Vol. 8, No. 4, August 2026

Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

A Socio-Technical Assessment of Information Security Management Using KAMI Index, ISO/IEC 27001:2022, and User Awareness

Nur Wachid Hidayatulloh[1], Dinar Mutiara Kusumo Nugraheni[2], Oky Dwi Nurhayati[3]

[1]Master of Information System, Postgraduate School, Diponegoro University, Semarang, Indonesia
[2]Informatics Department, Faculty of Sciences and Mathematics, Diponegoro University, Semarang, Indonesia
[3]Computer Engineering Department, Faculty of Engineering, Diponegoro University, Semarang, Indonesia

Received:
February 6, 2026
Revised:
June 27, 2026
Accepted:
July 22, 2026
Published:
August 22, 2026

Corresponding Author:
Author Name*:
Nur Wachid Hidayatulloh
Email*:
nwachid5833@gmail.com

DOI:
10.63158/journalisi.v8i4.1746

Abstract. ISO/IEC 27001:2022 is one of the certifications for Information Security Management Systems (ISMS). The study employs a mixed descriptive approach, analyzing maturity using the KAMI Index 5.0, ISO/IEC 27001:2022 clause implementation as a gap assessment, and user awareness of the ISMS, examined through socio-technical system theory at a university in Semarang. The results reveal a gap between the two subsystems: the technical subsystem shows high overall readiness but is not fully optimal, with weaker domain in Personal Data Protection (level II). The KAMI Index places the university's overall maturity at level V, while the ISO/IEC 27001:2022 gap assessment shows several clauses still unimplemented. Meanwhile, the social subsystem for user awareness revealed that the ISMS was less than optimal according to user interviews, even though the test achieved a score of 81.2% and was rated Very Worthy. Suitable standard operating procedures (SOPs) were also found lacking for several clauses and indicators. Socio-technical systems theory emphasizes joint consideration of social and technical elements in designing and implementing complex organizational systems such as information security; applying it here shows both subsystems must be evaluated holistically rather than separately.

Keywords: KAMI Index, ISO/IEC 27001:2022, IT Awareness, Socio-Technical System, ISMS

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

1. INTRODUCTION

In the current digital era, many digital platforms have developed and are used in various sectors. One sector that utilizes digital platforms is the education sector, from elementary to higher education in Indonesia. The existence of the various digital platforms indicates that a large amount of user data, especially from the Indonesian public, has been managed. In contrast to the abundance of these platforms, anomalous traffic attacks continue to occur in Indonesia. A report from the National Cyber and Crypto Agency (BSSN) stated that Indonesia experienced a total of 330,527,636 anomalous traffic attacks during 2024 [1]. Furthermore, the report explained that investigations to identify cyber incidents revealed 241 suspected data leaks, with 56,128,160 suspected data exposures on the darknet [1].

Based on reports related to anomalous traffic attacks and the discovery of data exposure that occurred in Indonesia, it can be seen that several agencies in Indonesia have deficiencies in maintaining IT awareness, especially in the implementation of the Information Security Management System (ISMS). IT awareness, also known as information technology awareness, is a way to motivate individuals to take preventative measures by creating vigilance or awareness of all possible lurking threats [2]. Meanwhile, information security is defined as the protection of information assets, including systems and devices, from various threats in order to ensure business continuity, minimize damage caused by threats, and accelerate return on investment and opportunities [3]. These two aspects relate to information security when applying IT awareness, which can be achieved through the implementation of various control instruments and policies or procedures [4].

The ISO/IEC 27001:2022 family is one of the standards that can be used to determine the implementation of the ISMS or Information Security Management System (ISMS) [5]. The ISO/IEC 27001:2022 family itself is an international standard for managing information security and was developed by the International Organization for Standardization (ISO) [6]. With ISO/IEC 27001:2022 certification, an agency can provide and serve users safely, recognize an attack, protect a system, recognize and respond to attacks, repair attacks that occur [7], and determine potential security with security standards and aim to minimize the risk of attacks that occur [8]. In addition, with the implementation or

certification of ISO/IEC 27001:2022, an agency can maintain and build relationships among business partners and foster trust among users in using the services provided [9]. Furthermore, based on observations, two universities have been found to have ISO/IEC 27001:2022 certification in Indonesia for their information security management systems. The first university, Telkom University, achieved ISO/IEC 27001:2022 certification for its Data Center and LMS through an audit conducted by the British Standards Institution (BSI) Indonesia [10]. The second university, Mercu Buana University, Yogyakarta, achieved ISO/IEC 27001:2022 certification for its web-based academic information system application management by the ICT Bureau through TUV Nord Indonesia [11].

When it comes to standardization, the National Cyber and Crypto Agency (BSSN) also has a national standard for measuring maturity levels, namely the Information Security Index (KAMI) [12]–[14]. In addition to measuring maturity levels, the KAMI Index can also be used to determine a company or organization's readiness to obtain ISO/IEC 27001:2022 [15]–[17]. However, when discussing IT awareness, we are not only talking about the technical aspects within an organization but also looking at the social side, namely user awareness. This is consistent with sociotechnical system theory, which states that good governance, ethical practices, and sociocultural beliefs shape and are shaped by technical performance and clinical workflows [18].

A socio-technical system (STS) is a system that involves complex interactions between humans (social components), machines (technical components), and the environmental components of a socio-technical work system [19]–[21]. Another opinion, from Emery (2000) in [22], states that STS, formally referred to as "Joint Optimization," essentially means equal consideration of human and technical elements in the development or redesign of socio-technical systems. Joint optimization refers to the process of achieving optimal conditions for the benefit of the entire system, rather than optimizing a single subsystem [22].

Several studies have been conducted using ISO/IEC 27001:2022 [2], [23]–[25] and the KAMI Index [13], [17], [26], [27]. These include studies using ISO/IEC 27001:2022:2013 and those using the older version of the KAMI Index. Furthermore, other similar studies using ISO/IEC 27001:2022 and the KAMI Index separately also failed to link the user awareness, particularly the socio-technical system, in the preparation and evaluation of ISMS.

Furthermore, this study combines the KAMI Index version 5, ISO/IEC 27001:2022, with the user awareness, which is reviewed based on socio-technical system theory.

Based on the explanations and gaps identified above, this study introduces a novel approach to examining information security management systems by applying a mixed-method descriptive analysis that integrates the KAMI Index, ISO/IEC 27001:2022, and user awareness through a socio-technical systems framework. PQR University was selected as the single case study site because observations revealed that this university does not yet have ISO/IEC 27001:2022 certification and there are very few universities as a higher education level that have ISO/IEC 27001:2022 certification. The socio-technical system perceptions used in this study were to determine the relationship between the technical sub-criteria of the KAMI Index and ISO/IEC 27001:2022, as well as the social sub-criteria of user awareness. ISO/IEC 27001:2022, as the international standard for information security management, and the KAMI Index, which determines the maturity level of the university, were used in this study.

2. METHODS

2.1. Research Procedure

Research procedures are the steps taken to solve problems in a study. The research procedures used in this study are shown in Figure 1. Based on the Figure 1, the procedure in this study begins with a literature study. This initial stage is to understand the KAMI Index and ISO/IEC 27001:2022, both in terms of theory and similar research to identify differences. The next stage is to conduct testing by analyzing the SOPs implemented by universities related to ISMS based on the KAMI Index indicators. The third stage is still the same as analyzing the SOPs implemented by university related to ISMS, only using clauses in ISO/IEC 27001:2022. The fourth stage is to analyze the user awareness regarding ISMS at universities. Finally, this study will produce a level of maturity, clause suitability, and feasibility from the user awareness regarding ISMS, which will then be concluded as influencing factors on IT awareness. Next, we obtain factors in IT awareness, reviewed from the sociotechnical system perception, taken from the technical sub-section through the KAMI Index and ISO/IEC 27001:2022, and the social sub-section from the user awareness results to determine the optimal level of the two sub-sections. This is because designing, optimizing, or implementing complex systems requires a

combination of social and technical subsystems and cannot be considered separately [30].

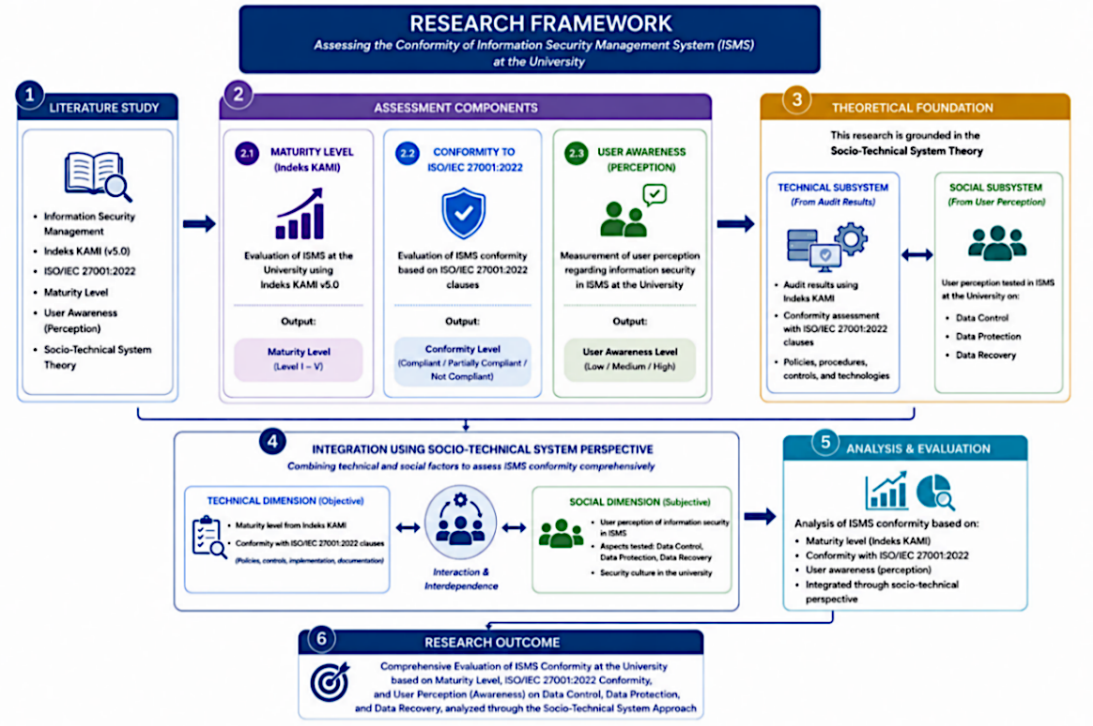

Figure 1. Research Procedure

2.2. Research Subjects

The research subject in this study is the information security management system evaluated based on ISO/IEC 27001:2022 and the KAMI Index. This evaluation was conducted a single case study the university in Semarang, namely PQR University. The selection of university was aimed at knowing the governance carried out by the university based on the research of [8] which focused on researching 1 university, and after observing the website pages of each university there was no information regarding the existence of ISO/IEC 27001:2022 certification. In addition to observing the university PQR websites, the selection of PQR universities as research locations and subjects was based on the small number of universities certified by ISO/IEC 27001:2022. In Indonesia, only Telkom University [10] and Mercu Buana University Yogyakarta [11] have ISO/IEC 27001:2022 certification, and PQR university were not included as research locations. Furthermore, the research subjects were classified into 3 subjects from each university from the research of [8] namely IT staff, educators (lecturers), and students.

2.3. Data Collection

Several data collection techniques were used in this study, including literature review, interview, observation, and questionnaires.

1) Literature review: This study was conducted by reading and understanding all publications related to the implementation of ISO/IEC 27001:2022, as well as all publications on the implementation of the KAMI Index related to determining maturity levels at universities.
2) Interview: This study was conducted by collecting data from 10 questions asked of IT departments at universities regarding ISO certification and the implementation of information security management systems. This interview with the head of IT was aimed at finding out the SOP and implementation of the ISMS that is applied at the university as a form of IT awareness. The 10 questions covered three topic areas: (1) existing ISMS governance and SOPs, (2) the university's ISO/IEC 27001:2022 certification status and plans, and (3) technical and organizational measures already in place. Interview responses were analyzed qualitatively through descriptive summarization and were cross-checked against the SOP documents provided by ICT Unit, which were then used to verify and triangulate the KAMI Index assessment and the ISO/IEC 27001:2022 gap assessment.
3) Observation: This study conducted observations to collect data related to the implementation and availability of ISO/IEC 27001:2022 certification at universities in Indonesia.
4) Questionnaires: This study consisted of two questionnaires. The first questionnaire, the KAMI Index version 5.0 and ISO/IEC 27001:2022, was addressed to the Head of the ICT Unit who is directly responsible for the flow of information security management performance at PQR University. This questionnaire was intended to assess the implementation of information security management at university. Meanwhile, the ISO/IEC 27001:2022 indicators were assessed using a modified questionnaire from [28] as an informal assessment. A second questionnaire was then administered to IT staff, educators and students regarding their perceptions of the importance of information security management at the university. The second questionnaire for users used indicators according to [29], including: data control, data management, and data recovery, distributed to 150 users. 14 collected

questions that have been adjusted from 3 indicators and then a reliability test was carried out. Content validity of these 14 items was established by adapting them directly from the established IT audit and information-security indicators in [29], a widely used professional reference; item wording was adjusted to fit the university ISMS context while preserving the original indicator constructs. The sample size was selected based on research conducted by [23]. A total of 150 users were distributed among IT staff, students, and educators. The students in question were undergraduates at the university, while the educators were active lecturers. The number of respondents was 10 lecturers, 5 IT staff, and the remainder were students.

2.4. Data Analysis Technique

Mixed method descriptive analysis was used in this study. This analysis was used to classify the results obtained from the evaluation based on the KAMI Index to measure the maturity level and readiness of the information security management system with ISO/IEC 27001:2022, user awareness perspective for ISMS also the socio-technical system framework as explained below.

2.4.1. Maturity Level with KAMI Index

The KAMI Index here, besides measuring the maturity level, will also be validated by how the SOP implemented by the university regarding ISMS is implemented. The analysis conducted to measure the maturity level of the Information Security Management System (ISMS) is based on the KAMI Index indicators assessment that used are I – Electronic System Category, II – Information Security Governance, III – Information Security Risk Management, IV – Information Security Management Framework, V - Information Asset Management, VI – Information Technology and Security, and VII – Personal Data Protection [15]. For determining maturity levels with the KAMI Index is categorized into 5 that explained in Table 1.

Table 1. KAMI Index Category for Maturity Level

Maturity Level	Category
I	Initial conditions
II	Implementation of the basic framework

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Maturity Level	Category
III	Defined and consistent
IV	Managed and measurable
V	Optimal

Each answer collected in the first category is assigned a score, which is then consolidated to produce an index number and used to display the evaluation results in the dashboard at the end of this process. The scores assigned to the questions according to their maturity level refer to Figure 2.

Security Status	Security Category		
	1	2	3
Not Implemented	0	0	0
In Planning	1	2	3
Partially Implemented or Being Implemented	2	4	6
Fully Implemented	2	4	6
Dity Implemented	3	6	9

Figure 2. KAMI Index Readiness Status

After completing all the KAMI Index questionnaires, the two KAMI Index groupings were then mapped in Figure 3 to provide two distinct perspectives: the level of security comprehensiveness and the level of security maturity. Respondent agencies can use these metrics as targets for their information security programs.

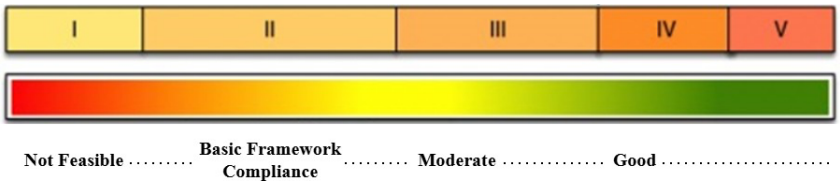

Figure 3. Range of security maturity and completeness levels [15]

Based on Figure 3 the range of security maturity have several categories that are Not Feasible for Level 1, Basic Framework Compliance for maturity in Level 2, Moderate for the maturity in Level 3, and Good when the security maturity in Level 4 to Level 5.

2.4.2. ISO/IEC 27001:2022 Assessment

Qualitative analysis of the ISO/IEC 27001:2022 testing was collected based on responses collected through the provided questionnaire by [28] and summarized to obtain the number of questions "Applied", "Not Applied", and "Other Comments" also this toolkit is for the informal assessment by the ISO27001 Forum. Evaluation with this toolkit is conducted by filling out the existing questionnaire with the answer "Applied" if the clause is implemented in the ISMS, "Not Applied" if the clause is not implemented at all at the university, and "Other Comments" if the clause is implemented with another implementation or is planned to be implemented. Furthermore, this evaluation is also validated with the SOP provided or implemented by the university. In addition to obtaining a summary of answers, the analysis was also carried out by providing recommendations that need to be implemented by the university regarding non-compliant implementations based on clauses 4-10 and Annex A Control of ISO/IEC 27001:2022.

2.4.3. User Awareness

A qualitative analysis to determine the feasibility of information security management disseminated to educators and students was measured using a Likert Scale [31]. The Likert Scale was chosen to gather feedback and opinions from users [16] and ensure accurate measurement of attitudes [13]. Table 2 shows the Likert Scale used.

Table 2. Likert Scale

Maturity Level	Category
5	Strongly agree (SS)
4	Agree (S)
3	Neutral (N)
2	Disagree (TS)
1	Strongly disagree (STS)

Next, calculations were carried out to determine user perceptions from lectures, IT staff and students. Calculations were carried out using Formula (1) as the total score and Formula (2) as the test percentage from [32] as follows.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

$$\sum Score = (J_{sts} \times 1) + (J_{ts} \times 2) + (J_n \times 3) + (J_s \times 4) + (J_{ss} \times 5) \quad (1)$$

Where Jsts = Number of responses from respondents who chose strongly disagree, Jts = Number of responses from respondents who chose disagree, Jn = Number of responses from respondents who chose neutral, Js = Number of responses from respondents who chose agree, Jss = Number of responses from respondents who chose strongly agree.

Next is to calculate the percentage of the total score using the following Formula (2)

$$Percentage = \frac{\sum score}{i \times r \times 5} \times 100\% \quad (2)$$

Where $\sum$ score = Calculation result of the total score of respondents' answers, i = Number of questions, r = Number of respondents.

After getting the percentage, continue with the conversion from Table 3 which was modified from [33].

Table 3. Conversion of Percentage

Range of Percentage	Category
0% - 25%	Very unworthy
26% - 50%	Not worthy
51% - 75%	Worthy
76% - 100%	Very worthy

Next, the consistency or reliability of the instrument was calculated using Cronbach's Alpha with SPSS. The interpretation of reliability is shown in Table 4.

Table 4. Cronbach's Alpha Interpretation [34]

Cronbach's Alpha	Interval Consistency
$\propto \geq .9$	Excellent
$.9 \geq \propto \geq .8$	Good

Cronbach's Alpha	Interval Consistency
$.8 \geq \propto \geq .7$	Acceptable
$.7 \geq \propto \geq .6$	Questionable
$.5 > \propto$	Unacceptable

3. RESULTS AND DISCUSSION

3.1. ISMS (Information Security Management System) in University

The Information Security Management System (ISMS) at a university in Semarang has been evaluated and is currently in the development stage. This finding was obtained after a direct interview with the Head of the Information and Communication Technology Unit (ICT Unit) at PQR University in Semarang. He stated that several steps have been taken to improve information security management at PQR University, including training and security workshops for existing human resources, and the implementation of a firewall subscription on the device side. Furthermore, the university has implemented simple standard operating procedures (SOPs) and a legal basis for information security management. These legal bases include Law No. 27 of 2022 concerning Personal Data Protection, the Electronic Information and Transactions Law (UU ITE), and standards established by the National Cyber and Crypto Agency (BSSN). In addition to these legal frameworks, the university also has 52 standard operating procedures (SOPs) for data management at the ICT Unit.

Regarding the Head of ICT's view on ISO/IEC 27001:2022 certification, the Head of ICT stated that the implementation of ISO/IEC 27001:2022 itself has not yet been implemented but is currently underway and under development. The reason for not having ISO certification is the desire to focus on developing human resources, particularly in information security management. This is because data at PQR University is currently very important to protect, such as employee and student data.

3.2. KAMI Index Evaluation

Testing with the KAMI Index was conducted at PQR University in Semarang. The results of this test can be seen in Figure 4. In addition to the test results in Figure 4, there are

also category labels for the test results which can be seen in Figure 5. Based on the results of Figure 4 and Figure 5, it is known that PQR University in Semarang has an SE (Electronic System) category in a strategic condition where it gets a test score of 44. This result is also supported by the testing of other indicators related to compliance with ISO/IEC 27001:2022. The overall results related to compliance with ISO/IEC 27001:2022 with the KAMI Index at this university are in a "Good" condition where it gets a score of 910 out of a total score of 918.

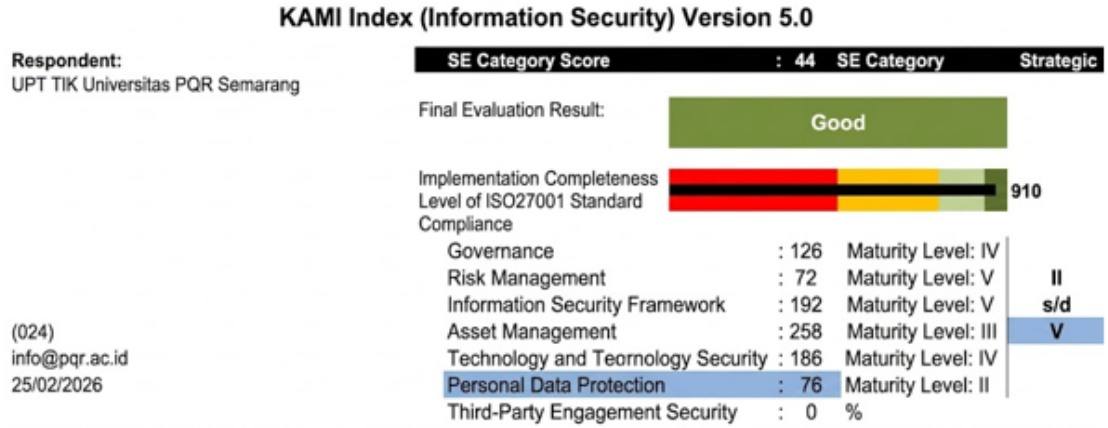

Figure 4. Result of KAMI Index Assessment

Figure 5. KAMI Index Testing Category Level

In addition to the total score of ISO/IEC 27001:2022 compliance using the KAMI Index, based on Figure 4, the maturity level at PQR University in Semarang is also at level V. This level is based on several existing test indicators, including:

1) Indicator II - Information Security Governance: PQR University scored 126 out of 126 and achieved a maturity level of IV. When converted to Table 1, this maturity level is "Managed and Measured";
2) Indicator III - Information Security Risk Management: PQR University scored 72 out of 72 and achieved a maturity level of V. When converted to Table 1, this maturity level is "Optimal";
3) Indicator IV - Information Security Management Framework: PQR University scored 192 out of 192 and achieved a maturity level of V. When converted to Table 1, this maturity level is "Optimal";
4) Indicator V - Information Asset Management: PQR University scored 258 out of 258 and achieved a maturity level of III. This maturity level, when converted to Table 1, is at the "Defined and Consistent" level;
5) Indicator VI - Information Technology and Security: PQR University scored 186 out of a total score of 186, ranking it at a maturity level of IV. When converted to Table 1, this maturity level is at the "Managed and Measurable" level;
6) Indicator VII - Personal Data Protection (PDP): PQR University scored 76 out of a total score of 84, ranking it at a maturity level of II. When converted to Table 1, this maturity level is at the "Implementation of the Basic Framework" level;
7) Indicator VIII - Supplement: PQR University was not tested, resulting in a score of 0%. This is because, after consulting the Head of the ICT Unit, PQR University independently manages information security management, particularly the management of its applications and websites.

Based on the analysis of the results, it was found that the information management implemented by PQR University in Semarang complies with ISO/IEC 27001:2022. However, several indicators remain poorly documented, including the lack of SOPs for the KAMI Index. Several indicators have been implemented and have SOPs, including indicators 2.6, 2.7, 3.1, 5.1, 5.11, 5.20, 5.22, 5.26, 5.48, and 6.3. Furthermore, the results also revealed that indicators II-Governance, V-Asset Management, and VI-Technology achieved maximum scores in the testing but did not yet reach an optimal maturity level. This is because the questions tested in the KAMI Index only reached security level IV for indicators II-Governance and VI-Technology Based on Figure 2. Meanwhile, in indicator V-Asset Management, the KAMI Index only tested questions up to security level III based on Figure 2 for readiness question. The university's test for indicator VII-PDP received a score of

76 out of a total of 84. This result is due to several indicators having a testing status of "In Implementation/Partially Implemented." These indicators are 7.2, 7.3, 7.14, 7.15, and 7.16. Furthermore, Based on Figure 2 for readiness status, indicator VII only tests questions up to maturity level III.

3.3. ISO/IEC 27001:2022 Evaluation

Testing with ISO/IEC 27001:2022 was conducted using a toolkit tested at PQR University in Semarang. The results of the ISO/IEC 27001:2022 test can be seen in Figure 6 below.

ISO/IEC 27001:2022 Gap Analysis Questionnaire - Answer Summary

	Yes	No/Not Applicable	Other Comments
ISO/IEC 27001:2022 Clause (28 questions)	25	1	2
ISO/IEC 27001:2022 Annex A Controls (133 questions)			
Domain 5 - Organizational Controls (66 questions)	61	2	3
Domain 6 - People Controls (15 questions)	14	0	1
Domain 7 - Physical Controls (14 questions)	14	0	0
Domain 8 - Technological Controls (38 questions)	38	0	0

Figure 6. ISO/IEC 27001:2022 Assessment

Based on the test results in Figure 6, it is known that of the 28 questions in Clauses 4-10 and 133 questions for Annex A Control in ISO/IEC 27001:2022, there are several clauses that have not been implemented, amounting to 3 and several clauses with the filling of "Other Comments" amounting to 6. Evaluation with the toolkit is conducted by filling out the existing questionnaire with the answer "Yes" if the clause is implemented in the ISMS, "Not Applied" if the clause is not implemented at all at the university, and "Other Comments" if the clause is implemented with another implementation or is planned to be implemented. Each "Yes" response was counted as one implemented clause/control, each "Not Applied" response was counted as one gap, and each "Other Comments" response was counted separately to indicate partial or alternative implementation; the toolkit then automatically summed these counts and converted the number of "Yes" responses into a percentage of the total 161 clauses and controls to obtain the overall ISO/IEC 27001:2022 implementation rate.

The clause that has not been implemented or does not apply to information security management for this university was shown in Table 5 with the practical implication.

Table 5. Unimplemented ISO/IEC 27001:2022 Clauses with The Practical Implication

Clauses	Requirement	Practical Implication
Clause 7.3 a	Personnel shall be aware of the information security policy	Employees may not fully understand the organization's information security policy, leading to inconsistent implementation of security practices and increased human-related security risks.
Control 5.1 a	An information security policy shall be established, approved, published, and communicated	Without formal communication and approval, security policies may not be consistently understood or applied across the organization.
Control 5.9 f	Asset inventory should include relevant ownership and management information.	Incomplete asset records may cause difficulties in asset protection, accountability, and risk assessment, increasing the likelihood of unmanaged security incidents

Furthermore, questions with the answer "Other Comments" are found in clauses 6.1c and 7.5b, while the control clauses that get this answer are in clauses 5.7b, 5.7c, 5.30b, and 6.7b. In addition to the test results, comments added to the test for the 6 clauses that received the answer "Other Comments" can be seen in Table 6 for the Mandatory Clauses of ISO/IEC 27001:2022 and Table 7 for the Control Clauses of Annex A in ISO/IEC 27001:2022.

Table 6. Comments that Given in Mandatory Clauses

Clause(s)	Comments
6.1c	Currently it is not implemented for SoA creation in the university

Clause(s)	Comments
7.5b	The documented information required by ISO/IEC 27001:2022 has not yet been directly implemented

Table 7. Comments that Given in Control Clauses

Clauses (s)	Category
5.7b	The management carried out is identifying risks, analyzing impacts and possibilities, determining risk treatment, and documenting the result
5.7c	The management carried out is to encourage the use of relevant intelligence sources
5.30b	Business Impact Analysis (BIA) in ICT Unit is currently not running
6.7b	The security measures taken for remote work include the availability of a remote working policy and provisions for the use of devices and networks outside the office

In addition to the test results obtained from the questionnaire, the test also revealed that there are still several clauses that do not have documentation such as SOPs, especially in carrying out information security management based on the ISO/IEC 27001:2022 test. The clause that already has an SOP in clauses 4-10 of ISO/IEC 27001:2022 is clause 5.3a regarding the establishment of a mechanism for communicating responsibilities and authorities for relevant roles. Meanwhile, the control clauses of Annex A in ISO/IEC 27001:2022 that have SOPs include clauses 5.9a, 5.9b, 5.9c, 5.9d, 5.9e, 5.9f, 5.10a, 5.10b, 5.10c, 5.11a, 5.11b, 5.15b, 5.16, 5.17a, 5.17c, 5.17d, 5.18a, 5.18b, 5.21, 5.22, 5.23a, 5.27, 5.28, 5.29, 5.30a, 5.33a, 6.1a, 6.1b, 61c, 6.6b, 6.6c, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 7.10, 7.11, 7.13, 7.14, 8.1, 8.2, 8.3, 8.5, 8.8a, 8.8b, 8.11, 8.12, 8.13, 8.15, 8.16a, 8.16b, 8.20, 8.22, and clause 8.31.

3.4. User Awareness

The test results were administered to 150 users at PQR University. A summary of the test results can be seen in Table 8.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Table 8. Result of User Awareness

Declaration	Total
Number of questions	14
Jsts	4
Jts	33
Jn	301
Js	1257
Jss	505

After obtaining the summary results in Table 8, the next step is to calculate the total test score using Equation (1), followed by Equation (2) to determine the percentage of the test results. The calculation using Formula (1) is as follows.

$$\sum Score = (J_{sts} \times 1) + (J_{ts} \times 2) + (J_n \times 3) + (J_s \times 4) + (J_{ss} \times 5)$$
$$\sum Score = (4 \times 1) + (33 \times 2) + (301 \times 3) + (1257 \times 4) + (505 \times 5)$$
$$\sum Score = 8526$$

After getting the total test score, the next step is to calculate it using Equation (2) to find out the test percentage results.

$$Percentage = \frac{\sum score}{i \times r \times 5} \times 100\%$$
$$Percentage = \frac{8526}{14 \times 150 \times 5} \times 100\%$$
$$Percentage = 81.2\%$$

Based on the result concluded the overall user awareness percentage result is 81.2% This percentage was then classified using Table 3 to determine the worthy of the ISMS at PQR University in Semarang from a user awareness. The classification results indicate that the ISMS at PQR University is "Very Worthy." In addition to the overall ISMS worthy results, percentages were also calculated for each question category tested. The

percentages for each category were calculated using Formulas (1) and (2). The percentages for each category are presented in Table 9.

Table 9. Result of User Awareness Based on Category

Category	Percentage (%)
Data control	83.52
Data management	80.8
Data recovery	79.2

Based on the Table 9 for each question category, it is known that the "Data Recovery" category has the lowest percentage compared to the other two categories. This is supported by statements from several student respondents who stated that some respondents did not know how data recovery occurs at PQR University. In addition, data recovery carried out at the university was quite slow because several users found incidents when the university website was hacked and it happened for quite a long time, especially during the lecture week. Furthermore, on the "Data Protection" side, several student respondents also stated that data protection at PQR University is still considered inadequate. One example that makes students feel that data protection at this university is lacking is during exams, both mid-term and final exams are CBT, where each student is given a different username but with the same password for the entire class. This has happened to a friend of the respondent who had difficulty being able to take the exam under his own name because it could not be removed. Furthermore, on the "Data Control" side, the user awareness on the ISMS at PQR University is quite good. This is supported by statements from respondents from the lecturer side who stated that the data control process has been adjusted to the existing SOP and efforts to obtain certification have been made through courses presented in the informatics and information technology study program, namely cyber security. From the student side, it was also revealed that overall the data control process is good which is supported by several applications and systems owned by the university such as digital attendance that allows each student to scan a QR code for attendance, as well as e-learning in each faculty that can help lecturers upload assignments and materials and help students to view assignments and materials from lecturers through e-learning available in each different faculty. In addition

to the results based on the test categories on user awareness, there are also test results based on respondent categories shown in the Table 10.

Table 10. Result of User Awareness Based on Respondent Category

Respondent Category	Percentage (%)
Lecturer	78
IT Staff	81
Students	81.4

Based on Table 10 suggest that user awareness represents a supporting factor for ISMS implementation rather than a direct indicator of ISO/IEC 27001:2022 compliance. While lecturers, IT staff, and students exhibit high awareness of information security practices, full compliance with the standard also requires formal organizational policies, documented procedures, management commitment, and comprehensive asset management. Consequently, improvements should prioritize addressing the identified ISO gaps while maintaining continuous awareness programs for all user groups. After obtaining the percentage results, reliability testing was conducted using SPSS. The test results are shown in Figure 7.

Case Processing Summary

		N	%
Cases	Valid	150	100,0
	Excluded[a]	0	,0
	Total	150	100,0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
,863	14

Figure 7. Reliability Testing

The reliability of the user awareness questionnaire was evaluated using Cronbach's Alpha in IBM SPSS Statistics. As shown in Figure 7, all 150 respondents were included in the

analysis, with no missing or excluded data. The questionnaire consisted of 14 items, representing the dimensions of Data Control, Data Protection, and Data Recovery.

The reliability analysis produced a Cronbach's Alpha coefficient of 0.863, indicating that the questionnaire has good internal consistency by classified on Table 4 and stated that the reliability testing is Good. According to commonly accepted reliability criteria, a Cronbach's Alpha value above 0.80 demonstrates that the instrument is highly reliable and that the questionnaire items consistently measure users' information security awareness. Therefore, the questionnaire is considered suitable for assessing user awareness and provides reliable data for analyzing the human aspect of Information Security Management System (ISMS) implementation within the university.

3.5. IT Awareness Factors Reviewed Based on Socio-Technical System Theory

After gathering all the research results, the comparative results of all evaluations can be concluded in Table 11.

Table 11. Comparison of the Results

Evaluation Aspect	Method & Scope	Score / Result	Key Finding
Organizational Information Security Readiness	KAMI Index v5.0 (BSSN) — self-assessment across 5 work areas	910 (SE Category Score: 44)	Governance (Level IV) and Risk Management/Information Security Framework (Level V) are relatively mature; Asset Management (Level III) and Personal Data Protection (Level II) are the weakest areas; Third-Party Engagement Security is 0%.
Compliance with ISO/IEC 27001:2022	Gap Analysis Assessment — 161	152 of 161 implemented (94.4%); 9 gaps	The main gaps are in foundational documentation (SoA,

Evaluation Aspect	Method & Scope	Score / Result	Key Finding
	core clauses & Annex A controls		Clause 6.1c; Information Security Policy, Annex A 5.1a) and business continuity (BIA, Annex A 5.30b); also includes asset-ownership transfer (5.9f) and threat-intelligence sharing (5.7c).
User Information Security Awareness	User Testing — 150 respondents (10 Lecturers, 5 IT Staff, 135 Students), 14 items	Percentage result 81.2%	Data Control scored highest (83.52%); Data Protection (80.8%); Data Recovery scored lowest (79.2%), indicating that user understanding of recovery/continuity procedures still needs strengthening.

Based on Table 11, these result instruments in this study map onto this two-part model in a complementary way. The KAMI Index and the ISO/IEC 27001:2022 gap assessment both assess the technical subsystem — governance maturity, security framework, asset management, formal policies, procedures, and documented controls. The user-awareness test and the follow-up interviews are the only instruments that directly capture the social subsystem — what users actually know, experience, and report. This is where the most important pattern emerges: the technical subsystem is relatively mature overall (KAMI Index "Good"; ISO gap assessment 94.4% implemented), yet the social subsystem lags proportionally in specific areas, especially Data Recovery (79.2%, the lowest of the three awareness aspects). This is not coincidental. Where the technical subsystem produces no artifact for a given domain (e.g., no documented recovery procedure, no BIA corresponding to the Annex A 5.30b finding), the social subsystem has nothing to build awareness from, and the two subsystems fail together.

Meanwhile, the social subsystem, based on user awareness results, achieved a percentage of 81.2%. Users also reported that the university website had been hacked and that passwords for one class were used during the CBT Test. From the explanation of the two subsystems of the socio-technical system, gaps are clearly visible, and it can be said that these gaps are less than optimal in both the technical and social subsectors. In the technical subsector, there is a lack of implementation of SOPs for ISMS, and in the social subsector, there is still a feeling of inadequacy in user behavior. Furthermore, even if a high score is achieved in documentation or technical implementation, it does not necessarily translate to a high score in behavior in daily operations.

This illustrates how a gap in the technical subsystem propagates directly into a gap in the social subsystem — consistent with the STS principle that the two subsystems must be evaluated, and improved, jointly rather than in isolation. As stated by [30] designing, optimizing, or implementing complex systems requires a combination of social and technical subsystems and cannot be considered separately.

3.6. Recommendation for ISMS and The Simulation Schedule to Take ISO/IEC 27001:2022 Certification

Based on the existing test results, a priority matrix appears, which is displayed in Figure 8.

Risk Level	Immediate (0–1 month)	Short-term (1–3 months)	Long-term (3–6 months)
HIGH	• SoA not implemented (6.1c) • Information Security Policy not established (5.1a) • BIA not conducted (5.30b) • CBT shared-password incident (occurred) • Website defacement incident (occurred)	• Personal Data Protection systemic improvement (KAMI Index: Level II)	—
MEDIUM	—	• Policy socialization (Clause 7.3a) • Document control (Clause 7.5b) • Asset ownership transfer (Annex A 5.9f) • Remote-working security strengthening (Annex A 6.7b) • Data Recovery awareness module (after BIA is available)	• Asset Management maturity improvement (KAMI Index: Level III)
LOW	—	—	• Threat categorization (Annex A 5.7b) • Threat intelligence sharing (Annex A 5.7c) • Third-party / vendor governance framework (KAMI Index: 0%)

Figure 8. Priority Matrix for ISMS

Based on Figure 8 Incorporating the concrete incidents uncovered through the student interviews (the CBT shared-password issue and the website defacement) alongside the ISO/IEC 27001:2022 gap-assessment and KAMI Index findings. Items confirmed as actual, already-occurred incidents are elevated directly into the High risk / Immediate category, since an exploited weakness represents a materially greater priority than a theoretical or documentation-only gap. In addition to the priority matrix in Figure 8, there is an improvement roadmap for ISMS recommendations at universities, including:

1) Phase 1 — Access Control (Month 1)

In addition to the planned asset ownership transfer (5.9f), this phase now explicitly includes a comprehensive audit of the CBT system's authentication design (not just password resets) to ensure the principle of individual accountability is truly implemented across all academic systems, not just CBT.

2) Phase 2 — SOP Documentation (Months 1–2)

Substantially unchanged (SoA, Information Security Policy, document control), but now defacement and password sharing incidents are used as concrete case studies in policy development, so that the document is not abstract but refers to real-life incidents at the institution.

3) Phase 3 — Risk Assessment (Months 2–3)

Added a post-incident review process for both real-life incidents as formal input to the risk register—not just a generic threat categorization (5.7b), but a root cause analysis of the incidents that have already occurred.

4) Phase 4 — BIA (Months 3–4)

Unchanged — remains crucial because the BIA is a prerequisite for the Data Recovery training materials to be developed in Phase 5.

5) Phase 5 — Awareness Training (Months 4–5)

Now explicitly differentiates roles (Lecturer priority, not just a generic one for all), and includes CBT and defacement incidents as real-world examples in the materials — this approach closes the feedback loop failure identified in the STS analysis: existing user

awareness needs to be responded to by the organization, and real-world case-based training is one form of that response.

6) Phase 6 — Incident Response (Months 5–6)

In addition to strengthening remote working (6.7b), this phase now includes the development of formal incident response procedures based on lessons learned from website defacements, as well as the initial development of a vendor/third-party risk governance framework (KAMI 0%) — although this full framework can realistically continue beyond 6 months as a long-term initiative.

Furthermore, to support PQR University in obtaining ISO/IEC 27001:2022 certification, the researchers provided a simulation created using Primavera P6, which can be used as a recommendation for the university to obtain ISO certification. This is shown in Figure 9.

Activity ID	Activity Name	Planned Duration	Remaining Duration	Schedule % Complete	Start	Finish	Total Float
IT-001	ISO 27001 Certification	345	345	0%	04-Jan-27	28-Apr-28	0
IT-001.IT-001.1	Gap Assessment & Risk Analysis	63	63	0%	04-Jan-27	31-Mar-27	0
IT-001.IT-001.1.1.1	ISMS Implementation Socialization	15	15	0%	04-Jan-27	22-Jan-27	1
A1000	ISO 27001 Certification Plan	5	5	0%	04-Jan-27*	08-Jan-27	1
A1010	Reviewing Planning	5	5	0%	11-Jan-27*	15-Jan-27	1
A1020	Certification Program Approval	5	5	0%	18-Jan-27*	22-Jan-27	1
IT-001.IT-001.1.1.2	ISMS Team / Certification Team Formation	10	10	0%	25-Jan-27	05-Feb-27	0
A1030	Creating a Certification Team	4	4	0%	25-Jan-27*	29-Jan-27	1
A1040	Job description division for each team	5	5	0%	01-Feb-27*	05-Feb-27	0
IT-001.IT-001.1.1.3	Determining Certification Scope	7	7	0%	08-Feb-27	16-Feb-27	0
A1050	Determining the Programs to be Certified	7	7	0%	08-Feb-27*	16-Feb-27	0
IT-001.IT-001.1.1.4	Risk Assessment / Gap Analysis	31	31	0%	17-Feb-27	31-Mar-27	0
A1060	Assessing the Risks of ISMS	18	18	0%	17-Feb-27*	12-Mar-27	0
A1070	Determining the Gap	13	13	0%	15-Mar-27*	31-Mar-27	0
IT-001.IT-001.2	Policy Development & Implementation	67	67	0%	01-Apr-27	02-Jul-27	0
IT-001.IT-001.2.2.1	Policy Harmonization (SOP Alignment)	32	32	0%	01-Apr-27	14-May-27	0
A1080	SOP / Policies Alignment	32	32	0%	01-Apr-27*	14-May-27	0
IT-001.IT-001.2.2.2	Policy Implementation	35	35	0%	17-May-27	02-Jul-27	0
A1090	Implementing Policies in ISMS	35	35	0%	17-May-27*	02-Jul-27	0
IT-001.IT-001.3	Internal Audit & Management Review	75	75	0%	05-Jul-27	15-Oct-27	0
IT-001.IT-001.3.3.1	Internal Audit	25	25	0%	05-Jul-27	06-Aug-27	0
A1100	Conducting Internal Audits	25	25	0%	05-Jul-27*	06-Aug-27	0
IT-001.IT-001.3.3.2	Audit Finding Remediation	25	25	0%	09-Aug-27	10-Sep-27	0
A1110	Correcting Inappropriate Risk Findings	25	25	0%	09-Aug-27*	10-Sep-27	0
IT-001.IT-001.3.3.3	Management Review	25	25	0%	13-Sep-27	15-Oct-27	0
A1120	Reviewing the Findings	25	25	0%	13-Sep-27*	15-Oct-27	0
IT-001.IT-001.4	External Audit	125	125	0%	18-Oct-27	07-Apr-28	0
IT-001.IT-001.4.4.1	Operational Documentation Audit	45	45	0%	18-Oct-27	17-Dec-27	0
A1130	Reviewing the ISMS Document	45	45	0%	18-Oct-27*	17-Dec-27	0
IT-001.IT-001.4.4.2	Control Implementation Audit	35	35	0%	20-Dec-27	04-Feb-28	0
A1140	Reviewing Control Implementation	35	35	0%	20-Dec-27*	04-Feb-28	0
IT-001.IT-001.4.4.3	Finding Remediation (Post-Audit)	45	45	0%	07-Feb-28	07-Apr-28	0
A1150	Improving Audit Results	45	45	0%	07-Feb-28*	07-Apr-28	0
IT-001.IT-001.5	Certification Decision & Issuance	15	15	0%	10-Apr-28	28-Apr-28	0
IT-001.IT-001.5.5.1	Issuance of Certification	15	15	0%	10-Apr-28	28-Apr-28	0
A1160	Determination and Issuance of Certification	15	15	0%	10-Apr-28*	28-Apr-28	0

Figure 9. Schedule Simulation to Get ISO/IEC 27001:2022 Certification

Based on Figure 9, a simulation is provided to support PQR University in Semarang in obtaining ISO/IEC 27001:2022 certification. This implementation simulation starts from the stages of gap assessment and risk gap analysis, policy development and implementation, internal audit & management review, external audit until the decision and issuance of certification. At each stage of this simulation, there are still several more stages below. Within these stages or steps, it's also clear that there are different numbers of activities involved in each step. This difference in number is based on the length of the process required to obtain ISO/IEC 27001:2022 certification for the issues at hand. In addition, there is also a timeline that can be applied to all stages which can be seen in Figure 9. Figure 9 also shows that the simulation for implementing ISO/IEC 27001:2022 certification will begin in January 2027 and continue until April 2028. Figure 9 it just the schedule simulation for the university to get the certification and is not the validation certification plan.

3.1. Discussion

Based on research findings to determine the influencing factors on IT awareness for information security management in higher education, it was found that each university or college has its own SOP for managing the information security of the data they manage. This is indicated by the differences between the SOP obtained from Telkom University [35] and that of PQR University, a university in Semarang. Despite these differences, several regulations share common legal foundations, such as the PDP Law and the ITE Law.

Furthermore, the KAMI Index version 5.0 was used to determine the maturity level of PQR University. The results showed that PQR University has a maturity level of Level V, or Optimal. Despite this optimal level, many test indicators in the KAMI Index still lack appropriate documentation or SOPs. Furthermore, in indicator VII-PDP, several indicators are still "In Implementation/Partially Implemented" in information security management. These indicators are 7.2, 7.3, 7.14, 7.15, and 7.16.

In addition to testing with the KAMI Index, this study also conducted testing using the ISO/IEC 27001:2022 testing toolkit. This testing revealed several clauses, such as clause 7.3a, that had not been implemented, while control clauses, such as clause 5.1a and clause 5.9f, had not been implemented. Furthermore, clauses 6.1c and 7.5b received "Other

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Comments" in the test, while control clauses 5.7b, 5.7c, 5.30b, and 6.7b received this result. Not only the KAMI Index testing, but the ISO/IEC 27001:2022 testing also found that many clauses lacked appropriate documentation or SOPs.

In the user-facing feasibility test, PQR University received a score of 81.2%, categorized as "Very Worthy." Although the test result was declared "Very Worthy," several respondents felt the university's Information Security Management System (ISMS) needed improvement. From a user awareness, improvements include managing the university website to prevent similar incidents, such as being used as an online gambling site, and ensuring that passwords assigned to students are distinguishable to prevent other students from making mistakes when entering their usernames during the CBT exam.

When viewed from a socio-technical system perspective, indicate that the Information Security Management System (ISMS) at PQR University has a gap between the technical and social subsystems. The gap assessment results for the technical subsystem show that the KAMI Index achieved a maturity level of V – Optimal, and the university's ISMS conformity to the ISO/IEC 27001:2022 clauses is almost fully implemented. Meanwhile, the social subsystem, based on user awareness results, achieved a percentage of 81.2%. Users also reported that the university website had been hacked and that passwords for one class were used during the CBT. From the explanation of the two subsystems of the socio-technical system, gaps are clearly visible, and it can be said that these gaps are less than optimal in both the technical and social subsectors. In the technical subsector, there is a lack of implementation of SOPs for ISMS, and in the social subsector, there is still a feeling of inadequacy in user behavior. Furthermore, even if a high score is achieved in documentation or technical implementation, it does not necessarily translate to a high score in behavior in daily operations. This illustrates how a gap in the technical subsystem propagates directly into a gap in the social subsystem — consistent with the STS principle that the two subsystems must be evaluated, and improved, jointly rather than in isolation. As stated by [30] designing, optimizing, or implementing complex systems requires a combination of social and technical subsystems and cannot be considered separately. By applying sociotechnical systems, policymakers will see both areas holistically and cannot consider them separately when running systems in organizations, particularly university.

Meanwhile, managers, especially IT heads at universities, can implement the improvement roadmap that has been provided and see the priority matrix in Figure 8. And if the university wants to carry out ISO/IEC 27001:2022 certification as the simulation process, it can see Figure 9.

4. CONCLUSION

The conclusion of the research is that PQR University, one of Semarang's universities, does not yet have ISO/IEC 27001:2022 certification. Furthermore, the university does have SOPs for data management, particularly information security management. Overall, the findings indicate that PQR University has established a solid foundation for Information Security Management System (ISMS) implementation, as demonstrated by an overall KAMI Index v5.0 maturity level of V (Optimal), a high level of compliance with ISO/IEC 27001:2022 (94.4%), and a user awareness score of 81.2%. This overall readiness, however, is not uniform: domain-level weaknesses remain in Asset Management (maturity level III), Personal Data Protection (maturity level II), and Third-Party Engagement Security (0%), and several gaps remain in documentation, standard operating procedures (SOPs), and the implementation of specific ISO clauses and controls, including Clause 7.3(a), Control 5.1(a), and Control 5.9(f). The proposed certification schedule (Figure 9) is likewise a planning simulation intended to guide the university's roadmap, not a validated or audited certification plan. These findings suggest that achieving a high level of technical maturity and standard compliance does not automatically ensure effective security practices in daily operations. From a Socio-Technical System (STS) perspective, the identified discrepancies between the technical subsystem and user behavior highlight that effective ISMS implementation depends on the alignment of organizational processes, technology, and human behavior rather than on technical controls alone. This study therefore demonstrates that evaluating technical maturity together with user awareness provides a more comprehensive assessment of ISMS effectiveness and enables organizations to identify hidden gaps that may not be detected through technical audits alone. Consequently, universities should prioritize improving documentation, policy communication, asset management, and user awareness programs while implementing the proposed improvement roadmap and priority matrix. By integrating technical and social improvements simultaneously, higher education institutions can achieve more

sustainable ISMS implementation and strengthen their readiness for ISO/IEC 27001 certification.

This study has limitations, namely, its focus on only one university institution. Future research could conduct two or more studies to determine the level of information management maturity in a region. Furthermore, by understanding this level of maturity, researchers can also determine the extent to which the university implements the clauses in ISO/IEC 27001:2022. Beyond limitations, other researchers could also integrate socio-technical systems theory with other information security or user acceptance frameworks such as TAM, UTAUT, and others. In addition, subsequent research can conduct research with many universities to find out the implementation of ISMS at the higher education level and can use formal audit evidence.

REFERENCES

[1] BSSN, "Lanskap Keamanan Siber Indonesia 2024," *BSSN*, 2024.

[2] A. A. Ipungkarti, "Penerapan IT Security Awareness Standar Keamanan ISO 27001 di BPJS Ketenagakerjaan Kantor Cabang," *J. Media Infotama*, vol. 19, no. 1, pp. 103–110, 2023, doi: 10.37676/jmi.v19i1.3481.

[3] Yurindra, *Keamanan Sistem Informasi*. Yogyakarta: Deepublish Publisher, 2014.

[4] IBISA, *Keamanan Sistem Informasi*. Yogyakarta: Penerbit Andi, 2011.

[5] ISO/IEC, "International Standard ISO 27001:2022," 2022

[6] L. N. Amali, M. R. Katili, S. N. Lahay, and M. H. Koniyo, *Audit of Information System*. Banyumas: Arta Media Nusantara, 2023.

[7] E. Ceko, "A Quality Managerial Approach on The Relationship Between The Digital Development," *CIT Rev. J.*, vol. May, no. 2024, pp. 10–19, 2024, doi: 10.59380/crj.vi5.5106.

[8] B. Ahmedi and A. Ibrahimi, "Mastering Information Security Through Standard Implementation," *Int. J. Informatics Commun. Technol.*, vol. 13, no. 3, pp. 428–435, 2024, doi: 10.11591/ijict.v13i3.pp428-435.

[9] A. de F. Fernandes, F. C. Santiago de Brito, F. F. Priard, G. A. V. Matias, M. S. Goncalves, and R. G. B. Filho, "The ISO 27000 Family and its Applicability in LGPD Adaptation Projects for Small and Medium-Sized Enterprises," in *ICSEA 2021: The Sixteenth International Conference on Software Engineering Advances*, 2021, pp. 43–49.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[10] IKU, "Telkom University Raih Sertifikasi ISO 27001:2022 untuk Data Center dan LMS," 2025.

[11] UMBY, "UMBY, Satu-satunya Perguruan Tinggi Tersertifikasi Keamanan Informasi," 2024.

[12] F. Wijayanti, D. I. Sensuse, A. A. Putera, and A. Syahrizal, "Assessment of Information Security Management System: A Case Study of Data Recovery Center in Ministry XYZ," in *2020 3rd International Conference on Computer and Informatics Engineering, IC2IE 2020*, 2020, pp. 393–398. doi: 10.1109/IC2IE50715.2020.9274574.

[13] F. N. Shakti and A. N. Hidayanto, "Measurement of Employee Information Security Awareness: Case Study at Financial Institution," *JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer)*, vol. 9, no. 2, pp. 172–179, 2024, doi: 10.33480/jitk.v9i2.4163.

[14] R. Savitri and M. S. Hasibuan, "Information Security Measurement using KAMI Index at Metro City," *J. Appl. Data Sci.*, vol. 5, no. 1, pp. 33–45, 2024, doi: 10.47738/jads.v5i1.152.

[15] BSSN, "Indeks Keamanan Informasi (KAMI) versi 5.0," 2023

[16] W. A. Prabowo, "Developing Compliant Audit Information System for Information Security Index: a Study on Enhancing Institutional and Organizational Audits Using Web-Based Technology and ISO 25010:2011 Total Quality of Use Evaluation," *Int. J. Informatics Vis.*, vol. 8, no. 1, pp. 343–351, 2024, doi: 10.62527/joiv.8.1.1845.

[17] T. T. Wulansari and D. Novandi, "Evaluation of Information Security Management Using the KAMI Index Framework," in *2022 International Conference of Science and Information Technology in Smart Administration, ICSINTESA 2022*, 2022, pp. 173–177. doi: 10.1109/ICSINTESA56431.2022.10041714.

[18] N. Elsayed, "Socio-technical risks of clinical speech-to-text systems: Transparency , privacy , and reliability challenges in AI-driven documentation Nelly Elsayed iD," *Int. J. Med. Inform.*, vol. 214, no. March, pp. 1–6, 2026, doi: 10.1016/j.ijmedinf.2026.106419.

[19] N. Ebert, T. Schaltegger, B. Ambuehl, L. Schöni, V. Zimmermann, and M. Knieps, "Learning from safety science: A way forward for studying cybersecurity incidents in organizations," *Comput. Secur.*, vol. 134, p. 103435, 2023, doi: 10.1016/j.cose.2023.103435.

[20] C. Münch, E. Marx, L. Benz, E. Hartmann, and M. Matzner, "Capabilities of digital servitization: Evidence from the socio-technical systems theory," *Technol. Forecast. Soc. Chang.*, vol. 176, no. December 2021, pp. 1–16, 2022, doi: 10.1016/j.techfore.2021.121361.

[21] Ø. Toftegaard, G. Grøtterud, and B. Hämmerli, "Operational Technology resilience in the 2023 draft delegated act on cybersecurity for the power sector—An EU policy process analysis," *Comput. Law Secur. Rev.*, vol. 54, no. August, pp. 1–12, 2024, doi: 10.1016/j.clsr.2024.106034.

[22] D. Hertati, I. Arundinasari, A. Faroqi, and V. I. Pertiwi, "Tata Kelola Sosio-Teknologi dalam Mempromosikan Transparansi Informasi Publik di Pemerintahan Daerah," *Cakrawala J. Litbang Kebijak.*, vol. 19, no. 2, pp. 201–215, 2025, doi: 10.32781/cakrawala.v19i2.889.

[23] R. Fadlika, Y. Ruldeviyani, Z. T. Butarbutar, R. A. Istiqomah, and A. A. Fariz, "Employee Information Security Awareness in the Power Generation Sector of PT ABC," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, pp. 594–603, 2023, doi: 10.14569/IJACSA.2023.0140465.

[24] M. Suorsa and P. Helo, "Information Security Failures Identified and Measured – ISO/IEC 27001:2013 Controls Ranked Based on GDPR Penalty Case Analysis," *Inf. Secur. J. A Glob. Perspect.*, vol. 33, no. 3, pp. 285–306, 2024, doi: 10.1080/19393555.2023.2270984.

[25] B. Ahmedi and A. Ibrahimi, "Mastering information security through standard implementation," *Int. J. Informatics Commun. Technol.*, vol. 13, no. 3, pp. 428–435, 2024, doi: 10.11591/ijict.v13i3.pp428-435.

[26] A. Supriyanto, A. Jananto, J. A. Razaq, B. Hartono, and F. Damaryanti, "Alignment of KAMI Index with Global Security Standards in Information Security Risk Maturity Evaluation," *Cybern. Inf. Technol.*, vol. 25, no. 2, pp. 173–192, 2025, doi: 10.2478/cait-2025-0018.

[27] K. M. Sari, Y. Saintika, and W. A. Prabowo, "Penyusunan Manajemen Risiko Keamanan Informasi dengan Standar ISO 27001 Studi Kasus Institut Teknologi Telkom Purwokerto," *J. Sist. dan Teknol. Inf.*, vol. 10, no. 4, pp. 423–428, 2022, doi: 10.26418/justin.v10i4.48977.

[28] M. Carter, "ISO 27001 Toolkit," *ISO27k Forum*, 2024. https://www.iso27001security.com/toolkit (accessed Oct. 25, 2025).

[29] IBISA, *Komputer Audit dan Sekuriti*. Yogyakarta: Penerbit Andi, 2023.

[30] A. M. S. Ø. Jakobsen and W. Vanhaverbeke, "A socio-technical perspective on product configuration systems: Insights from Grundfos," *Technol. Forecast. Soc. Chang.*, vol. 225, no. December 2025, pp. 1–19, 2026, doi: 10.1016/j.techfore.2026.124564.

[31] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Yogyakarta: Alfabeta, 2019.

[32] N. W. Hidayatulloh and P. Dellia, "Evaluasi Sistem Informasi Terintegrasi Instagram dan WhatsApp Berdasarkan Pengujian ISO 25010," *JSI J. Sist. Inf.*, vol. 15, no. 2, pp. 3330–3342, 2023, doi: 10.18495/jsi.v15i2.134.

[33] P. Dellia, S. D. Saputro, R. Faisal, L. Rosidah, and N. W. Hidayatulloh, "Kualitas Perpustakaan Berdasarkan ISO 25010," *J. Teknol. dan Inf.*, vol. 15, no. 1, pp. 54–65, 2025, doi: 10.34010/jati.v15i1.15092.

[34] H. Setiawan and H. Jati, "Analisis Kualitas Sistem Informasi Pantauan Pembentukan Karakter Siswa di SMKN 2 Depok Sleman," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 2, no. 1, pp. 102–109, 2017, doi: 10.21831/elinvo.v2i1.16427.

[35] R. E. Indrajit, "Kebijakan Keamanan Informasi," *Universitas Telkom*, 2021.