. (2023) state that the risk management process itself consists of four sequential process stages: identification, analysis, evaluation, and risk management.

RESEARCH METHODS

This research was compiled using a Gap Analysis approach commonly used in ISO implementation . This research uses a descriptive quantitative approach to evaluate the readiness and effectiveness of information security governance in the IT Unit of Higher Education . The research methodology is divided into several main stages , namely 1) Instrument Preparation , 2) Data Collection , 3) Gap Analysis , 4) Risk Assessment , and 5) Recommendation Design.

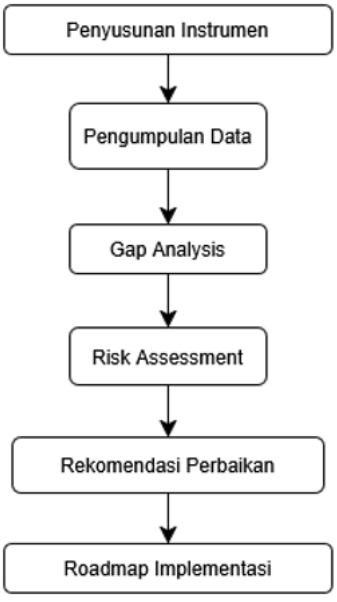

Figure 1. Research Method

The research instrument used is the ISO/IEC 27001 control compliance checklist . This checklist is compiled based on Annex A of the ISO/IEC 27001:2022 standard which contains 93 security controls , grouped into four broad categories : (1) Organization, (2) People, (3) Physical, and (4) Technology . Zalukhu et al. (2025) stated that in compiling the audit instrument each Annex A control is converted into a statement item that can be filled in by respondents or evaluated directly based on organizational documents and procedures . This

instrument will be used to measure the extent to which controls have been implemented . Assessment of the level of implementation of security controls is carried out using the Maturity Level Assessment model with a score range of 0–5. A score of 0 indicates that controls have not been implemented , while a score of 5 indicates that controls have been implemented optimally , documented , monitored , evaluated , and experienced continuous improvement . This model is used to measure the maturity level of security control implementation based on the information security governance evaluation principles commonly used in ISO /IEC 27001 audits and assessments .

Data Collection

To obtain a comprehensive picture , data triangulation was conducted through three things : 1) Field Observation : Direct review of the physical and logical infrastructure in the IT Unit, including server rooms , data centers , and network device access management. 2) Documentation : Analysis of formal documents such as Information Security Policies (ISOs), Standard Operating Procedures (SOPs), and cyber incident reports . 3) Questionnaires : to measure the maturity level with 93 Annex A controls . The data obtained were analyzed using risk analysis based on the ISO/IEC 27001 framework , including identification of assets , threats , and vulnerabilities . According to Jelita et al. (2024) this was done to help provide recommendations to universities to improve information security so that data leaks do not occur.

Gap Analysis

The gap analysis stage according to Warisaji et al. (2026) aims to measure the extent of current governance maturity compared to the ISO /IEC 27001:2022 standard . The analysis is carried out by mapping existing conditions against the Main clauses (Clauses 4-10) used in assessing aspects of leadership , planning , support , operations , performance evaluation , and improvement . In addition , there are 93 Annex A controls to audit control implementation . The results of this analysis will be expressed in percentages which will then be used as a basis for determining security priorities and selecting security controls for systematic and sustainable risk mitigation .

Risk Assessment

Identifying information assets , threats , and vulnerabilities using a risk- based methodology to determine improvement priorities . From the identification results , all identified assets will be subjected to a risk analysis to determine the high and low criticality of the asset to the organization and to determine the vulnerability , impact , threats , and how likely the threat is to occur for the asset. This was also conveyed by Putra et al. (2016) .

Design Recommendations

The results of the risk assessment and gap analysis form the basis for compiling a new Statement of Applicability (SoA) document . The main focus in this stage is 1) Preparation of the Roadmap by Creating a short -term implementation schedule (urgent technical improvements), medium- term (policy updates), and long -term (certification and internal audits). 2) Risk Mitigation : Determining risk treatment schemes such as mitigation , transfer, or acceptance of risk based on the availability of IT Unit resources .

RESULTS AND DISCUSSION

The research results were analyzed into several main aspects, namely: (1) Evaluation of the level of compliance with security controls based on ISO/IEC 27001 (2) Identification of factors that influence the effectiveness of ISMS implementation in supporting sustainable organizational data security governance. (3) Recommendations for Improvement and Implementation Roadmap.

Evaluation of the level of compliance with security controls based on ISO/IEC 27001

Compliance levels were measured in this study using questionnaires , interviews, and direct observation. The following table displays the results of the compliance level evaluation based on 93 security controls:

Table 1. Evaluation of compliance levels based on ISO/IEC 27001

Score	Information	Control SMKI
0	There is no implementation of any policies / procedures at all.	16%
1	Starting to be implemented but not documented	14%
2	It has been implemented and documented but is not yet comprehensive.	6%
3	It has been running according to SOP, but needs development	40%
4	Development has been completed , There has been monitoring and periodic evaluation	14%
5	Requirements have been met , are fully operational , are actively monitored and improved , and there is substantial evidence .	10%
	Total	100%

Based on the analysis of the implementation level of the Information Security Management System (ISMS) based on ISO/IEC 27001, the distribution of the maturity level of information security controls was obtained, which shows the variation in the level of implementation in higher education . These results illustrate that most security controls have reached the operational implementation stage, although there are still several areas that require further strengthening and development. Based on the results of the weighting of the maturity level of security controls, the average compliance value was 54%, which indicates that the implementation of the ISMS is in the medium category (moderately implemented).

Sixteen percent of ISMS controls scored 0, indicating that security controls or supporting policies and procedures were not yet implemented in these areas. This indicates that information security aspects remain undiagnosed and remain under-managed, potentially posing risks to the confidentiality, integrity, and availability of organizational information.

At a score of 1, 14% of controls indicate that information security implementation has begun but has not yet been formally documented. This indicates that some security activities are already running practically, but do not yet have written standard procedures or adequate documentation to support consistent implementation. Six% of controls are at a score of 2, meaning security controls have been implemented and documented, but their implementation is still not comprehensive across all organizational units or processes. This condition indicates

that the organization has a foundation for information security governance, but its implementation still requires expansion of scope and increased consistency.

The highest percentage was at score 3, at 40%, indicating that most information security controls were implemented in accordance with established standard operating procedures (SOPs). However, this implementation still requires further development to optimize the effectiveness of security controls. This finding indicates that the organization already has a sound foundation for implementing an ISMS in its operational aspects.

Furthermore, 14% of controls scored 4, indicating that the security control development process has been completed and the organization has implemented regular monitoring and evaluation. This reflects the organization's commitment to continuous monitoring and improvement in information security management.

Meanwhile, only 10% of controls achieved a score of 5, the highest maturity level in ISMS implementation. At this stage, information security requirements have been fully met, security controls are operating effectively, are actively monitored, and are supported by substantial evidence of implementation. This percentage indicates that there is still room for improvement for more security controls to reach optimal levels.

Overall, the analysis shows that the organization's ISMS implementation is at a medium to mature level, with operational controls operating in accordance with standard operating procedures (SOPs). However, improvements are still needed in documentation, implementation consistency, monitoring, and ongoing development to ensure all security controls meet the optimal ISO/IEC 27001 standards.

Identify factors that influence the effectiveness of ISMS implementation

Based on the evaluation results, 16% of controls still scored 0 and 14% of controls scored 1. These findings indicate that some information security areas lack adequate policies, procedures, or formal documentation. This indicates that information security governance has not been fully integrated into the organization's management processes. In higher education environments, the complexity of organizational structures and the diversity of work units often result in inconsistent implementation of information security policies.

Implementing ISO/IEC 27001 requires adequate human resources, technology, and funding. Some controls that have not been optimally implemented may be due to budget constraints for providing security infrastructure, monitoring devices, or conducting regular security audits. These resource limitations can potentially cause organizations to prioritize operational needs over strengthening information security.

The characteristics of higher education institutions that prioritize information transparency and academic collaboration also present challenges in implementing ISMS. A strong culture of information sharing often has the potential to conflict with the strict access control principles required by ISO/IEC 27001. Therefore, a balance is needed between academic transparency and the protection of institutional information assets.

The study results show that only 24% of controls have reached the monitoring and optimization level (scores 4 and 5). This indicates that information security evaluation mechanisms still need improvement. Suboptimal monitoring can cause organizations to be late in identifying system

weaknesses or emerging threats. Therefore, consistent implementation of the PDCA (Plan-Do-Check-Act) cycle is a crucial factor in increasing the effectiveness of ISMS implementation.

Recommendations for Improvement and Implementation Roadmap

Table 2. Recommendations for Improvement and Implementation Roadmap

Focus on Improvement	Priority Programs	Target Achievement
Basic fixes and documentation	1) Identify controls that have not been implemented 2) Preparation and revision of information security policies 3) Complete SOPs and control documentation 4) Formation of an information security team 5) Initial socialization of ISO/IEC 27001 implementation Implementation of audit gap analysis	1) All controls have formal documentation 2) Availability of an information security governance structure Increasing early awareness of officers
Strengthening implementation and monitoring	1) Implement comprehensive security controls 2) Improved access control and system monitoring 3) Implementation of log management and data backup 4) Implementation of information security training 5) Monitoring compliance with SOP implementation Periodic internal audits	1) Security controls run more consistently 2) Decrease in the number of audit findings 3) Increase the level of implementation compliance Security monitoring starts to run effectively
Continuous optimization and improvement	1) Integration of ISMS with the organization's IT governance 2) Development of security monitoring dashboard 3) Implementation of PDCA-based continuous improvement 4) Periodically evaluate the effectiveness of security controls 5) Cyber security incident handling simulation Preparation for ISO/IEC 27001 certification	1) Most of the controls reach a high level of maturity. 2) Information security culture is formed 3) The organization is ready to face the certification audit. Security systems are more adaptive to cyber threats

CONCLUSION AND SUGGESTIONS

Overall, the adoption of the ISO/IEC 27001:2022 standard is a crucial strategic step for Higher Education IT Units in ensuring the sustainability of information security governance. The analysis shows that the implementation of the ISMS has been quite successful, with a moderate level of compliance, with most operational aspects aligned with standard operating procedures (SOPs). However, significant gaps remain, such as uneven security controls, lack of formal documentation, and suboptimal monitoring and evaluation. The success of this system depends heavily on the synergy between management support and human resource awareness of information security culture. As a follow-up step, organizations need to commit to continuous improvement by strengthening internal audits, refining documentation, and enhancing personnel competencies to achieve a more resilient and adaptive ISMS maturity level to the dynamics of cyber threats.

BIBLIOGRAPHY

Bakri, M., & Irmayana, N. (2017). Analysis and Implementation of the BPKP SIMHP Information Security Management System Using the ISO 27001 Standard. Jurnal Tekno Kompak, 11(2), 41. https://doi.org/10.33365/jtk.v11i2.162

Basuki, HEUA, Hafiz, A., & Sallu, S. (2026). Implementation of the ISO/IEC 27001:2022 Information Security Management System in the Information Technology Unit of Higher Education. REMIK: Research and E-Journal of Computer Informatics Management, 10(1), 396–406. https://doi.org/10.33395/remik.v10i1.15907

Budiarto, R. (2017). Information System Security Risk Management Using FMEA and ISO 27001 Methods in XYZ Organization. 2(2).

Damanik, AP, Zaki, A., Fiddarain, S., & Nasution, AB (2023). Implementation of ISO 27001:2013 in Information System Security at the ANNUR PRIMA Islamic Education Foundation. Journal of Science and Technology (JSIT), 3(1), 74–79. https://doi.org/10.47233/jsit.v3i1.488

Goeritno, A., & Hendrawan, AH (2016). Implementation of ISO/IEC 27001:2013 for the Information Security Management System (SMKI) at the Faculty of Engineering, UIKA-Bogor.

Hendayun, M., & Zulianto, A. (2019). Security Audit of Academic Information System of General Achmad Yani Health College Using SNI ISO/IEC 27001:2013.

Hisyam, GF, & Rojabi, MA (2025). Analysis and Implementation of Point of Sales Application Security Management System Using ISO 27001. Integrative Perspectives of Social and Science Journal, 2(February 1), 1087–1094.

Izzani, M., Nellatul, N., Ismatul, A., & Hamdani, A. (2026). Evaluation of Information Security Implementation at SIAKAD Ibrahimy University Based on ISO/IEC 27001:2022. Information Systems Scientific Journal, 5(1), 175–185. https://doi.org/10.51903/d3bktm29

Jelita, LDA, Azam, MNA, & Nugroho, A. (2024). Information Technology Security Evaluation Using Information Security Index 5.0 and ISO/EIC 27001:2022. Saintekom Journal: Science, Technology, Computers and Management, 14(1), 84–94. https://doi.org/10.33020/saintekom.v14i1.623

Laily, ATN, & Siahaan, DT (2023). The Role of ISO 27001:2013 Certification for Scaling Up Business Startup Delman.IO. UDA Journal, 31(5), 216–227. https://doi.org/10.46930/ojsuda.v31i5.3802

Mustaqillah, S., & Aziz, AS (2025). Analysis of ISO 27001: 2022 on the Resilience of Higher Education ICT Infrastructure Against Ransomware Attacks (Case Study of ICT at UIN

Ar-Raniry). Innovative: Journal of Social Science Research, 5(4), 7542–7556. https://doi.org/10.31004/innovative.v5i4.20950

Pia Suci Lestari, Fatimah Zahra Tambunan, Ariq Wiratama Nasution, Monika Amelia Manurung, Ropika, Cherine Lita Purnama Panjaitan, & Dear Selvanathan Sinaga. (2025). Implementation of ISO 27001 in Increasing User Trust in the Industrial Sector: Research. Journal of Community Service and Educational Research, 4(1), 1152–1167. https://doi.org/10.31004/jerkin.v4i1.1565

Putra, AA, Nurhayati, OD, & Windasari, IP (2016). Planning and Implementation of Information Security Management System Using ISO/IEC 27001 Framework. Journal of Computer Technology and Systems, 4(1), 60. https://doi.org/10.14710/jtsiskom.4.1.2016.60-66

Rahman, A., Fachrurozi, F., & Safitri, S. (2024). The Urgency of Implementing ISO 27001 in Islamic Banking in Indonesia. Madani Syari'ah, 7(1), 71–83. https://doi.org/10.51476/madanisyariah.v7i1.640

Ramadhanty, N. (2024). Implementation of the NIST and ISO/IEC 27001 Security Frameworks in Facing Cyber Risk Threats. Journal of Indonesian Management, 4(4). https://doi.org/10.53697/jim.v4i4.1973

Setiawan, S., & Wardhani, IP (2026). Evaluation of the Effectiveness of Cybersecurity Mapping in the Implementation of an ISO/IEC 27001:2022-Based Information Security System at PT JASA RAHARJA. JATI (Informatics Engineering Student Journal), 10(2), 2787–2794. https://doi.org/10.36040/jati.v10i2.17827

Sholikhatin, SA, Setyanto, A., & Luthfi, ET (2018). Information System Security Analysis with ISO 27001 (Case Study: Academic Information System of Muhammadiyah University of Purwokerto). CIDA IT Scientific Journal, 4(1). https://doi.org/10.55635/jic.v4i1.75

Siregar, MNH & Mardiah. (2025). Data Security Analysis in Information Systems Using the ISO/IEC 27001 Method. Journal of Computer Science and Informatics Engineering, 1(2), 58–64. https://doi.org/10.64803/juikti.v1i2.52

Suprayitno, A. (2026). Data Security Governance Model in the Muhammadiyah Education Ecosystem: Synthesis of ISO 27001:2022 and PHIWM Values. Peradaban Journal of Interdisciplinary Educational Research, 4(1), 37–49. https://doi.org/10.59001/pjier.v4i1.803

Warisaji, TT, Wijaya, G., & Kurniawati, LS (2026). Designing a Data Security System Based on the ISO 27001 Standard in an Informatics Engineering Laboratory Environment.

Zalukhu, D., Yasin, V., & Yulianto, AB (2025). Evaluation of Academic Information System Security at STMIK Jayakarta Based on ISO/IEC 27001:2022.