Progresif: Jurnal Ilmiah Komputer
https://ojs.stmik-banjarbaru.ac.id/index.php/progresif/index
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat - Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0877

Evaluation of Information Security Readiness Using the KAMI Index 5.0 and ISO/IEC 27001:2022

DOI: http://dx.doi.org/10.35889/progresif.v21i2.2882

Creative Commons License 4.0 (CC BY – NC)

Beri Novriyadi[1*], Muhammad Jazman[2], Megawati[3], M. Afdal[4]
Information System, Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru, Indonesia
*e-mail *Corresponding:* 11950311543@students.uin-suska.ac.id

Abstract

Information security evaluation is a crucial process for organizations to assess their level of readiness and to establish clear security management roles and responsibilities. Higher education institutions, such as Tuanku Tambusai University of Heroes, have significant responsibilities in safeguarding sensitive data. The institution maintains extensive records that include students' personal information, academic transcripts, financial data, and information relating to faculty and staff. Given that multiple organizational units access this information, ensuring data protection and compliance with privacy regulations is paramount. This research purposes to assess the readiness and maturity of information security at Tuanku Tambusai Heroes University using the KAMI Index version 5.0, using the ISO/IEC 27001:2022 standard. This assessment covers six information security domains and shows maturity levels ranging from I+ to II, which indicates that the institution is at an early stage of development, with only the fundamental framework established. In addition, the completeness of the ISO/IEC 27001 implementation was assessed as "Unqualified", with a score of 379, corresponding to maturity levels I+ to II. These findings highlight the need for targeted improvements to meet the requirements for ISO/IEC 27001:2022 certification.

Key word: *Evaluation; ISO/IEC 27001:2022; Information Security; KAMI Index*

Abstrak

Mengevaluasi keamanan informasi sangat penting bagi organisasi karena membantu menilai tingkat kesiapan keamanan informasi dan menentukan peran dan tanggung jawab manajer keamanan. Institusi pendidikan tinggi, seperti Universitas Pahlawan Tuanku Tambusai, bertanggung jawab untuk menjaga informasi sensitif. Institusi ini menyimpan sejumlah besar data mahasiswa, termasuk rincian pribadi, catatan akademis, informasi keuangan, dan data mengenai dosen dan staf. Karena banyak unit mengakses data ini, sangat penting untuk memastikan perlindungan dan kepatuhannya terhadap peraturan privasi. Studi ini bertujuan untuk menilai kesiapan dan kematangan keamanan informasi di Universitas Pahlawan Tuanku Tambusai menggunakan Indeks KAMI versi 5.0 dan standar ISO/IEC 27001:2022. Evaluasi, yang mencakup enam area keamanan informasi, mengungkapkan tingkat kematangan mulai dari I+ hingga II, yang menandakan bahwa institusi tersebut berada pada tahap awal, dengan hanya kerangka dasar yang tersedia. Lebih jauh, kelengkapan implementasi ISO/IEC 27001 dinilai sebagai "Tidak Memenuhi Syarat," dengan skor 379, juga dalam level I+ hingga II. Hasil ini menunjukkan perlunya perbaikan signifikan dalam tata kelola keamanan informasi untuk memenuhi persyaratan sertifikasi ISO/IEC 27001:2022.

Kata kunci: *Evaluasi; Indeks KAMI; ISO/IEC 27001:2022; Keamanan Informasi*

1. Introduction

Information and communication technology (ICT), such as E-Government, is a form of data that is easily accessible and vulnerable to hacking on web portals. Information security challenges continue to grow along with technological developments, and cyber attacks are becoming increasingly sophisticated and detrimental [1]. The information security in question is about confidentiality, integrity, and availability. In protecting information, an information security assessment must be carried out to identify information security gaps and deficiencies, and prevent the misuse of the information [2], [3]. Universities are one of the entities that have a great responsibility in maintaining their information security [4]. Maintaining information system security is very important for universities in carrying out their operations or activities effectively and protecting valuable information assets [5].

Pahlawan Tuanku Tambusai University stores a significant amount of sensitive information, including students' data, academic records, financial details, as well as information related to lecturers and employees. With access to this data spread across various units, it is crucial to ensure strong protection and compliance with privacy regulations. This is in line with Indonesian Personal Data Protection Law (UU Personal Data Protection) Article 35, which states that processors of personal data shall ensure the protection and safety of legitimate personal information by applying appropriate administrative and procedural steps to protect personal data and prevent any form of interference [6]. Currently, Pahlawan Tuanku Tambusai University faces not only the risk of losing sensitive data, but also increasingly complex and often far-reaching cyberattacks. In addition, each university has unique characteristics, both academically and in terms of the academic community, including the environment, such as a complex IT infrastructure comprising networks, database systems, and widely accessible applications. These unique characteristics can impact the security needs and risks associated with higher education information systems. Therefore, college information system security governance needs to be tailored to the unique characteristics of each college, and this requires universities to have standards to help manage security risks, including Pahlawan Tuanku Tambusai University [7].

Pahlawan Tuanku Tambusai University collaborates with external service providers, including cloud vendors, which requires strong information security management. By KOMINFO Regulation No. 4 of 2016 and BSSN Regulation No. 8 of 2020, institutions are encouraged to implement the SNI ISO/IEC 27001 standard to manage security risks related to external partnerships [8], [9]. Compliance with ISO/IEC 27001:2022 also demonstrates a university's commitment to information security, which can positively impact its reputation both publicly and in regulatory contexts [7]. Furthermore, based on BSSN Regulation No. 8 of 2021, Electronic System Operators are permitted to conduct self-assessments using the Information Security Index (Indeks KAMI) as a standardized tool to evaluate their level of security readiness [10]. Although the KAMI Index is not designed to measure the effectiveness of specific controls, it provides organizational leaders with an overall picture of their institution's security posture. The latest version, KAMI Index 5.0, aligns with ISO/IEC 27001:2022 and offers a more comprehensive and structured approach for assessing and improving information security in higher education institutions [3]. Based on research, evaluated information system security using the KAMI Index 5.0 and ISO/IEC 27001 standards. Fauzia et al. assessed university information systems based on KAMI elements aligned with SNI ISO 27001 [3]. Lucia and her team applied the KAMI Index 5.0 and ISO/IEC 27001:2022, resulting in a score of 674 ("Fairly Good") with maturity levels ranging from Level II to IV [11]. I Nyoman Adi Artha Wibawa evaluated hospital information security with a score of 177 ("Not Qualified"), recommending improvements in governance, risk management, asset inventory, and data protection [12]. Rafii Nur Akmal found strong incident management in SIMRS using ISO 27001, but suggested regular evaluations [13]. Evariani reported low security maturity at STIK Bina Husada (score 417), highlighting the need for better policies and governance [14]. Rudolf Sinaga developed a compliance model for ISO 27001:2022 in a university, showing good physical security, but areas like policy, risk management, and access control still required improvement [7].

Based on the background previously discussed, this research aims to evaluate the information security readiness of a higher education institution by utilizing the KAMI Index version 5.0 by the ISO/IEC 27001:2022 standard. The assessment is intended to measure the maturity level of existing information security practices, identify critical gaps, and provide recommendations for improvement. By integrating national regulatory frameworks with internationally recognized standards, the research facilitates the development of more effective information security governance, risk management, and policy implementation. The findings are expected to serve as a strategic foundation for enhancing institutional efforts in securing information assets. Furthermore, the study contributes to the university's preparedness in achieving compliance with ISO/IEC 27001:2022 and strengthening its overall information security posture.

2. Literature Review

Previous research by [3] analyzed the security of information systems in universities based on the KAMI Index, which is aligned with the standard elements of SNI ISO 27001. The analysis results show significant differences between the two private universities. College A obtained a score of 713, which was categorized as “Good Enough”, with excellence in governance, personal data protection, and technological aspects. In contrast, College B only achieved a score of 321, indicating an “Inadequate” security level, although it still has strengths in the personal data protection aspect. Meanwhile, [11] evaluated information technology security using the KAMI 5.0 Index and ISO/IEC 27001:2022, with the results of an electronic system score of 19 (high category) and a final score of 674 (category “Good enough”). The maturity level of the ISO 27001 standard implementation is at Levels II to IV.

Another research was conducted by [7], who developed a model for assessing compliance with the ISO / IEC 27001: 2022 standard in a university environment. The results show a high level of compliance with physical and environmental security aspects, but there are still deficiencies in information security policies, risk management, asset management, access control, network security, and incident management. Through this model, a comprehensive picture of the level of compliance is obtained as well as recommendations for improving information system security. In addition, [15] evaluated information technology security governance at STMIK Mardira Indonesia using the KAMI Index. The electronic sector score reaches a high value (21), but the overall governance score is only 117, which is categorized as “Not Feasible”, so significant improvements are needed in information technology security governance at the institution.

Previous research has used the KAMI Index and ISO/IEC 27001 to assess information security in higher education, but as in the research of [3] have not integrated the two in depth, while [7] and [15] emphasize aspects of compliance or governance without aligning with the latest version of international standards. So this study utilizes the KAMI Index version 5.0 which has been adapted to ISO/IEC 27001:2022, to provide an assessment that is more relevant to modern information security challenges. This research also reinforces this direction by presenting a comprehensive evaluation model to assess information security readiness, especially in the context of institutional cooperation with third parties. This integration provides a more complete and strategic picture for improving information security governance and compliance in higher education.

3. Methodology

The research stages are illustrated in the flow chart in Figure 1. This research was conducted through several main stages, namely planning, data collection, validation, and analysis.

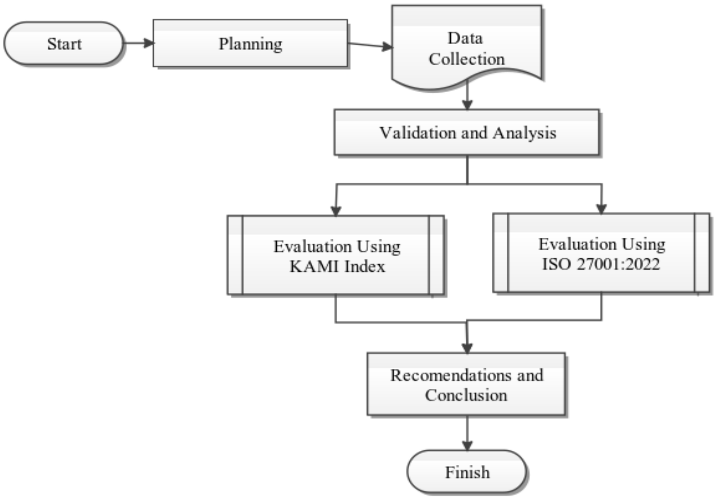

Start
Planning
Data Collection
Validation and Analysis
Evaluation Using KAMI Index
Evaluation Using ISO 27001:2022
Recomendations and Conclusion
Finish

Figure 1. Methodology Research

This research begins with a planning stage, which includes identifying problems through observations at Pahlawan Tuanku Tambusai University to understand the running business processes, determining objectives to determine the level of integrity and maturity of information security, and determining problem boundaries so that the research focus remains directed. The required data is determined based on relevant literature and information security data. At the data collection stage, field observations, interviews with IT parties, and literature studies of relevant references and previous research were carried out, to select the right evaluation method, namely the KAMI Index version 5.0 and ISO / IEC 27001: 2022. Furthermore, at the data validation and analysis stage, a checklist is carried out on the questionnaire that has been filled out to ensure the validity of the data based on real conditions. The results of the questionnaire were then calculated to determine the completeness and maturity scores of information security, then compared with the controls in ISO/IEC 27001: 2022. Based on the evaluation results, recommendations are made for improvements in each area that has not met the standards, so as to improve the readiness and effectiveness of the information security system at Pahlawan Tuanku Tambusai University.

3.1 Information Security

Information security encompasses measures designed to protect the confidentiality, integrity, and availability of information [16], [17]. According to ISO/IEC 27002 (2005), this standard provides guidelines for protecting information from various threats, aiming to ensure business continuity, mitigate risks, and improve both investment returns and business prospects. Consequently, information security indirectly supports the sustainable operation of businesses over the long term [18], [19]. This field involves managing access, usage, modification, distribution, and disposal of information to guard against fraudulent activities [20]. Additionally, information security is commonly divided into multiple domains, including physical security, personnel security, operational security, communication security, and network security [18].

3.2 KAMI Index

The Information Security Index (ISI) functions as an instrument to measure and evaluate the maturity and preparedness of an ISMS [15]. Likewise, the KAMI Index acts as a strategic tool offering organizational leaders a detailed insight into the current state of information security readiness within the organization [21], [22]. The KAMI Index version 5.0 represents the latest update from version 4.2 and was officially released in March 2023. This version incorporates new controls introduced in the SNI ISO/IEC 27001:2022 standard. Notable updates in the annex of SNI ISO/IEC 27001:2022 include a restructuring of control categories, the addition of 11 new controls, and modifications to existing ones. In alignment with these updates, the KAMI Index has also been revised and updated from version 4.2 to version 5.0 to reflect the latest changes in the standard [12].

3.3 SNI ISO/IEC 27001:2022

The ISO/IEC 27001:2022 standard was officially published in October 2022. This standard is a revision of ISO/IEC 27001:2013 and is designed to help organizations protect information, as well as increase the relevance and effectiveness of the standard in the context of evolving information security threats and practices [3], [23].

Table 1. Comparison of ISO/IEC 27001:2013 and ISO/IEC 27001:2022

Aspect	ISO 27001:2013	ISO 27001:2022
Release Date	October 2013	October 2022
Number of Controls	114 controls	93 controls
Annex A Structure	14 domains	4 themes
New Controls	None	11 new controls added

The SNI ISO/IEC 27001:2022 introduces new controls and a restructured Annex, marking a significant update from the 2013 version. Unlike the earlier standard that primarily focused on documentation, the 2022 edition emphasizes integrated processes, cybersecurity, and privacy. Additionally, it places greater importance on sustainability, which was less highlighted in the previous version [12], [22]. The latest version of ISO/IEC 27001 includes the addition of 11 new controls [24]:

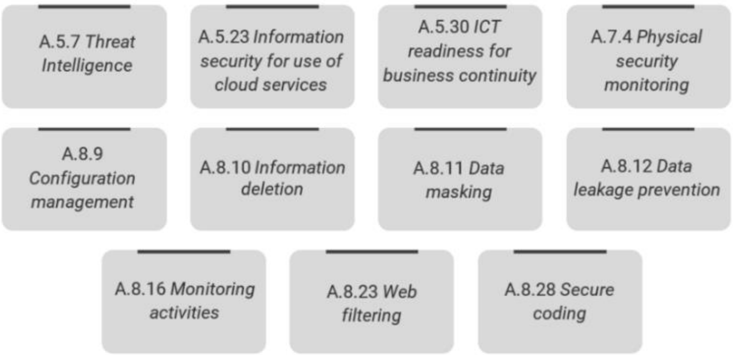

A.5.7 Threat Intelligence
A.5.23 Information security for use of cloud services
A.5.30 ICT readiness for business continuity
A.7.4 Physical security monitoring
A.8.9 Configuration management
A.8.10 Information deletion
A.8.11 Data masking
A.8.12 Data leakage prevention
A.8.16 Monitoring activities
A.8.23 Web filtering
A.8.28 Secure coding

Figure 2. New Controls ISO 27001:2022

4. RESULTS AND ANALYSIS

4.1 Data Collection

This stage involves an initial assessment of the level of information security readiness at Pahlawan Tuanku Tambusai University using the KAMI Index version 5.0 measurement tool, which is based on the ISO/IEC 27001:2022 standard. Based on interviews with the head of PUSKOM, it was found that the university had never conducted a formal assessment of its information security, either using the KAMI Index approach or the ISO standard. As part of this process, a sample of data was obtained in the form of a list of information assets within the university environment, including hardware, data, websites, networks, physical facilities, human resources, and campus buildings. This evaluation covers several assessment categories in the KAMI Index version 5.0, namely the Electronic Systems Category used by the Institution, Information Security Governance, Information Security Risk Management, Information Security Framework, Information Asset Management, Information Technology and Security, and Personal Data Protection, as well as a Supplement as an evaluation area for the aspect of Securing Third-Party Service Provider Involvement.

The questions in the Information Security Index (KAMI Index) are grouped into two main categories. The first category is designed to assess an organization's readiness to implement information security in accordance with the ISO/IEC 27001:2022 standard. The assessment is conducted through stages of basic framework implementation, effectiveness and consistency of implementation, and the organization's ability to make continuous improvements. Each answer is given a specific score, which is then compiled to produce an overall index value, visualized in the form of a radar chart to illustrate the level of maturity on a scale of 1 to 3 as a benchmark. The second category groups questions based on the maturity level of information security implementation, referencing frameworks such as COBIT or CMMI. This maturity level is used to map and classify information security readiness, particularly within government agencies. In this case, the KAMI Index divides maturity levels into five levels, namely: Level I (Initial Condition), Level II (Basic Framework Implementation), Level III (Defined and Consistent), Level IV (Managed and Measurable), and Level V (Optimal).

4.2 Evaluation using KAMI Index Version 5.0 and ISO 27001:2022

The KAMI Index measurement process begins with the preparation of a checklist that aims to validate the data that supports the KAMI Index results. After the checklist is completed to ensure the data's suitability with the actual conditions, the next step is to verify and calculate the results of the KAMI Index. This procedure is followed by analyzing and assessing the completeness and maturity levels of the information security system. The outcomes of the KAMI Index measurement are subsequently compared with the controls specified in ISO 27001. After the comparison is made, the next step is to provide recommendations, which contain input to improve the shortcomings that Pahlawan Tuanku Tambusai University has not implemented.

Table 2. KAMI Index Assessment Result Score

Control Category	Total Questions	Aggregate Score	Respondents
Governance	22	126	46
Risk Management	16	72	27
Framework	33	192	43
Asset Management	53	258	110
Technology Aspect	35	186	93
Personal Data Protection (PDP)	16	84	60

Table II shows the KAMI Index Assessment Result Score for each of the six assessment categories used in the KAMI Index version 5.0. The scores in this table reflect the level of maturity of information security management in each category, obtained from the evaluation results of Pahlawan Tuanku Tambusai University. Further explanation of the meaning of the scores obtained in each assessment category is presented as follows.

4.2.1 Information Security Governance

In the information security governance assessment stage, a university is expected to be able to prepare and implement a structured governance mechanism, where the duties and responsibilities of information security management are divided among the information technology manager or staff. Based on the results shown in Table II, the assessment of the information security governance area obtained a score of 46 out of a maximum total score of 126. This score indicates that the governance maturity level is at level I+, which reflects the initial conditions in implementing information security governance. These results indicate that Pahlawan Tuanku Tambusai University has not fully defined the requirements or standards of competence and expertise required, and has not secured information according to applicable standards. Moreover, the integration of information security needs and requirements into the organization's operational processes remains incomplete, and several issues persist concerning the comprehensive implementation of information security governance.

4.2.2 Information Security Risk Management

The objective of the information security risk management evaluation phase is to assess the preparedness of risk management strategies and to verify their applicability within the university environment to effectively reduce potential threats. The completeness score obtained is 27 from the maximum value of the area of 72, as stated in Table II. These results show that the conditions in the information security risk management area currently have a measurement value of the I+ maturity level. It is necessary to implement a documented information security risk management framework, carry out structured information security risk management of existing information assets, arrange mitigation steps according to the priority level and completion target, and need to conduct regular evaluations/assessments related to the risk management framework.

4.2.3 Information Security Governance Framework

The information security governance framework assessment section contains policies and procedures that will be the center of attention for work readiness. These aspects will be used as steps to implement information security. Table II shows the completeness score of the information security management framework section obtained 43 from a maximum value of 43 area of 192. These results can describe the current state of maturity of the information security framework, which is at the I+ maturity level. Pahlawan Tuanku Tambusai University has not carried out official procedures, and there is no policy related to information security, nor is there a secure system development process (Secure SDLC). Pahlawan Tuanku Tambusai University has also not conducted internal audits in evaluating the level of compliance, consistency, and effectiveness of information security. However, Pahlawan Tuanku Tambusai University has developed a strategic plan for improving information security over the medium to long term (1, 3, and 5 years), with a commitment to consistent implementation.

4.2.4 Asset Management

The information asset management section assesses the thoroughness of information asset protection and outlines the entire lifecycle of asset utilization within the organization. Based on Table II, the completeness score obtained in the management of information assets is 110 from the maximum value of the area of 258, which shows the measurement value of the I+ maturity level. From these results, it can be seen that the current condition of the information asset management area, where configuration management has not been consistently applied, then the process of identifying and inventorying information assets by laws and regulations has not been implemented if it has passed the retention limit. Procedures for using access and access rights that have not been followed, if there is a discrepancy with the policy.

4.2.5 Technology and Information Security

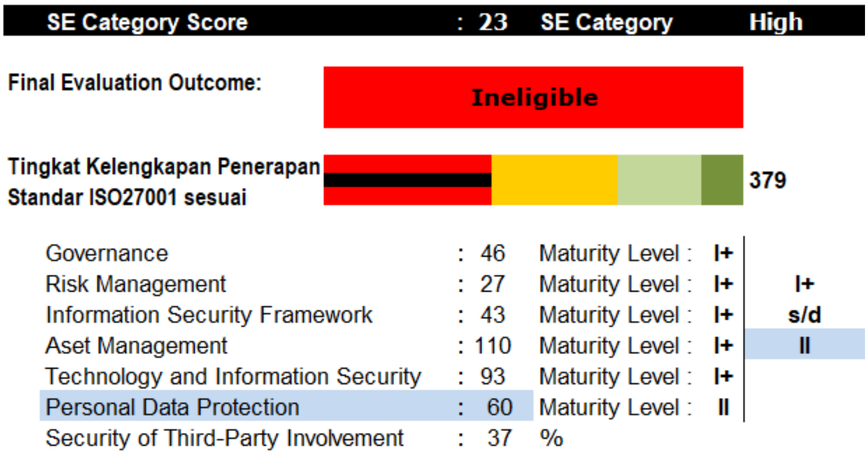
The assessment of technology's role is reflected in the extent, consistency, and effectiveness of its application. The degree of technological completeness directly influences the feasibility of ensuring information security. As presented in Table II, the technology and information security section achieved a completeness score of 93 out of a maximum possible 186. The maturity level for technology and information security is currently at the I+ stage. However, certain issues remain unresolved, such as the lack of documented records and trace analysis results, as well as the absence of regularly and systematically updated antivirus and malware attack reports. Additionally, the development and testing environments, which should adhere to established technology platform standards and be utilized throughout the system development life cycle, have yet to be fully implemented.

4.2.6 Personal Data Protection

The personal data protection section assesses how complete, consistent, and effective the implementation of security measures is in safeguarding personal data. Based on Table II, the completeness score obtained in the amount of 60 out of the maximum value of the area of 80, which indicates the value of measuring the maturity level II. From these results, it can be seen that the current condition of the personal data protection area has implemented some policies related to personal data protection. However, there are still several policies that are still in planning, such as the personal data protection mechanism that has been implemented is not by risk mitigation and applicable laws. Also, Pahlawan Tuanku Tambusai University has not carried out a program to increase understanding/awareness among all employees regarding personal data protection, including matters related to regulations.

4.2.7 Assessment Results

The Electronic System Category Score, Final Evaluation Results, ISO 27001 Standard Implementation Level per Category, and final score with maturity level for each area can be seen in Figure 2.



SE Category Score : 23 SE Category High

Final Evaluation Outcome: Ineligible

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai 379

Governance	: 46	Maturity Level :	I+	
Risk Management	: 27	Maturity Level :	I+	I+
Information Security Framework	: 43	Maturity Level :	I+	s/d
Aset Management	: 110	Maturity Level :	I+	II
Technology and Information Security	: 93	Maturity Level :	I+	
Personal Data Protection	: 60	Maturity Level :	II	
Security of Third-Party Involvement	: 37	%		

Figure 2. Information Security Evaluation Results Pahlawan Tuanku Tambusai University

Based on the evaluation results, the electronic system category score is 23, which can be seen in Figure II. The results show that the level of dependence on information technology is in the high category. In addition, the results of the analysis also show that the total annual operating budget allocated for electronic system management is over IDR 1 billion, with the value of electronic system investments reaching more than IDR 3 billion.

Based on Figure II, the score obtained in the supplementary area is 37%. The supplement area includes evaluation questions related to the completeness, consistency, and effectiveness of the implementation of security mechanisms related to the risk of external third-party involvement in the operation of the agency/company service delivery.

The measurement results for the six areas of information security, as shown in Figure II, indicate that the information security maturity level at Pahlawan Tuanku Tambusai University is between levels I+ and II. This reflects a still early stage, where only the basic framework has been implemented. In parallel, the degree of adherence to the ISO 27001 standard is classified as "Ineligible", with a total score of 379, which also corresponds to levels I+ and II. This highlights that, despite the intensive use of electronic systems, the university has not yet achieved a satisfactory level of information security protection. Considering that the minimum threshold for obtaining ISO certification is set at level III+, it is necessary to undertake significant corrective actions and improvements to meet the requirements of the SNI ISO/IEC 27001 certification.

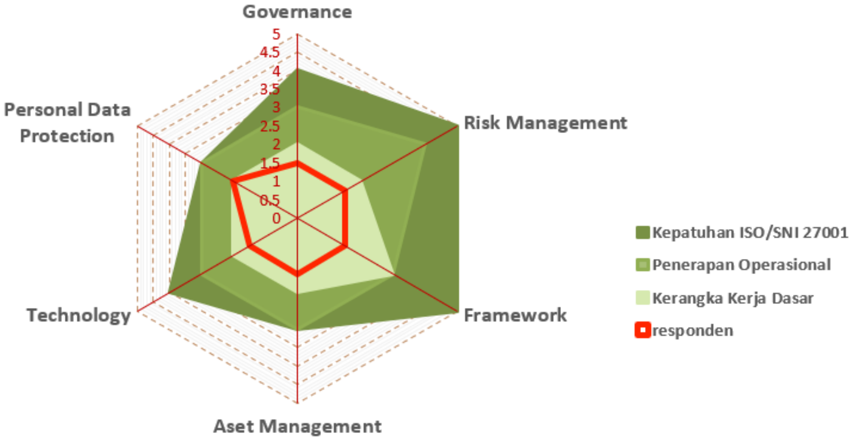


Figure 3. Radar Chart Display of Information Security Evaluation Results, Pahlawan Tuanku Tambusai University

Figure 3 presents the six-axis radar diagram section. The evaluation is shown as a thick red line that ranges from 0 to 1.5, with three thresholds representing the level of completeness (light green to dark green for Levels 1 to 3). The results show the assessment meets the light green threshold, indicating a basic framework level.

4.3 ISO/IEC 27001:2022 Recommendation

The results of the KAMI index analysis show that the scores obtained do not meet the criteria required for SNI ISO/IEC 27001 certification. Therefore, the researcher proposes a series of recommendations that can serve as a guide for developing information security governance to strengthen information protection at Pahlawan Tuanku Tambusai University. The recommendations are based on the SNI ISO/IEC 27001:2022 standard. They are formulated by identifying the gaps in each assessed area, with a direct comparison with the controls required by the standard. The following table illustrates the specific recommendations for each information security assessment area.

Table 3. ISO 27001:2022 Recommendations

No	Present Conditions	ISO 27001:2022 Recommendations	Discussion
1	Competency standards and qualification requirements for information security managers have not been established, and there are no programs in place to enhance the skills and knowledge of information	A.6.3 *Information security awareness, education and training* The university creates a document/ procedure for competency standards and expertise for information security management implementers, and a training program to improve	Competence supports the effective implementation of security controls. An ISACA that organizations with structured training experience a 30% reduction in incidents. ISO 27001:2022 also recommends awareness and training components as key security measures.

No	Present Conditions	ISO 27001:2022 Recommendations	Discussion
	security managers.	competencies and expertise	
2	There is no socialization program and increased understanding of information security for related parties, and no publication of information security regulations	A.5.1 *Policies for information security* Publish information security regulations to all staff/employees that are easily accessible if needed, and create a socialization program to increase understanding of information security	Policies are the foundation of ISMS. Research show emphasizes that structured policies support consistency, compliance, and risk preparedness. ISO 27001:2022 also recommends management involvement in policy approval.
3	There has been no coordination of agency information security managers with related work units, as well as interested internal parties, to ensure and implement information security compliance related to work processes that involve various parties	A.5.5 *Contact with authorities* Create regulations related to coordination in managing information security in implementing information security compliance with all relevant parties, including work units, internal parties, and other related parties	Communication with authorities speeds up incident handling and ensures legal compliance. Previous research shows that organizations with structured contacts respond to incidents 30% faster.
4	There is no document regulating the work program and framework for managing information security risks	A.5.24 *Information security incident management planning and preparation* Develop documentation and regulations about work programs and frameworks for managing information security risks	The creation of incident management documents is important as a written reference for handling information security incidents consistently. These documents ensure that every role, responsibility, and procedure has been agreed upon and is easy to follow when an incident occurs.
5	No established information security risk management framework outlines the relationships and classification levels of information assets, as well as the threat levels and potential impacts of losses to the organization.	A.5.12 *Classification of information* Create information security risk management framework documents and regulations that include the definition of relationships and classification levels of information assets, threat levels, and the impact of losses to the company	Classification helps protect information according to its value and risk. ISO 27002:2022 emphasizes classification as the basis for protection controls, including for personal, confidential, and public data.
6	The company's risk mitigation measures were not aligned with its priorities to achieve its objectives, the company did not have a risk management officer, and there was no safety and risk management status report.	A.6.8 *Information security event reporting* Reorganized risk management mitigation steps by priority and objective achievement, assigned risk managers, and reported on the status of information security risk management.	Early reporting enables rapid mitigation. A study found that 35% of incidents were handled late due to the lack of clear reporting channels. ISO 27001:2022 recommends transparent and secure reporting mechanisms.
7	Information security regulations do not reflect the need to mitigate information security risks.	A.5.26 *Response to information security Incidents* develop information security regulations and procedures that address mitigation requirements identified through the results of information security risk assessments.	Prompt handling reduces the impact of incidents, and documented response procedures reduce the average cost of incidents.
8	There is no information security identification process in the applicable follow-up procedures	A.5.27 *Learning from information security incidents* Create a document that provides a process that identifies conditions that compromise information security and applicable follow-up procedures	Learning from incidents drives continuous improvement. ISO 27001:2022 recommends this process as part of the incident management cycle. A study shows that organizations that implement incident post-mortems demonstrate up to a 40% increase in security maturity.
9	Lack of an information security exception management process	A.5.36 *Compliance with policies, rules and standards for information security*	The document formally regulates requests and approvals for exceptions to information security controls through risk assessment,

No	Present Conditions	ISO 27001:2022 Recommendations	Discussion
		Create a document containing formal procedures for managing an exception to the application of information security, including a follow-up process	documentation, and periodic reviews, so that each exception is managed in a controlled manner without compromising the integrity of the security system, in accordance with ISO/IEC 27001:2022.
10	There are no policies and procedures related to security patches	A.5.37 *Documented operating procedures* Create operational policies and procedures to manage security patches and the allocation of responsibilities	Documentation helps with consistency and training new staff. ISO 27001 requires documentation as part of operational controls and also emphasizes the importance of documented procedures for IT governance.
11	The discussion of information security in project management has not been carried out	A.5.8 *Information security in the project management* Creating documentation to explain information security in project management	Information security is often overlooked in projects, even though it can pose serious risks. The Project Management Institute (PMI) recommends integrating security aspects from the planning stage, so that risks can be anticipated early on and projects can run more securely.
12	A secure system development process (Secure SDLC) has not been implemented	A.8.25 *Secure development life cycle* Create a secure software development regulation (Secure SDLC)	The implementation of SDLC plays an important role in preventing vulnerabilities from the early stages of system development. SDLC shows that addressing security aspects from the outset can provide significant cost efficiencies compared to mitigation at the final stage.
13	There is no process or policy in place to mitigate the risks of implementing a new system	A.8.30 *Outsourced development* Implement regulations or procedures that can mitigate new risks arising from the implementation of new systems, as well as strategies for the use of information technology	Outsourcing is risky if not supervised. ISO 27001: 2022 provides guidance on third-party risk management. Research shows that 60% of breaches originate from unmonitored third parties.
14	There has been no internal audit that evaluates the level of compliance with information security implementation, identifies corrective and preventive measures, and there is no report on the results of the internal audit evaluation to the leadership	A.8.34 *Protection of information systems during audit testing* Prepare internal audit reports that contain the results of internal audits that assess the compliance, consistency, and effectiveness of information security implementation, as well as audits that were conducted to identify improvements and preventive actions for information security	The unmanaged audit process can open unauthorized access or disrupt operational systems. Therefore, it is very important to establish audit procedures that are secure and do not interfere with ongoing services. ISO 27001 emphasizes the need for risk mitigation during audits to prevent service disruption or data breaches.
15	Compliance assessments of the information security program were not conducted regularly.	A.8.14 *Redundancy of information processing facilities* Develop a timetable for regular evaluation and compliance testing of the information security program	Establishing a schedule for regular compliance evaluations and testing is important to ensure that security controls remain effective and aligned with applicable standards. This helps detect weaknesses early and prevent incidents or non-compliance that could impact the organization.
16	There is no clearly defined matrix to record access levels and access assignments for each type of information asset.	A.5.10 *Acceptable use of information and other associated assets* Create documents containing asset information	The creation of a university IT asset usage policy is important for regulating user behavior in the safe and responsible use of IT resources. This policy helps prevent misuse, protect digital assets, and raise awareness of information security within the university environment.
17	There is no process in place to identify and inventory	A.8.10 *Information Deletion*	Developing procedures for the secure deletion of information, both on digital

No	Present Conditions	ISO 27001:2022 Recommendations	Discussion
	information asset retention requirements by existing laws and regulations, and no process in place to evaluate compliance with retention requirements and delete information assets if they have passed the retention limit	Create a document that contains inventory information, including retention requirements for information assets as mandated by laws and regulations, and a process for evaluating compliance with these requirements and deleting information assets once they have exceeded their retention limit.	and physical media, is important to prevent data leaks. ISO/IEC 27001 emphasizes the importance of data sanitization processes appropriate to the type of storage media, to ensure that information cannot be recovered.
18	No configuration management process is consistently applied	A.8.18 *Use Of Privileged utility programs* University IT staff must perform configuration management processes regularly and consistently	Special utility programs should be restricted and only used by authorized personnel, with activity logging to prevent misuse. IT staff also need to perform regular configuration management to keep the system secure and under control.
19	A procedure for reviewing user access and access rights, including corrective actions in cases of non-compliance with applicable policies, has not been established	A.8.2 *Privileged access rights* Create documents that discuss user access review procedures and user access rights.	Privileged access rights need to be strictly managed because they are often the target of cyber attacks. The process of granting, reviewing, and revoking these rights must be carried out regularly to prevent misuse and ensure that only authorized parties have access.
20	Agencies/companies have not evaluated the security feasibility of cloud services, including aspects of their availability and fulfillment of ISO 27001-based service certification	A.5.19 *Information security in supplier relationships* Evaluate information security, including cloud services, using information security standardization such as the KAMI Index.	Hubungan dengan pihak ketiga menimbulkan risiko tambahan, sehingga perlu perjanjian keamanan informasi dan evaluasi berkala. ISO 27001:2022 menyarankan agar kontrol keamanan dicantumkan dalam kontrak vendor.
21	There are no documented records or analysis (audit trails) verifying that antivirus/antimalware software is updated regularly and systematically, nor are there reports on the follow-up and resolution of successful or failed virus/malware attacks	A.8.7 *Protection against malware* Create periodic reports related to the results of technology analysis/audit, containing antivirus/antimalware, that are followed up on.	Malware protection is essential to prevent infections that can result in data theft, system damage, or service disruption. The use of up-to-date antivirus software, user education, and active monitoring help detect and stop threats early on, as well as reduce the risk of human error as a major factor in the spread of malware.
22	Organizations have yet to implement secure application development principles (secure coding) for in-house or externally developed applications, and current applications lack defined security specifications and features that are verified and validated throughout the development and testing phases	A.8.28 *Secure Coding* The University must apply the principles in developing applications that are safe to use both internally and externally, and have been verified/validated in the application development process.	Implementing secure coding standards such as OWASP and providing regular training to developers is important because coding errors are often the entry point for attacks. OWASP shows that application vulnerabilities are a common cause of data breaches. Google and Microsoft also emphasize the importance of regular training as a preventive measure to improve software security.
23	Organizations have not established a development and testing environment secured according to existing technology platform standards, which is utilized throughout the entire system development lifecycle	A.8.31 *Separation of development, test, and production environments* The University should implement a secure development and test environment by existing technology platform standards.	Separating development, testing, and production environments is important to prevent cross-contamination between systems, data leaks, and configuration conflicts. ISO 27001 emphasizes that this separation is an important part of change control and protection of system operational security.

5. Conclusion

Evaluation of information security readiness at Pahlawan Tuanku Tambusai University, using the KAMI Index version 5.0, reveals a readiness status of “Ineligible” for ISO/IEC 27001:2022 compliance, with a total score of 379. While the Electronic Systems Category shows a “high” score of 23 and the Technology and Personal Data Protection areas show progress in maintaining confidentiality, integrity, and availability, other areas are still at the Basic Framework maturity level (I to I+). These findings highlight the need for substantial improvements, including the establishment of a dedicated information security team, a structured risk management program, and a comprehensive security policy. Furthermore, prioritizing network segmentation, improving personal data protection, and maintaining an up-to-date asset inventory are important steps. By implementing the provided recommendations, conducting regular audits, and enhancing staff knowledge of information security, Pahlawan Tuanku Tambusai University can strengthen its information security measures and align them with the ISO/IEC 27001:2022 standard, thereby ensuring better protection of student and employee data.

References

[1] E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, “Manajemen Keamanan Cyber Di Era Digital,” *J. Bus. Entrep.*, vol. 11, no. 1, pp. 23-34, 2023, doi: 10.46273/jobe.v11i1.365.

[2] Setiyowati and Sri Siswanti, “Penilaian Kematangan Proses Keamanan Sistem Informasi Pendaftaran Pasien Menggunakan Framework Cobit 4.1,” *SATIN - Sains dan Teknol. Inf.*, vol. 7, no. 1, pp. 123–133, 2021, doi: 10.33372/stn.v7i1.694.

[3] F. A. S. Ningrum, Y. Riwanto, I. Y. R. Pratiwi, and M. A. Fikri, “Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI,” *J. Inform. Polinema*, vol. 10, no. 3, pp. 437–444, 2024, doi: 10.33795/jip.v10i3.5154.

[4] H. Wahyudi, A. Zulianto, A. Maulana, S. Mardira Indonesia, and U. Langlangbuana, “Audit Keamanan Sistem Informasi Manajemen Akademik DanKemahasiswaan Menggunakan Sni Iso/Iec 27001:2013,” *J. Comput. Bisnis*, vol. 14, no. 1, pp. 40–46, 2020.

[5] R. R. Wijayanti, “Implementasi Octave-S Dan Standar Pengendalian Iso 27001:2013 Pada Manajemen Risiko Sistem Informasi Perguruan Tinggi,” *J. Petir*, vol. 11, no. 2, pp. 221–233, 2018, doi: 10.33322/petir.v11i2.351.

[6] G. Fox, T. Lynn, and P. Rosati, “Enhancing consumer perceptions of privacy and trust: a GDPR label perspective,” *Inf. Technol. People*, vol. 35, no. 8, pp. 181–204, 2022, doi: 10.1108/ITP-09-2021-0706.

[7] R. Sinaga, “Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO 27001:2022,” *J. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 3, pp. 381–394, 2024, doi: 10.28932/jutisi.v9i3.6850.

[8] F. Rifai, M. Jazman, Angraini, and Megawati, “Design Of Application Information Security Self-Assessment Using VBA AND MSXML2.XMLHTTP Case Study: Diskominfo Kabupaten Kampar,” *J. Tek. Inform.*, vol. 4, no. 6, pp. 1523–1534, 2023.

[9] F. A. A. Setyoso, R. Mulyana, and R. A. Nugraha, “Utilizing ISO 27001 : 2022 In Information Security Design For BPRCCo SME Digital Transformation,” *J. Multidiscip. Res. Dev.*, vol. 6, no. 6, pp. 2544–2553, 2024.

[10] D. I. Khamil, “Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 dan ISO/IEC 27001:2013 (Studi Kasus : Diskominfo Kabupaten Gianyar),” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 3, pp. 1948–1960, 2022, doi: 10.35957/jatisi.v9i3.2310.

[11] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, “Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022,” *J. SAINTEKOM*, vol. 14, no. 1, pp. 84–94, 2024, doi: 10.33020/saintekom.v14i1.623.

[12] I. N. A. A. Wibawa, A. A. N. H. Susila, and M. A. Pasirulloh, “Information Security Evaluation at Hospital Using Index KAMI 5 . 0 and Recommendations Based on ISO / IEC 27001 : 2022,” *J. Inf. Syst. Informatics*, vol. 6, no. 4, pp. 3070–3086, 2024, doi: 10.51519/journalisi.v6i4.949.

[13] R. N. Akmal, D. D. Susilo, and E. H. Rouf, “Evaluasi Keamanan Sistem Informasi Rumah Sakit : Metode Pengujian ISO 27001 di RS Khusus Mata Purwokerto,” *J. Indones. Manaj. Inform. dan Komun.*, vol. 6, no. 1, pp. 560–569, 2025.

[14] Evariani, M. I. Herdiansyah, E. S. Negara, and T. Sutabri, “Sistem Di Sekolah Tinggi Ilmu Kesehatan Bina Husada Menggunakan Indeks-Kami,” *Djtechno J. Teknol. Inf.*, vol. 6, no. 1, pp. 219–236, 2025, doi: 10.46576/djtechno.

[15] A. R. Riswaya, A. Sasongko, and A. Maulana, “Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks Kami Untuk Persiapan Standar Sni Iso/Iec 27001 (Studi Kasus: Stmik Mardira Indonesia),” *J. Comput. Bisnis*, vol. 14, no. 1, pp. 10–18, 2020.

[16] M. F. Husin, H. . Wowor, and S. D. . Karouw, “Implementasi Indeks Kami Di Universitas Sam Ratulangi,” *J. Tek. Inform.*, vol. 12, no. 1, 2017.

[17] H. H. R. H. Ananza, I. Darmawan, and R. Mulyana, “Perancangan Tata Kelola Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) Menggunakan Standar ISO 27001:2013 (Studi Kasus : Diskominfotik Kabupaten Bandung Barat),” *e-Proceeding Eng.*, vol. 6, no. 2, p. 8368, 2019.

[18] F. A. Basyarahil, H. M. Astuti, and B. C. Hidayanto, “Evaluasi Manajemen Keamanan Informasi pada DPTSI ITS Surabaya,” *J. Tek. Its*, vol. 6, no. 1, pp. 122–128, 2017, [Online]. Available: https://www.neliti.com/publications/193043/evaluasi-manajemen-keamanan-informasi-menggunakan-indeks-keamanan-informasi-kami

[19] H. A. Pratiwi and L. Wulandari, “Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor,” *J. Ind. Eng. Manag. Res.*, vol. 2, no. 5, pp. 146–163, 2021, [Online]. Available: https://www.jiemar.org/index.php/jiemar/article/view/196

[20] N. D. Ramadhani, W. H. N. Putra, and A. D. Herlambang, “Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 5, pp. 1490–1498, 2020, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/7259

[21] G. D. S. Barani, W. H. N. Putra, and B. S. Prakoso, “Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami (Keamanan Informasi) 4.0 (Studi Kasus: Dinas Komunikasi Dan Informatika Provinsi Jawa Timur),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 9, pp. 3218–3224, 2020, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/download/7922/3722

[22] Y. D. Wijaya, “Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) Iso/Iec 27001:2013,” *J. Sist. Inf. dan Inform.*, vol. 4, no. 2, pp. 115–130, 2021, doi: 10.47080/simika.v4i2.1178.

[23] R. Sinaga and F. Taan, “Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala,” *Nuansa Inform.*, vol. 18, no. 2, pp. 46–54, 2024, doi: 10.25134/ilkom.v18i2.205.

[24] I. P. S. Syahindra, C. Hetty Primasari, and A. Bagas Pradipta Iriantor, “Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi Xyz Menggunakan Indeks Kami Dan Iso 27005 : 2011,” *J. Teknoinfo*, vol. 16, no. 2, p. 165, 2022, doi: 10.33365/jti.v16i2.1246.