Journal of Applied Informatics and Computing (JAIC)
Vol.10, No.4, August 2026, pp. 3796~3807
e-ISSN: 2548-6861

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

Nasya Ananda Rozi1*, Agus Wijayanto2*, Wahyu Nur Alimyaningtias3*
* Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia
nasyarozi@students.universitasmulia.ac.id [1], aguswijayanto@universitasmulia.ac.id [2], wahyu.nur@universitasmulia.ac.id [3]

Article Info

Article history:

Received 2026-06-26
Revised 2026-07-24
Accepted 2026-08-12

Keywords:

KAMI Index 5.0,
Information Security,
ISO/IEC 27001.

ABSTRACT

Information security is a strategic aspect that determines the continuity of organizational operations amid an increasing dependence on digital systems. PT. QAZ, as a regionally owned business entity providing clean water services, relies on information systems to support customer management, payment systems, and distribution network management, so evaluating the readiness of its information security is crucial. This study aims to measure the level of information security readiness of PT. QAZ through the integration of the KAMI Index 5.0 with ISO/IEC 27001:2022 control using a mixed methods approach. The results of the evaluation of the Electronic Systems Category obtained a score of 19 points with a high category, while the accumulation of the sixth score in the evaluation area reached 372 out of a maximum total of 918 points, with the achievement of the supplement category of 26%. In detail, the maturity level of each domain is: Level I+ Information Security Governance, Level II Risk Management, Level I Information Security Management Framework, Level I+ Information Asset Management, Level II Information Technology and Security, and Level I Personal Data Protection.

I. INTRODUCTION

The development of information technology has increased the dependence of organizations on information systems to support business processes and services. However, this condition also increases information security risks, such as data leaks, unauthorized access, and cyberattacks that can disrupt organizational operations and reduce public trust [1]. There are many cases of data loss and damage caused by cybercrime that can attack anyone without exception[2]. According to cybersecurity landscape data from the State Cyber and Cryptography Agency in 2023, the number of attacks that occurred during January – December 2023 was 403,990,813 [3]. As a regional company providing clean water services, PT. QAZ utilizes information systems to support customer management, payment, and water distribution, so information security is a very important aspect. PT. QAZ relies heavily on information systems to support operational activities such as customer management, payment systems, and clean water distribution network management. Information security protection is a crucial component in the operational sustainability aspect of organizations that rely on digital systems, because weaknesses in this aspect can pose a risk of data leakage[4]. Disruption or data leakage on such systems can have a direct impact on the company's services and reputation. Therefore, information security is an important aspect that must be considered comprehensively — not only from the technological side, but also from governance, policies, and employee awareness [5][6].

PT. QAZ was chosen as the object of the research because of its characteristics that represent essential public service provider organizations, particularly in the clean water management sector. As a BUMD, PT. QAZ manages large amounts of customer data and a massive and sustainable payment system, while the services it provides are directly related to the basic needs of the community so that even the slightest disruption has the potential to have a wide social impact. In addition, until now PT. QAZ has never conducted a systematic and standardized evaluation of information security, thus making this organization a relevant case study to illustrate the condition of information security readiness in BUMDs providing basic public services.

To assess the level of information security readiness, the State Cyber and Cryptography Agency (BSSN) developed the KAMI Index 5.0 which refers to the ISO/IEC 27001 standard. The ISO/IEC 27001:2022 standard itself is an international framework for the implementation of an Information Security Management System (ISMS) that helps organizations manage information security risks systematically [7][8]. Organizations that conduct evaluations using the KAMI Index will have an idea of their readiness to adopt these international standards[9]. Evaluation is needed to observe the readiness of the things that the organization has done in carrying out information security measures[10].

However, most previous studies evaluating information security readiness still use the older version of the KAMI Index (such as version 4.0 or 4.2) mapped to ISO/IEC 27001:2013, even though ISO/IEC 27001:2022 has undergone a significant update to the security control structure (*Annex A*), which is simplified to 93 controls grouped into four main themes. As a result, the results of the older version-based evaluation are potentially less relevant in representing the organization's readiness for the latest information security requirements. The research that specifically maps the KAMI Index 5.0 with ISO/IEC 27001:2022 on regional-based public service provider organizations, such as clean water BUMDs, is also still limited in number, leaving research *gaps* that need to be filled.

Several previous studies have shown that many public agencies in Indonesia are still in the "Not Feasible" category in the implementation of information security based on the results of the evaluation of the KAMI Index 5.0, especially in the aspects of governance and risk management [1], [11]. Based on the research gap, the novelty (*novelty*) of this study lies not only in the use of the KAMI Index as a tool for evaluating the readiness of ISO/IEC 27001 which has indeed been widely applied to various types of organizations but also in the application of the integration of the latest version of the KAMI Index (5.0) with the updated ISO/IEC 27001:2022 control structure, in the context of regionally owned clean water service provider organizations that are characteristically different from previous research objects (hospitals, educational institutions, as well as government agencies). The scientific contribution of this research is to produce a mapping of information security readiness that is specific to the context of BUMD public basic service providers, as well as to prepare improvement recommendations that are in line with the latest controls in ISO/IEC 27001:2022, so that it can be a practical reference for similar organizations in designing information security improvements towards readiness for international standard certification.

Therefore, this study aims to evaluate the level of information security readiness at PT. QAZ uses the KAMI Index 5.0 mapped with ISO/IEC 27001:2022 controls. The results of the research are expected to be the basis for the preparation of improvement recommendations to improve information security and organizational readiness towards the implementation of ISMS in accordance with international standards.

Information security is becoming an increasingly crucial aspect as organizations become increasingly dependent on digital systems and information technology[12]. Every organization, both public and private, needs to ensure that the information systems they use have an adequate level of readiness to protect data, assets, and services from cyber threats[13]. Thus, information security plays an important role in supporting the business continuity of an organization and minimizing risks that may arise[14]. In its application, information security has several key aspects known as the CIA Triad [15]. To assess this readiness, various studies have used the Information Security Index (KAMI Index) version 5.0 and the international standard ISO/IEC 27001:2022 as an evaluation framework.

Previous research has shown that the combination of the KAMI Index 5.0 and ISO/IEC 27001:2022 is effective in mapping the level of information technology security readiness in an organization. Their study results show that the company's security systems evaluated are in the "moderately good" category, but still need improvement in some aspects of governance and risk management. The researcher also emphasized the importance of the conformity of organizational policies with the clauses contained in the ISO/IEC 27001:2022 standard as an international reference in information security management [16].

The next research is on the online regional tax system in Sumedang Regency using the KAMI Index 5.0 which refers to ISO/IEC 27001:2022. The results of the study show that although the tax system has a fairly good readiness, there are still shortcomings in the aspects of risk management, governance, and asset management. These findings indicate that the implementation of information security standards in the public sector still requires more attention to achieve optimal maturity. [17].

Furthermore, research on the implementation of ISO/IEC 27001:2022 highlights that many organizations still face obstacles in adjusting to the new structure and requirements introduced in the version of the standard. Key challenges include understanding the organizational context, leadership in the implementation of security policies, and performance evaluation systems and continuous improvement. This study shows that the successful implementation of ISO standards depends not only on technical procedures, but also on organizational commitment and governance [18].

Then the research was conducted in a university environment, namely Darul 'Ulum University Jombang, using the KAMI Index 5.0 and associating it with ISO/IEC 27001:2022. They found that the level of information security maturity in these institutions is still relatively low. Through root cause analysis using the "5 Whys" Root Cause Analysis method, this study recommends strengthening security controls, increasing user awareness, and adjusting security policies in accordance with ISO/IEC 27001:2022 clauses [19].

Meanwhile, research on information security readiness at the Communication and Information Service (Diskominfo) of Gianyar Regency, Bali. This study uses the KAMI Index version 4.2 which is aligned with ISO/IEC 27001:2013 to assess the level of readiness and maturity of information security in local government institutions. Through an evaluative approach involving interviews, questionnaires, and data validation, the study assesses seven key areas in the KAMI Index, including governance, risk management, information security frameworks, asset management, technological aspects, and personal data protection. The results showed that the Gianyar Regency Diskominfo obtained a final score of 190, with the status of "Not Feasible" to meet the ISO/IEC 27001:2013 certification standard [20].

II. METHOD

This study applies a mixed methods approach, which combines quantitative and qualitative approaches in one research process to obtain more comprehensive results. The selection of this approach was based on the need for research that not only focused on measuring the level of information security readiness, but also required a more in-depth analysis to formulate improvement recommendations. The research began with a quantitative approach to measure the level of information security readiness at PT. QAZ using the KAMI 5.0 Index instrument. The measurement results are in the form of scores or values that represent the level of information security maturity in accordance with applicable standards. Meanwhile, the qualitative approach aims to analyze the results of the evaluation and prepare recommendations for improvement. At this stage, the researcher interprets the results of the KAMI Index assessment and relates it to real conditions in the field, so that it can produce relevant and applicable recommendations.

The evaluation methodology in this study is prepared through several stages that are sequential and continuous. The first stage is the initial data collection through interviews and observations to identify the existing conditions of information security at PT. QAZ. The second stage is the filling of the KAMI Index 5.0 instrument which is carried out with the resource persons to obtain scores in each evaluation area. The third stage is data triangulation, which is the process of comparing the results of interviews with the results of observation and document review to ensure the consistency of answers before the final score is determined. The last stage is data validation, which is the process of reconfirming to the resource person the results of the assessment that have been inputted, to ensure that the score recorded really reflects the actual condition of the organization and not just the respondent's momentary perception.

The respondents in this study were two people, namely Supervisors and Staff of the Infrastructure and Network Development Sub-Division at the Management Information System (SIM) Division of PT. QAZ. The selection of respondents was carried out purposively (purposive sampling) with the main criteria, namely; Have direct authority and responsibility in the management of information technology and information security of the company, understand the technical conditions and internal policies related to the electronic systems used, and have an adequate working period to be able to explain the history of the implementation of information security in the organization. This limited number of respondents is in line with the characteristics of the KAMI Index 5.0 instrument which is designed to be filled by those who have authority and a comprehensive understanding of organizational information security governance, not by a large number of respondents as in conventional quantitative survey research.

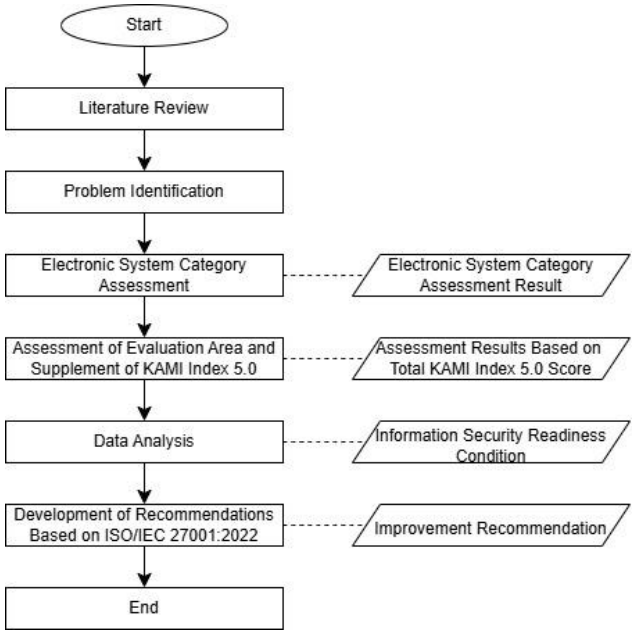

Figure 1. Research Flow

The research stages in this study are systematically arranged. From Figure 1 above, it shows the flow of research stages starting from problem identification, literature study, determination of research methods, data collection, to data analysis and preparation of recommendations.

A. Literature Studies

The first stage carried out in this study is to conduct a literature study with the aim of collecting and analyzing information relevant to the topic being researched. This stage is carried out by collecting various kinds of references in the form of journals, e-books, reports, and sites that discuss information security evaluation, the KAMI Index method version 5.0, and the ISO/IEC 27001:2022 Standard by considering the relevance of the sources obtained.

B. Problem Identification

This stage is carried out through interviews and observations based on the conditions in PT. QAZ. The interview was conducted to find out the problems based on the existing conditions at PT. QAZ is currently so that the existing problems are found. The questions asked are about

the information technology unit and the state of the information and information technology systems that are currently being used. After obtaining this information, problem mapping can be carried out so that the solution can be determined in a relevant manner.

C. Electronic Systems Category Level Assessment

At the assessment stage at the electronic system category level, this process is carried out by asking 10 questions that are available on the KAMI Index dashboard version 5.0 which is processed using Microsoft Office Excel software. The results of this assessment will be classified into three levels, namely Low, High, and Strategic. This stage aims to find out the extent of dependence of PT. QAZ against the electronic system used.

D. *Evaluation and Supplement Area Assessment of the KAMI Index Version 5.0*

This stage was carried out to assess six main areas along with supplement categories in the KAMI Index Version 5.0 as a reference for measuring the level of maturity and readiness of information security at PT. QAZ. All data that has been collected is processed using the KAMI Index Version 5.0 dashboard in Microsoft Excel, resulting in a total score that reflects the assessment of the six areas and categories of supplements. The scoring mechanism in the KAMI 5.0 Index is carried out by assigning a score to each question based on the implementation status chosen by the respondents, namely "Not Done" (score 0), "In Planning" (score 1), "Partially Implemented/In Implementation" (score 2 or 3, depending on the level of the security category of the question), to "Applied Thoroughly" (the highest score according to the weight of the question). Each question on the KAMI Index 5.0 has a different score weight depending on the security category (stages 1, 2, or 3) and the level of maturity (levels I to V) it represents. The scores of all questions in one area are then summed and compared with the minimum score threshold at each stage and maturity level, so that an interpretation is obtained in the form of; the status of security completeness in the form of "Valid" or "Invalid" in each security category and the level of maturity stated on a scale of I (Initial Condition) to V (Optimal), as displayed by the system through a combination of colors on the dashboard, namely red "Not Feasible", orange and yellow "Basic Framework Has Been Met", light green "Quite Good", and dark green "Good". The final interpretation of the organization's readiness for ISO/IEC 27001:2022 certification is determined by comparing the level of maturity achieved against the minimum required standard, i.e. Maturity Level III+ (Defined and Consistent).

The mapping process between the KAMI Index 5.0 and the ISO/IEC 27001:2022 control in this study is based on the conformity of the substance between the evaluation areas in the KAMI Index and the security clauses and controls (Annex A) in ISO/IEC 27001:2022, which have been officially designed in harmony by the State Cyber and Cryptography Agency (BSSN) as the development agency of the KAMI Index. The conceptual basis of this mapping refers to the similarity of the scope of the control substances, as presented in Table 1 below.

TABLE I.

KAMI INDEX 5.0 AREA MAPPING AGAINST ISO/IEC 27001:2022 CLAUSES AND CONTROLS

KAMI Index Area 5.0	Related ISO/IEC 27001:2022 Clauses/Controls	The Basis of Substance Linkage
Information Security Governance	Clause 5 (Leadership), Organizational Theme Control A.5.1–A.5.4	Assess information security policies, organizational structures, and management roles and responsibilities
Information Security Risk Management	Clause 6 (Planning), Controls A.5.7 and A.8.8	Measure the process of identifying, analyzing, and handling information security risks
Information Security Management Framework	Clauses 7–10 (Support, Operation, Performance Evaluation, Upgrade), Control A.5.24–A.5.30	Assess SOPs, incident management, and service continuity
Information Asset Management	Organizational Theme Control A.5.9–A.5.14	Assess the inventory, classification, and lifecycle of information assets
Information Technology and Security	Technology Theme Control A.8.1–A.8.34	Assess technical controls, such as system access, network security, and vulnerability management
Personal Data Protection	Control A.5.34	Assess the compliance of personal data management with applicable regulations

To ensure the validity of the assessment results, the evaluation process in this study not only relies on oral answers from interviews, but is also complemented by direct observation of operational conditions in the field, document review (such as information security policies, SOPs, and information system management guidelines), as well as requests for implementation evidence in the form of supporting documents, screenshots of system configuration, and operational records relevant to the questions on KAMI Index 5.0. The three data sources are then confirmed with each other (data triangulation) before the final score on each question is determined.

Considering that this study involves one assessor (researcher) who assesses independently, the consistency and reliability of the assessment are maintained through two mechanisms. First, the use of standard *scoring guidelines* that have been available in the KAMI Index 5.0 instrument, so that

the interpretation of answers to scores follows standardized criteria and does not depend on the subjective interpretation of the researcher. Second, a re-verification process is carried out to the resource person on the assessment results that have been input before it is considered final, to ensure that there is no misinterpretation between the resource person's answer and the recorded score. As a form of *cross-validation*, the interview results of the two speakers were compared with each other to see the consistency of the answers between the respondents to the same question. If a discrepancy is found, the researcher conducts further clarification and refers to supporting documents as objective evidence to determine the final score that best represents the real condition of the organization.

The researcher realizes that this assessment process has the potential to be biased, considering that the scores produced are highly dependent on respondents' answers and the availability of internal organizational documents. Potential bias may arise if respondents tend to provide answers that describe conditions better than reality (*social desirability bias*), or if the available supporting documents do not fully reflect daily operational practices. To minimize these risks, the researcher applied data source triangulation as described earlier, although this limitation still needs to be noted in interpreting the overall research results.

E. Research Data Analysis

At this stage, an analysis was carried out on the score results that have been obtained from the assessment of the electronic system category and also the assessment of all evaluation areas in the KAMI Index 5.0 based on the KAMI 5.0 Index dashboard and spider chart through Microsoft Office Excel regarding the level of readiness or maturity of information security at PT. QAZ.

F. *Preparation of Recommendations with ISO/IEC 27001:2022*

At the stage of preparing recommendations based on the ISO/IEC 27001:2022 standard, information security recommendations were prepared addressed to PT. QAZ. This recommendation is focused on questions that have "In Planning" and "Not Done" statuses, because they indicate a plan that has not been implemented and actions that have not been taken. Therefore, recommendations are needed so that the right improvement steps can be taken immediately. In addition, the status also shows that PT. QAZ has not fully complied with the requirements of the ISO/IEC 27001 standard.

III. RESULTS AND DISCUSSION

A. Electronic Systems (SE) Category Assessment

The results of the evaluation of the Electronic System Category level at PT. QAZ obtained a total score of 19 points. The score is in the range of 16–34 points so it is classified as "High". This score is obtained from the results of the summation of 10 questions asked, with each question having a value range of 1, 2, and 5. Of the total questions, one question was answered with criterion A, five questions with criterion B, and four questions with criterion C. The high level of dependence on Electronic Systems shows that the continuity of business and operational processes of PT. QAZ is heavily influenced by the electronic systems used.

B. KAMI Index Area Assessment 5.0

TABLE II.TEXT SIZE REFERENCE LEVEL OF SECURITY COMPLETENESS OF GOVERNANCE AREA

Security Category (Stages)	**Number of Information Security Governance Area Questions**	**Total Score**
1	8	13
2	8	40
3	6	0
Minimum Stage 3 Score	-	48
Total Stages 1 and 2	16	45

TABLE III.
MATURITY LEVEL OF GOVERNANCE AREA SECURITY

Maturity Level Category	**Number of Information Security Governance Area Questions**	**Score**	**Maturity Status Level**
II	13	31	I+
III	3	14	Yes
IV	6	0	Yes
Quantity	22	45	

Table 2 shows the level of security completeness in each security category of the Information Security Governance area. To determine the status of security completeness, a comparison was made between the total score of the security category at the implementation stages 1 and 2 with the minimum score limit of implementation stage 3 as stated in the KAMI 5.0 Index, which is 48 points. The total score in the implementation stages 1 and 2 is 45 points. This value has not reached the standard of implementation stage 3, so it is still in the status of Invalid assessment.

Table 3 shows the level of maturity in each category in the Information Security Governance area of PT. QAZ. At maturity level II there were 13 questions with a total score of 31 points. The maturity status is at level I+ because it has met the minimum score of maturity level II, which is 12 points, but it is not yet at maturity level II because it has not reached the maturity level achievement score II, which is 36 points. At maturity level III there were 3 questions with a total score of 14 points. Even though the score has met the maturity level III achievement score of 14 points, the maturity status is still declared "No" because the validity of maturity level II is also declared "No". Meanwhile, at the IV maturity level, there were 6 questions with a total score of 0 points. His maturity status was declared No because he did not meet the minimum score of 24 points at the IV maturity level or the achievement

score set at 54 points. Thus, it can be concluded that the status or maturity level in the Information Security Governance area is at level I+ (Initial Condition).

TABLE IV.
LEVEL OF SECURITY COMPLETENESS OF RISK MANAGEMENT AREA

Security Category (Stages)	Number of Information Security Governance Area Questions	Total Score
1	10	24
2	4	20
3	2	0
Minimum Stage 3 Score	-	40
Total Stages 1 and 2	14	44

TABLE V.
RISK MANAGEMENT AREA SECURITY MATURITY LEVEL

Maturity Level Category	Number of Information Security Governance Area Questions	Score	Maturity Status Level
II	10	24	II
III	2	10	Yes
IV	2	10	Yes
V	2	0	Yes
Quantity	16	44	

Table 4 shows the level of security completeness in each security category in the Information Security Risk Management area. To determine the status of security completeness, a comparison was made between the total score of the security category at the implementation stages 1 and 2 with the minimum score limit of implementation stage 3 contained in the KAMI Index 5.0, which is 40 points. The total score in the implementation stages 1 and 2 was 44 points. The value has reached the minimum limit of implementation stage 3, but the assessment of implementation stage 3 is still categorized in the assessment status of "Invalid" because the fulfillment status of implementation stage 1 is "No".

Table 5 shows the level of maturity in each category in the Information Security Risk Management area at PT. QAZ. At maturity level II, there were 10 questions with a total score of 24 points. Because the score has reached the maturity level achievement score of II, which is 20 points, the maturity level status is "II". At maturity level III there are 2 questions with a total score of 10 points. This score has met the minimum score and also achieved a maturity level III achievement score of 8 points. However, because the validity of maturity level III is in the status of "No", the maturity level III is also automatically in the status of "No". Furthermore, at maturity level IV there are 2 questions with a total score of 10 points. This score meets the minimum score of 8 points, but has not reached the level IV achievement score of 12 points. In addition, because maturity levels II and III have the status of "No", level IV also has the status of "No". Finally, at maturity level V there are 2 questions with a score of 0 points, so the maturity status is also "No". Thus, it can be concluded that the status or level of maturity in the area of Information Security Risk Management is at level II (Application of the Basic Framework).

TABLE VI.
LEVEL OF SECURITY COMPLETENESS INFORMATION SECURITY MANAGEMENT FRAMEWORK AREA

Security Category (Stages)	Number of Information Security Governance Area Questions	Total Score
1	12	17
2	11	28
3	10	0
Minimum Stage 3 Score	-	68
Total Stages 1 and 2	23	45

TABLE VII.
SECURITY MATURITY LEVEL INFORMATION SECURITY MANAGEMENT FRAMEWORK AREA

Maturity Level Category	Number of Information Security Governance Area Questions	Score	Maturity Status Level
II	11	8	Yes
III	17	37	Yes
IV	3	0	Yes
V	2	0	Yes
Quantity	33	45	

Table 6 shows the level of security completeness in each security category of the Information Security Management Framework area. To determine the status of security completeness, a comparison was made between the total score of the security category at the implementation stages 1 and 2 with the minimum score limit of implementation stage 3 contained in the KAMI Index 5.0, which is 68 points. The total score in the implementation stages 1 and 2 is 45 points. The value does not reach the minimum limit of implementation stage 3, so it is categorized in the assessment status of "Invalid".

Table 7 shows the level of maturity in each maturity category in the Information Security Management Framework area at PT. QAZ. At maturity level II, there were 11 questions with a total score of 8 points. The score does not reach the maturity level II achievement score specified in the KAMI Index 5.0, which is 24 points, and has not met the minimum score of maturity level II of 15 points, then the maturity status is declared "No". At maturity level III there were 17 questions with a total score of 37 points. This score also did not meet the minimum score of 56 points or the achievement score of maturity level III of 84 points, so the maturity status was also declared "No". As for the maturity level IV and V, all questions received a score of 0, so the

maturity status was also declared "No". Thus, the level of maturity of the Information Security Management Framework area at PT. QAZ is at Level I (Initial Condition).

TABLE VIII.
LEVEL OF COMPLETENESS OF INFORMATION ASSET MANAGEMENT AREA

Security Category (Stages)	Number of Information Security Governance Area Questions	Total Score
1	27	58
2	19	42
3	7	0
Minimum Stage 3 Score	-	130
Total Stages 1 and 2	46	100

TABLE IX.
MATURITY LEVEL OF SECURITY INFORMATION ASSET MANAGEMENT AREA

Maturity Level Category	Number of Information Security Governance Area Questions	Score	Maturity Status Level
II	32	78	I+
III	21	22	Yes
Quantity	53	100	

Table 8 shows the level of security completeness in each security category in the Information Asset Management area. To determine the status of security completeness, a comparison was made between the total score of the security category at the implementation stages 1 and 2 with the minimum score limit of implementation stage 3 contained in the KAMI Index 5.0, which is 130 points. The total score in the implementation stages 1 and 2 is 100 points. The value does not reach the minimum limit of implementation stage 3, so it is categorized in the assessment status of "Invalid".

Table 9 presents the level of maturity in each category in the Information Asset Management area at PT. QAZ. At maturity level II there were 32 questions with a total score of 78 points. This value has met the minimum limit of maturity level II, which is 39 points, so it is at level I+. However, this value has not reached the maturity level II achievement score of 88 points, so it cannot be categorized at maturity level II. Furthermore, at maturity level III there were 21 questions with a total score of 22 points. This score has not met the minimum score of maturity level III of 83 points or an achievement score of 118 points, so the maturity status is "No". Thus, the maturity level in the Information Asset Management area at PT. QAZ is at level I+ (Initial Condition).

TABLE X.
LEVEL OF SECURITY COMPLETENESS IN THE TECHNOLOGY AND INFORMATION SECURITY AREA

Security Category (Stages)	Number of Information Security Governance Area Questions	Total Score
1	14	34
2	15	66
3	6	24
Minimum Stage 3 Score	-	88
Total Stages 1 and 2	29	100

TABLE XI.
MATURITY LEVEL OF SECURITY IN THE TECHNOLOGY AND INFORMATION SECURITY AREA

Maturity Level Category	Number of Information Security Governance Area Questions	Score	Maturity Status Level
II	14	34	II
III	18	84	Yes
IV	3	6	Yes
Quantity	35	124	

Table 10 shows the level of security completeness in each security category in the Technology and Information Security area. To determine the status of security completeness, a comparison was made between the total score of the security category at the implementation stages 1 and 2 with the minimum score limit of implementation stage 3 contained in the KAMI 5.0 Index, which is 88 points. Based on the results of the calculation, the total score in the implementation stages 1 and 2 is 100 points. This value exceeds the minimum limit of implementation stage 3, but the status of fulfillment of stage 1 results "No", so it is still categorized in the assessment status of "Invalid".

Table 11 presents the level of maturity in each category in the area of Information Technology and Security at PT. QAZ. At maturity level II, there were 14 questions with a total score of 34 points. This value has reached the maturity level II achievement score of 28 points, so that the maturity status is at level II. Furthermore, at maturity level III there were 18 questions with a total score of 84 points. This score has met the minimum score of 68 points but did not reach an achievement score of 92 points, so the maturity status is "No". Then, at maturity level IV there are 3 questions with a total score of 6 points, these values do not reach the total score of achievement of maturity level IV which is 21 points so that the maturity status is also declared "No". Thus, the level of maturity in the area of Information Technology and Security at PT. QAZ is at level II (Implementation of the Basic Framework).

TABLE XII.
LEVEL OF SECURITY COMPLETENESS OF PERSONAL DATA PROTECTION AREA

Security Category (Stages)	Number of Information Security Governance Area Questions	Total Score
1	4	6
2	12	8
3	0	0
Minimum Stage 3 Score	-	56
Total Stages 1 and 2	16	14

TABLE XIII.
MATURITY LEVEL OF SECURITY OF PERSONAL DATA PROTECTION AREA

Maturity Level Category	Number of Information Security Governance Area Questions	Score	Maturity Status Level
II	6	6	Yes
III	10	8	Yes
Quantity	35	124	

Table 12 shows the level of security completeness in each security category in the Personal Data Protection area. To determine the status of security completeness, a comparison was made between the total score of the security category at the implementation stages 1 and 2 with the minimum score of the implementation stage 3 contained in the KAMI Index 5.0, which is 56 points. Based on the calculation results, the total score in the implementation stages 1 and 2 is 14 points. This value is still below the minimum score limit of implementation stage 3, so it is categorized in the assessment status of "Invalid".

Table 13 presents the level of maturity in each category in the Personal Data Protection area at PT. QAZ. At maturity level II, there are 6 questions with a total score of 6 points. The score does not reach the maturity level II achievement score of 16 points and has not met the minimum score of maturity level II of 8 points, so the maturity status is declared "No". Furthermore, at maturity level III there were 10 questions with a total score of 8 points. This score also did not reach a minimum score of 36 points and an achievement score of 48 points, so the maturity status was also "No". Thus, the level of maturity in the Personal Data Protection area at PT. QAZ is at level I (Initial Condition).

To facilitate the identification of the areas with the lowest level of readiness, the results of the assessment of the six evaluation areas are presented concisely and comparatively in Table 14 below.

TABLE XIV.
SUMMARY OF COMPARATIVE MATURITY LEVELS BETWEEN AREAS

Evaluation Area	Total Score	Maturity Level	Status against Minimum Threshold III+
Information Security Governance	45	I+	Not yet achieved
Information Security Risk Management	44	II	Not yet achieved
Information Security Management Framework	45	I	Not yet reached (largest gap)
Information Asset Management	100	I+	Not yet achieved
Information Technology and Security	124	II	Not yet achieved
Personal Data Protection	14	I	Not yet reached (largest gap)

Based on the comparison in Table 14, it can be identified that the status of "Not Feasible" in PT. QAZ is most contributed by the two areas with the lowest level of maturity, namely the Information Security Management Framework and Personal Data Protection, both of which are at Level I (Initial Condition). In the Framework area, out of the 33 questions assessed, all maturity level categories II to V obtained a status of "No", with the total score at implementation stages 1 and 2 reaching only 45 out of the minimum limit of 68 points indicating that standard operating procedures (SOPs), incident management, and service continuity planning have not been adequately documented. Similar conditions also occur in the Personal Data Protection area, where the total score of stages 1 and 2 only reached 14 out of the minimum limit of 56 points, indicating that the customer data protection policies and mechanisms at PT. QAZ is still very limited. In contrast, the areas of Risk Management and Technology and Information Security showed relatively better achievement with maturity level II, so both domains contributed less to the overall low score than the Personal Data Protection and Framework. Thus, controls in the two areas with the largest gaps need to be a top priority in the preparation of improvement recommendations.

C. *Research Data Analysis*

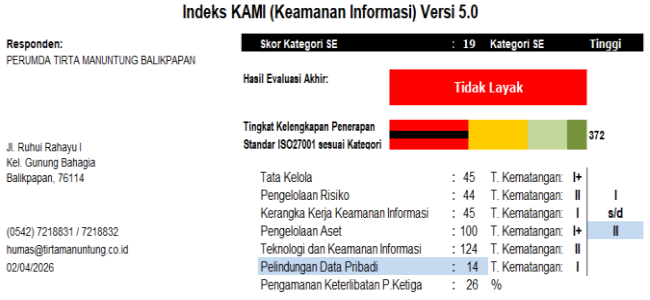

Figure 2. Assessment Dashboard PT . QAZ

Figure 2 above shows the dashboard display of the evaluation results using the KAMI Index version 5.0. The information presented in the dashboard includes several components, namely the Electronic System category, the Level of Completeness of Information Security Implementation, the Maturity Level in each area, and the results of the final evaluation. Based on the results of the assessment, the Electronic System at PT. QAZ obtained a score of 19, which falls into the "High" category, indicating that the organization has a high level of dependence on electronic systems. Furthermore, the level of completeness of the implementation of the ISO 27001 standard displayed in the form of a bar chart shows a total value of 372 points. This indicator is visualized through a combination of colors on the bar chart, where the value position is still in the red zone, which indicates that the level of information security readiness is still in the "Not Feasible" condition. In addition, the results of the evaluation also show the level of maturity in all areas, as well as the value of securing third-party involvement / supplements in the form of a percentage, which is 26%. These values show variations in the level of maturity that still need to be improved in several aspects to achieve the expected standard.

In addition, the dashboard is also equipped with a spider chart that functions to visualize the level of information security maturity in each evaluation area. This visualization makes it easy to see the overall comparison of achievements in each domain. To find out the detailed description, you can see Figure 3 below.

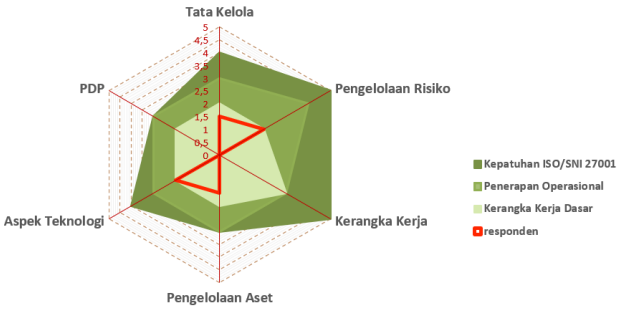

Figure 3. Spider Chart Area Evaluation

The spider chart uses three color gradations that represent the security category. The bright green color depicts the Basic Framework, the light green color depicts the Operational Implementation, while the dark green color depicts Compliance with the ISO/SNI 27001 standard. Meanwhile, the red line indicates the position of the assessment results. Based on the graph, it can be seen that the achievement in some areas such as Risk Management and Framework is relatively higher than in other areas. However, in aspects such as Personal Data Protection and Asset Management, the value obtained is still low. In general, the position of the respondent line is still in the range of low maturity level (around levels I to II), thus showing that the implementation of information security at PT. QAZ still needs to be improved in order to achieve a more optimal level of maturity.

Based on the results of the assessment of the maturity level of information security in each area, it can be seen that the overall maturity level at PT. QAZ is in the range of levels I to II. This can be seen from the achievements in each domain, where several areas such as Risk Management and Technology Aspects have reached level II, while other areas such as Governance and Asset Management are at level I+, and Personal Data Protection Framework and Protection (PDP) are still at level I. Referring to these conditions, the level of maturity achieved is still included in the category of basic security with the status of "Implementation of the Basic Framework", which indicates that the implementation of information security is still in the early stages of development and has not been fully defined consistently.

As seen in the radar chart of maturity level comparison above, the achievement line of PT. The QAZ (blue color) is well below the minimum standard line of Level III+ certification (dotted red) in all six evaluation areas without exception. The widest gap was seen in the area of the Information Security and Personal Data Protection Management Framework, while the gap was relatively narrower in the areas of Risk Management and Technology and Information Security. This visualization reinforces the findings in Table 14 that improvements need to be focused first on the two areas with the lowest achievement in order for the overall level of organizational maturity to be more effective. As for the condition of the level of security maturity at PT. QAZ can be seen in Tabel 15 below.

FIGURE XV.
THE SECURITY MATURITY LEVEL CONDITION OF PT. QAZ

Level	Conditions
I	Initial Conditions
II	Application of the Basic Work Framework
III	Defined and Consistent
IV	Managed and Scalable
V	Optimal

Based on the reference level of maturity of the KAMI Index, this condition indicates that the implementation of information security at PT. QAZ has not met the minimum standards required for ISO/IEC 27001 certification, where the minimum expected maturity level is at level III+ (defined and consistent). Therefore, improvements are still needed in various aspects in order to achieve a higher level of maturity and in accordance with applicable standards.

The low level of information security readiness at PT. QAZ cannot be separated from several interrelated root causes. First, from the governance aspect, the lack of formal policies and clear responsibility structures related to information security causes the security decision-making process to tend to be reactive, not planned [15]. Second, from

a policy aspect, the absence of documented Standard Operating Procedures (SOPs) in the Framework area causes the handling of information security incidents and service sustainability planning to not have a standard reference. Third, from the technological aspect, although the achievements in the area of Information Technology and Security are relatively better than other areas, technical controls such as vulnerability management and network security monitoring still need to be strengthened in order to reach the required level of maturity. Fourth, from the aspect of human resources, the limited number of personnel who handle information security also limits the organization's capacity to carry out all security functions as a whole. Fifth, from the aspect of security culture, the low awareness of information security among employees has slowed down the implementation of security policies that have been or will be prepared [21].

These findings are in line with research on the implementation of ISO/IEC 27001:2022 which confirms that the successful implementation of information security standards does not only depend on technical aspects, but also on the commitment and governance of the organization as a whole [22]. Based on these findings, improvement recommendations are prepared in stages based on the order of risk priority, so that they can be used as an implementation roadmap for PT. QAZ. This prioritization approach refers to risk management principles that place the areas with the largest maturity gaps and the highest potential impacts as top priorities [23]. The proposed implementation roadmap is as follows:

1. Short term (0–6 months): preparation and ratification of basic information security policies, appointment of information security person in charge, and preparation of SOPs for handling incidents in the Information Security Management and Personal Data Protection Framework area, considering that these two areas have the largest maturity gap.
2. Medium term (6–12 months): implementation of information asset management controls, including asset inventory and classification, as well as strengthening of personal data protection controls in accordance with applicable laws and regulations.
3. Long-term (12–24 months): strengthening advanced technical controls in the areas of Information Technology and Security and Risk Management, followed by internal audits to prepare organizations for ISO/IEC 27001:2022 certification readiness.

To show the position of the readiness level of PT. QAZ is comparatively similar to similar studies in other organizations. In the evaluation of information security in a hospital using the KAMI Index 5.0, the organization also obtained a readiness status that did not meet the ISO/IEC 27001:2022 standard, with the main challenges in terms of governance and risk management [1]. The pattern is similar to the findings in PT. QAZ. In the evaluation of the online regional tax system in Sumedang Regency, although the level of readiness is quite good, shortcomings are still found in the aspects of risk management and asset management [24], which shows that problems in this aspect are relatively common in various organizations. Meanwhile, in the evaluation of a regional communication and informatics office with the KAMI Index version 4.2 approach, the organization obtained the status of "Not Feasible" to meet the ISO/IEC 27001 standard [25], reinforcing the indication that many public sector organizations and BUMDs in Indonesia are still in the early stages of information security maturity. Compared to these studies, the position of PT. QAZ is relatively low, especially in the area of the Personal Data Protection and Framework, which shows a larger maturity gap than similar organizations that have been evaluated in previous studies.

In addition to being compared with similar studies, the KAMI Index 5.0 approach in this study also needs to be reviewed relative to other commonly used information security frameworks, namely the National Institute of Standards and Technology (NIST) Cybersecurity Framework and Control Objectives for Information and Related Technology (COBIT). The NIST Cybersecurity Framework emphasizes five core functions, namely Identify, Protect, Detect, Respond, and Recover, which are more oriented towards operational cyber risk management. Meanwhile, COBIT focuses more on the governance and management of information technology as a whole, including the alignment of IT strategy with the organization's business objectives [26]. Compared to the two frameworks, the KAMI Index 5.0 has advantages in the form of its suitability with the context of Indonesian national regulations and ease of implementation because it is equipped with a standardized assessment dashboard by BSSN. However, on the other hand, the KAMI Index 5.0 has limitations compared to NIST CSF and COBIT in terms of depth of operational technical guidance and strategic integration of information technology governance, so the combination of the KAMI Index with this framework has the potential to enrich the results of evaluations in future research [27].

The results of this evaluation have significant implications for the business continuity of PT. QAZ, considering that this organization provides basic services in the form of clean water distribution to the community. The low maturity of the Information Security Management Framework area, one of which includes service sustainability planning, has the potential to increase the risk of operational disruption in the event of an information security incident. In terms of regulatory compliance, the low maturity in the Personal Data Protection area also poses a risk of non-compliance with laws and regulations related to personal data protection that apply in Indonesia. In terms of organizational risk management in general, this condition shows that PT. QAZ still needs to be strengthened in the entire risk management cycle, from identification, analysis, to handling information security risks on an ongoing basis.

D. Recommended Improvements

After conducting an assessment in all areas based on the KAMI Index version 5.0 at PT. QAZ, then analyzes the results of the assessment and then obtains the final results of all areas based on the KAMI Index version 5.0, the next stage is to provide recommendations for improvement for questions whose status is "Not Done" and "In Planning". The goal is to be able to increase compliance with current information security controls and adjust to the ISO/IEC 27001:2022 standard. Recommendations for improving the area of information security governance were given for 6 (six) questions with the status of "Not Done" based on the results of the KAMI Index 5.0 assessment at PT. QAZ. Recommendations for improving the area of the information security management framework were given for 17 (seventeen) questions with the status of "Not Done" based on the results of the KAMI Index 5.0 assessment on PT. QAZ. Recommendations for improving the area of information asset management were given for 18 (eighteen) questions with the status of "Not Done" based on the results of the KAMI Index 5.0 assessment on PT. QAZ. Recommendations for improvement in the area of technology and information security were given for 6 (six) questions with the status of "Not Done" based on the results of the KAMI Index 5.0 assessment on PT. QAZ. Recommendations for improving the area of personal data protection were given for 11 (eleven) questions with the status of "Not Done" based on the results of the KAMI Index 5.0 assessment at PT. QAZ. Recommendations for supplement improvement were given for 19 (nineteen) questions with the status of "Not Done" based on the results of the KAMI Index 5.0 assessment on PT. QAZ. This recommendation is made with reference to the ISO/IEC 27001:2022 standard

The improvement recommendations prepared in this study are the result of the researcher's interpretation of the results of the KAMI Index 5.0 assessment which is mapped with ISO/IEC 27001:2022 control, and has not gone through a formal validation process by the management of PT. QAZ and external information security experts. Therefore, before being implemented, this recommendation is recommended to be reviewed and validated with the management to ensure its suitability with the condition of resources, business priorities, and organizational capacity of PT. QAZ.

IV. CONCLUSION

The evaluation of information security readiness carried out at PT. QAZ uses the KAMI Index 5.0 instrument mapped to ISO/IEC 27001:2022 control resulting in an Electronic System Category score of 19 points, classified as a "High" category, which reflects the organization's high dependence on electronic systems in supporting its operational sustainability. The accumulated score from the six evaluation areas was recorded at 372 points out of a maximum total of 918 points, while the achievement of the supplement category only reached 26%. This condition places the level of information security maturity of PT. QAZ in the range of Level I to II, well below the minimum Level III+ threshold required to meet the ISO/IEC 27001:2022 certification standard, so the final status obtained is declared "Not Feasible". A total of 77 improvement recommendations were prepared for questions with "Not Done" status in the six evaluation areas to support improving organizational compliance in the future. However, it needs to be explicitly emphasized that all of the findings and score achievements are portraits of the specific conditions that apply to PT. QAZ as the only object of research, with distinctive governance characteristics, organizational structure, and operational context as a region-owned clean water service provider. Therefore, the results of this evaluation cannot be generalized broadly to represent the information security readiness of organizations or other sectors, and their application in different contexts requires separate studies and adjustments.

As a concluding note, it should be noted that the KAMI Index 5.0 as a measuring tool has fundamental limitations, namely its orientation which focuses more on the maturity of the implementation of policies and procedures, and has not directly measured the effectiveness of the implementation of security controls technically in the field [28]. Thus, the "Unfeasible" status obtained by PT. The QAZ in this study represents the level of readiness in terms of completeness of governance and documentation, but does not necessarily describe the actual level of technical vulnerability in the electronic system used. Further research that combines the KAMI Index 5.0 with technical testing, such as penetration testing or vulnerability assessment, is recommended to obtain a more comprehensive picture of information security readiness [29].

REFERENCE

[1] I Nyoman Adi Artha Wibawa, "Information Security Evaluation at Hospital Using Index KAMI 5 . 0 and Recommendations Based on ISO/IEC 27001 : 2022," vol. 6, no. 4, pp. 3070–3086, 2024, doi: 10.51519/journalisi.v6i4.949.

[2] T. Rochmadi and I. Y. Pasa, "Measurement of Risk and Evaluation of Information Security Using The Information Security Index in BKD XYZ Based on ISO 27001/SNI," *CyberSecurity and Digit Forensics.*, vol. 4, no. 1, pp. 38–43, 2021, doi: 10.14421/csecurity.2021.4.1.2439.

[3] D. Rohmaniah, W. M. Ashari, Lukman, and A. D. Putra, "Enhancing Website Security Using Vulnerability Assessment and Penetration Testing (VAPT) Based on OWASP Top Ten," *J. Appl. Informatics Comput.*, vol. 9, no. 2, pp. 404–411, 2025, doi: 10.30871/jaic.v9i2.9069.

[4] M. T. Akbar, R. T. Veronica, R. I. Widyana, and H. Nurahman, "Evaluation of BAWASLU ABC Information Security Readiness Evaluation of BAWASLU ABC Using KAMI Index 5 . 0," vol. 9, no. 1, pp. 88–97, 2026.

[5] A. D. Saputra, F. Dione, and I. Uluputty, "Management of Information Security and Encryption at the Communication and Information Service of East Kalimantan Province," *J. Techno. and Commun. Government.*, vol. 5, no. 2, pp. 159–187, 2023, doi: 10.33701/jtkp.v5i2.3735.

[6] F. Anis Sekar Ningrum, Y. Riwanto, I. Yanuar Risca Pratiwi, and M. A. Fikri, "Security Analysis of Higher Education Information Systems Based on OUR Index," *J. Inform. Polynesian*, vol. 10, no. 3, pp. 437–444, 2024.

[7] A. Apriany and A. Wibowo, "Analysis of the Implementation of ISO 27001: 2022 and KAMI Index in Enhancing the Information Security Management System in Consulting Firms," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 18, no. 4, pp. 417–428, 2024, doi: 10.22146/ijccs.100385.

[8] O. J. Pratomo, M. U. A. Al Huraibi, and M. Ridwan, "Evaluation of Information Security in DNY Skincare Company Based on the Information Security Index (WE) ISO/IEC 27001:2013," *Inf. Syst. Educ. Prof. J. Inf. Syst.*, vol. 10, no. 2, p. 117, 2025, doi: 10.51211/isbi.v10i2.3670.

[9] A. H. Nadanta, H. Farisi, and D. W. Brata, "Evaluation Analysis of the KAMI Index (Information Security) 5.0 in Information Security Management at SMK Telkom Purwokerto," *J. Pengemb. Technology. Inf. and Computing Science.*, vol. 9, no. 8, pp. 1–9, 2025.

[10] Y. Rahmah, W. Hayuhardika, and A. Dwi herlambang, "Evaluation of Information Security at the Communication and Information Service of Mojokerto Regency using the Information Security Index (KAMI)," *Pengemb. Technology. Inf. and Computing Science.*, vol. 3, no. 6, pp. 840–846, 2019.

[11] B. Novriyadi, M. Jazman, M. Megawati, and M. Afdal, "Evaluation of Information Security Readiness Using the KAMI Index 5.0 and ISO/IEC 27001: 2022," *Progressive J. Ilm. Computer.*, vol. 21, no. 2, pp. 573–585, 2025.

[12] M. Fadhli Ma'arif, Melwin Syafrizal, Jeki Kuswanto, and Aiko Nur Hendry Yansyah, "Security Risk Analysis of QRIS Implementation in Public Locations Using ISO 31000:2018 Framework," *J. Appl. Informatics Comput.*, vol. 9, no. 4, pp. 1670–1680, 2025, doi: 10.30871/jaic.v9i4.9877.

[13] Y. R. Rizky and H. Said, "EVALUATION OF INFORMATION SECURITY AT SMAN 1 TANGGAMUS USING OUR INDEX VERSION 4.2," vol. 13, no. 2, pp. 181–187, 2023.

[14] F. S. Wati, D. A. Prambudi, and H. I. Sunardi, "Evaluation of Information Security at XYZ University Using the KAMI Index 4.2," *Equiva J.*, vol. 2, no. 1, pp. 1–7, 2024.

[15] S. Nurul, S. Anggrainy, and S. Aprelyani, "Factors Affecting Information System Security: Information Security, Information Technology and Network (Sim Literature Review)," vol. 3, no. 5, pp. 564–573, 2022.

[16] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, "Evaluation of Information Technology Security Using the Information Security Index 5.0 and ISO/EIC 27001:2022," *J. SAINTEKOM*, vol. 14, no. 1, pp. 84–94, 2024, doi: 10.33020/saintekom.v14i1.623.

[17] G. Fitria, D. Yuniarto, and D. Setiadi, "Evaluation of the Security of the Online Regional Tax System of Sumedang Regency Using the Information Security Index 5.0," *J. Tek. Machinery, Ind. Electrical and Inform.*, vol. 4, no. 1, pp. 232–242, 2025.

[18] R. Sinaga and F. Taan, "The Application of ISO/IEC 27001:2022 in Information Systems Security Governance: Process Evaluation and Constraints," *Nuances Inform.*, vol. 18, no. 2, pp. 46–54, 2024, doi: 10.25134/ilkom.v18i2.205.

[19] S. Salisa, A. Zahra, I. Aknuranda, and H. Farisi, "Evaluation of the Maturity Level of Information Security Using the KAMI Index 5 . 0 at Universitas Darul ' Ulum Jombang," vol. 9, no. 9, pp. 1–7, 2025.

[20] D. I. Khamil, "Evaluation of Information Security Readiness Level Using Our Index 4.2 and ISO/IEC 27001:2013 (Case Study: Diskominfo Gianyar Regency)," *JATISI (Tek Journal. Inform. and Sist. Information)*, vol. 9, no. 3, pp. 1948–1960, 2022, doi: 10.35957/jatisi.v9i3.2310.

[21] A. H. Harahap, C. D. Andani, A. Christie, and A. Fauzi, "The Importance of the CIA Triad's Role in Information and Data Security for Stakeholders or Stakeholders," vol. 1, no. 2, pp. 73–83, 2023.

[22] Frangky and R. Sinaga, "The Application of ISO / IEC 27001: 2022 in Information System Security Governance: Process Evaluation and Constraints," vol. 18, pp. 46–54, 2024.

[23] Nyoman, "Information Security Risk Analysis Using the Octave Allegro Method and Analytical Hierarchy Process at the Buleleng Regency Government Data Center," 2022, *Ganesha University of Education*.

[24] G. Fitria and D. Yuniarto, "Evaluation of the Security of the Online Regional Tax System of Sumedang Regency Using the Information Security Index 5.0," vol. 4, 2025.

[25] D. I. Khamil, G. Made, A. Sasmita, A. Agung, and N. Hary, "Evaluation of Information Security Readiness Level Using Our Index 4 . 2 And ISO / IEC 27001 : 2013 (Case Study: Diskominfo Gianyar Regency)," vol. 9, no. 3, pp. 1948–1960, 2022.

[26] A. P. Putra *et al.*, "Journal Information System Audit Using COBIT 5 Framework on DSS01 and DSS05 Domains," vol. 3, no. 1, pp. 649–658, 2024.

[27] S. Watkins, "ISO/IEC 27001: 2022: An introduction to information security and the ISMS standard," 2022.

[28] A. R. Riswaya and A. Sasongko, "Using Our Index for the Preparation of the SNI ISO/IEC 27001 Standard (Case Study: STMIK Mardira Indonesia)," *J. Comput. Business*, 2020.

[29] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing on ARS University Website Using the Open Web Application Security Project (OWASP)," pp. 77–86, 2021.