Equivalent: Jurnal Ilmiah Sosial Teknik
Volume 8, Issue 2, 507-519
e_ISSN: 2775-0833
https://jurnalequivalent.id/index.php/jequi/index
DOI: doi.org/10.59261/jequi.8i2.322

Information Security Maturity Assessment Using the KAMI Index 5.0 Based on ISO/IEC 27001:2022: A Case Study of a Government Agency Under the Ministry of Finance of the Republic of Indonesia

M. Ihsan Alfani Putera[1*]
Institut Teknologi Kalimantan, Indonesia

Nana Aulia Tabita[2]
Institut Teknologi Kalimantan, Indonesia

Dwi Nur Amalia[3]
Institut Teknologi Kalimantan, Indonesia

***Corresponding author:**
M. Ihsan Alfani Putera, Institut Teknologi Kalimantan, Indonesia.
✉ihsanalfani@lecturer.itk.ac.id

Article Info:

Article history:
Received: April 17, 2026
Revised: May 15, 2026
Accepted: June 5, 2026

Keywords:
Information Security Index (KAMI) 5.0, ISO/IEC 27001:2022; Information Security; XYZ Agency.

Abstract

Background: XYZ Agency has adopted information technology but faces phishing attacks, spam, unclear information security roles, and a lack of prior security evaluation. Therefore, its readiness and maturity must be assessed using the *KAMI Index 5.0* and ISO/IEC 27001:2022.
Objective: This study aims to evaluate the level of information security readiness and maturity at Institution XYZ, a government agency under the Ministry of Finance of the Republic of Indonesia, using the *KAMI Index Version 5.0* aligned with ISO/IEC 27001:2022, and to formulate structured improvement recommendations.
Methods: This study employed a qualitative descriptive case study approach through interviews, observation, and document review. Data were assessed using *KAMI 5.0*, validated through triangulation and member-checking, with coder reliability confirmed by Cohen's Kappa.
Results: The assessment results obtained for the Electronic Systems Category were 29 points, indicating a high level of dependency, with a total score of 347 points across the six evaluation areas. The maturity level falls within the range of I–II, corresponding to a status of basic framework compliance. Subsequently, 97 recommendations for improvement were provided, referring to ISO/IEC 27001:2022.
Conclusion: The formulation of these recommendations is expected to assist XYZ Agency in enhancing information security management and mitigating identified risks.

To cite this article: Putera, M. I. A., Tabita, N. A., & Amalia, D. N. (2026). Information Security Maturity Assessment Using the KAMI Index 5.0 Based on ISO/IEC 27001:2022: A Case Study of a Government Agency Under the Ministry of Finance of the Republic of Indonesia. *Equivalent: Jurnal Ilmiah Sosial Teknik*, 8(2), 507-519. https://doi.org/10.59261/jequi.v8i2.322

INTRODUCTION

The development of information technology over the last few decades has progressed at a remarkable pace and has had a broad impact on various sectors of life, including the government sector. Digital transformation is no longer merely an option but has become a fundamental necessity for supporting the effectiveness of modern organizations. In the context of government, the use of information technology plays a crucial role in enhancing the quality of public services through more integrated and faster systems capable of reaching a wide community. This aligns with the view that bureaucratic digitalization can accelerate administrative processes and increase transparency in governance (Diva et al., 2020; Sugiantoro, 2025).

The use of information technology in the public sector also presents significant opportunities for managing data and information at a more complex scale. Information systems enable government agencies to access, process, and distribute information in real-time with higher accuracy compared to conventional methods. This positive impact further supports the

creation of good governance, particularly regarding transparency, accountability, and the efficiency of public services. Government policy through the implementation of the Electronic-Based Government System (SPBE) represents a concrete effort to encourage the optimization of information technology within government agencies.

Moreover, efforts to accelerate digital transformation in Indonesia are reinforced through strategic policies emphasizing the integration of national digital services. These regulations not only aim to improve service quality but also ensure alignment between systems across various government agencies. With this integration, operational efficiency and enhanced data-driven decision-making are expected. However, the successful implementation of digital transformation depends not only on technology availability but also on human resource readiness and adequate system governance (Afiansyah & Kadarwati, 2023).

Conversely, the increased use of information technology in public services is accompanied by a heightened potential for information security risks. Cyber threats are a major challenge that modern organizations, particularly government agencies managing strategic and sensitive data, must confront. These risks can include data breaches, operational disruptions, and the misuse of information that could harm both the institution and the public. Therefore, information security is a critical aspect that cannot be overlooked in information system management (Putri et al., 2022).

The concept of information security fundamentally focuses on protecting information assets from various internal and external threats. In practice, information security refers to three primary principles known as the CIA Triad: Confidentiality, Integrity, and Availability. These principles form the foundation for designing security systems capable of maintaining data confidentiality, ensuring information accuracy, and guaranteeing system availability when required by authorized users (Gupta et al., 2026). The application of these principles is increasingly essential for government agencies responsible for safeguarding public data.

The urgency of implementing information security is further reinforced by national regulations governing information security systems. Every electronic system operator is mandated to adhere to specific security standards to minimize the risk of cyberattacks and operational disruptions. This regulation emphasizes that information security is not only a technical responsibility but also a component of organizational governance that must be systematically planned and executed (Suyahman, 2025).

Based on empirical evidence obtained through interviews, it is known that Institution XYZ has leveraged information technology to support operations and public services. Monitoring and evaluation activities have also been conducted regularly to ensure business process continuity and compliance with standard operating procedures. However, the implementation of these activities still primarily focuses on operational aspects and has not specifically measured the level of information security. This indicates a gap between information system management and its security aspects (Magnusson et al., 2025).

Furthermore, Institution XYZ has experienced security incidents, such as phishing attacks and spam emails targeting internal users. Phishing attacks typically employ social engineering techniques that exploit user negligence to obtain sensitive information, including account credentials or other critical data. Emails mimicking official entities are often used in these attacks, making them difficult for users to detect (Puspitasari & Sutabri, 2023; Putra, 2021). These incidents demonstrate that cyber threats are not merely theoretical but have tangible potential to cause serious impacts.

This situation is exacerbated by the absence of a clear division of responsibilities related to information security management within Institution XYZ. The lack of dedicated personnel or units for information security results in suboptimal monitoring and risk mitigation processes. Additionally, a comprehensive information security evaluation has never been conducted, leaving potential security gaps unidentified. This highlights the need to enhance the organization's capacity to manage information security (Bahary & Sugiantoro, 2024).

From an internal policy perspective, restricting third-party involvement in system development aims to maintain control over data and systems. However, this policy also introduces challenges, particularly concerning limited human resources and technical expertise in

information security. Without sufficient expert support, the management of information security systems may be suboptimal, increasing vulnerability risks (Hidayat & Bakhtiar, 2023).

Additional issues are observed in the information technology supporting infrastructure, particularly regarding server room facilities that do not fully comply with security standards. Environmental factors, such as temperature, humidity, and physical security measures, play a critical role in maintaining technological device reliability. Non-compliance with these standards can increase the risk of equipment damage, operational disruptions, and data loss, potentially harming the organization (Jelita et al., 2024).

Given these challenges, a comprehensive evaluation is necessary to assess the readiness and maturity of information security at Institution XYZ. This evaluation aims to provide an in-depth overview of the actual condition of information security and to identify areas requiring improvement. One method suitable for this purpose is the Information Security Index (KAMI), an evaluation tool developed by the National Cyber and Crypto Agency (BSSN) referencing the international standard ISO/IEC 27001 (Wibawa et al., 2024).

The latest version of the KAMI Index, version 5.0, has been adapted to reflect updates in the ISO/IEC 27001:2022 standard and encompasses eight comprehensive evaluation areas. Using this method enables organizations to measure information security maturity systematically and structurally. Furthermore, evaluation results provide a foundation for formulating sustainable improvement recommendations (Firmansyah & Nugroho, 2024).

According to ISO/IEC 27002 Leme et al. (2026), information security is a method of protecting information from various types of threats to ensure business continuity, minimize business risks, and optimize investment returns. Information security is a process aimed at maintaining the security of data or information assets from external threats that could potentially compromise the confidentiality, integrity, and availability of data, which can have a serious impact on an organization (Souhoka et al., 2025). Therefore, to minimize threats from external parties, an information security evaluation aligned with national or international standards is required. Information security management encompasses three main aspects: confidentiality, integrity, and data availability, commonly referred to as the CIA triad (Harahap et al., 2023).

According to ISO 27001, in the implementation of information security, the CIA Triad serves as the primary principle guiding individuals or organizations in designing procedures, policies, systems, or applications related to information security. The CIA Triad is an acronym for Confidentiality, Integrity, and Availability. The explanation of each CIA aspect are confidentiality; the process of maintaining the secrecy of data and ensuring that only authorized personnel can access it. Integrity; the wholeness and accuracy of information or data within a processing system, meaning information must remain intact and not be altered or manipulated without proper authorization. Availability: ensures that information and systems are accessible and usable at any time by authorized parties.

ISO 27001 is a globally recognized international standard for information security, developed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to help organizations safeguard their information assets. This standard serves as a reference for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS) (Anteng, 2026). Furthermore, this standard is the primary reference for auditing and certifying an organization's information security framework (Alrehili & Alhazmi, 2023). ISO 27001 was first published in 2005, updated in 2013, and most recently revised in October 2022 as ISO/IEC 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Controls. Compared to ISO/IEC 27001:2013, the 2022 update provides more detailed guidance regarding information security, cybersecurity, and privacy protection.

This updated version can be applied during the transition period from ISO/IEC 27001:2013, and organizations are encouraged to adapt to the new ISO standard (Pathirana & Wilenius, 2025). ISO/IEC 27001:2022 emphasizes the protection of sensitive information with strategic value to an organization. The standard is designed to help organizations build, implement, operate, monitor, maintain, and improve an information security management system. Compared to the previous version, ISO/IEC 27001:2022 introduces structural and

content changes, revisions to the number of control categories, enhanced privacy protection, updates to Annex A, and adjustments to the number of security controls (Rojabi, 2025).

The Information Security Index (KAMI) is an application designed to assist in assessing and evaluating the level of readiness, covering both completeness and maturity, in the implementation of information security in accordance with the SNI ISO/IEC 27001 standard. The KAMI Index aims to visualize the readiness condition (completeness and maturity) of the information security framework for agency leaders and can be used periodically to provide a clear overview of the development of information system security within the agency (Rojabi, 2025).

The Information Security Index (KAMI) evolves with technological advancements and updates to ISO/IEC 27001, leading to the release of the latest version, Information Security Index (KAMI) Version 5.0. Version 5.0 comprises eight evaluation areas: (1) Electronic System (ES) Category, (2) Information Security Governance Area, (3) Information Security Risk Management Area, (4) Information Security Management Framework Area, (5) Information Asset Management Area, (6) Information Technology and Security Area, (7) Personal Data Protection Area, (8) Supplements

In the assessment process for all areas of the Information Security Index (KAMI) Version 5.0, there are five main maturity levels, Level I: Initial Condition, Level II: Basic Framework Implementation, Level III: Defined and Consistent, Level IV: Managed and Measured, and Level V: Optimal

With four additional maturity levels, namely I+, II+, III+, and IV+, the KAMI 5.0 Index encompasses a total of nine maturity levels. At the initial stage, agencies conducting this evaluation are assigned a maturity category of Level I. The minimum level required by ISO/IEC 27001 for certification readiness is Level III+. After all areas are assessed, Information Security Index (KAMI) Version 5.0 produces a final score visualized in the form of a radar chart.

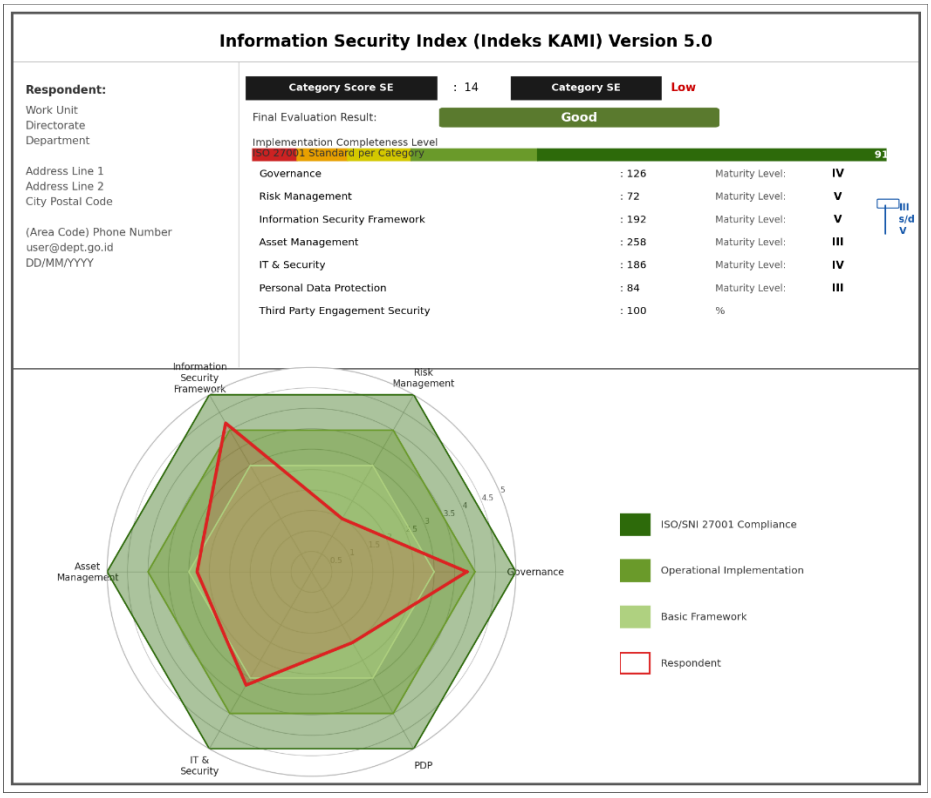

Figure 1. KAMI 5.0 Index Dashboard
Source: research data

Despite a growing body of literature on KAMI Index evaluations in Indonesian public institutions (Bahary & Sugiantoro, 2024; Diva et al., 2020; Jelita et al., 2024), a critical research gap remains: no prior study has applied KAMI Index 5.0 in a sub-ministerial fiscal or customs

government agency that simultaneously faces high electronic system dependency, restrictive third-party access policies, and an absence of dedicated information security personnel. Most existing studies utilize the earlier KAMI 4.2 version (Hidayat & Bakhtiar, 2023) or examine agencies with more established IT governance structures. Moreover, previous studies rarely link assessment outcomes to specific ISO/IEC 27001:2022 control clauses, limiting the applicability of recommendations for institutions seeking formal certification.

The novelty of this study is threefold: (1) it provides the first documented KAMI 5.0 baseline assessment for a sub-ministerial fiscal government institution in Indonesia, offering sector-specific benchmarking data previously absent from the literature; (2) it employs a multi-source validated data collection protocol (interviews, observations, document reviews) confirmed by institutional representatives, enhancing result reliability beyond single-method approaches; and (3) all 97 improvement recommendations are explicitly mapped to ISO/IEC 27001:2022 control clauses, providing a direct actionable pathway toward certification readiness. This study therefore contributes both empirically and practically to information security management in the Indonesian public sector.

Thus, this research aims to evaluate the maturity and readiness level of information security at Institution XYZ using the KAMI Index version 5.0. The results are expected to yield strategic recommendations that the institution can use to improve information security management sustainably and to support the development of a safer, more effective, and trustworthy government system (Beri, 2022; Wijaya, 2021).

METHOD

This study employed a qualitative descriptive research design using a single-case study approach. Data were collected from seven purposively selected key informants at Institution XYZ: one Head of the IT Work Unit, four IT technical staff members, and two administrative staff responsible for data management. Informants were selected based on their direct involvement in IT system operations and information security activities.

Three complementary data collection techniques were employed: (1) semi-structured interviews guided by the KAMI 5.0 questionnaire; (2) direct observation of server room facilities, network infrastructure, and daily security practices; and (3) document review of internal IT policies, system logs, and existing security procedures.

The KAMI 5.0 assessment instrument, comprising 201 questions across eight evaluation areas, served as the primary research instrument. Each question was scored on four implementation status levels: Not Implemented (0), In Planning (1), Partially Implemented (2), and Fully Implemented (3). A "Not Applicable/Relevant" option was provided for specific questions.

Data validity was ensured through source triangulation and member-checking, in which all assessment results were reviewed and confirmed by an institutional representative from Institution XYZ. Reliability was assessed through inter-rater agreement between two independent researchers who coded the same interview transcripts, yielding a Cohen's Kappa coefficient of $\kappa = 0.84$, indicating strong agreement.

Ethical approval for this study was obtained prior to data collection. All participants provided written informed consent and were assured of confidentiality and anonymity throughout the research process.

The following were the stages in conducting information security assessment and evaluation at Institution XYZ:

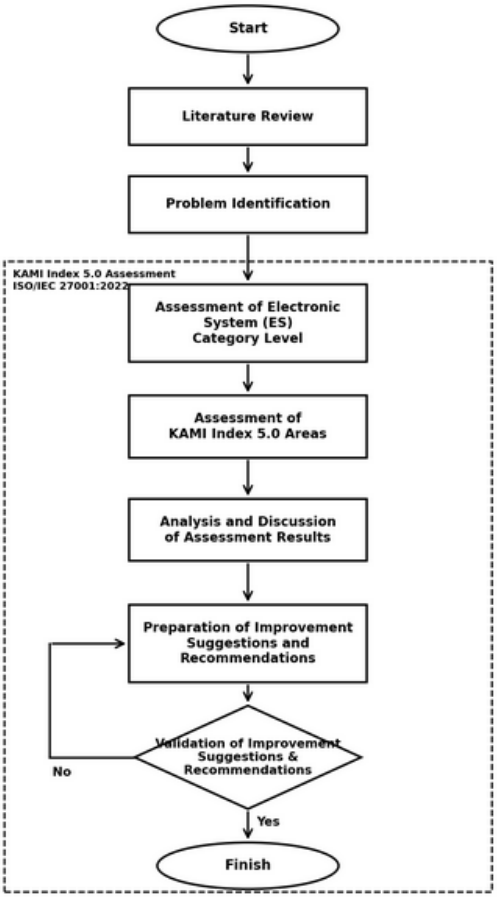

Figure 2. Research Method
Source: research data

Literature Study

This stage involved conducting a literature study by collecting relevant theories from articles, journals, books, and theses related to information security, the Information Security Index (KAMI), ISO/IEC 27001, and the technical assessment of KAMI Index areas.

Problem Identification

Problem identification was carried out through an interview process with sources from Institution XYZ. This stage aimed to understand the current conditions and to obtain data from Institution XYZ.

Assessment of Electronic System (ES) Category Level

This stage assessed the Electronic System category by asking several questions categorized into low, high, and strategic levels. At the end of this stage, all responses were accumulated and used to determine the dependency category that matched the current conditions of Institution XYZ.

Assessing the Information Security Index (KAMI) 5.0 Areas

The next stage involved assessing all evaluation areas of the Information Security Index (KAMI) 5.0, which included six main areas with different numbers of questions in each area: information security governance with 22 questions, information security risk management with 16 questions, information security management framework with 32 questions, information asset management with 53 questions, information technology and security with 35 questions, personal data protection with 16 questions, plus a supplement of 27 questions. The assessment was conducted using interviews and direct observations with the relevant work units at Institution XYZ to obtain comprehensive data that reflected actual field conditions. Each area and the

supplement were assessed based on four implementation status levels: not implemented, in planning, partially implemented, and fully implemented. The results of this assessment produced a maturity and readiness score for information security in each evaluation area, which was then used to map the overall information security condition and served as a basis for formulating sustainable improvement recommendations.

Analysis and Discussion of Assessment Results

The data presented on the evaluation dashboard were analyzed to assess the level of readiness and maturity of information security at Institution XYZ. The KAMI Index dashboard displayed the total score of the Electronic System (ES) category, the assessment results for each area, and the final evaluation score as the basis for analysis. The final score from the six evaluation areas determined the maturity level of information security, while the results in the supplement area were presented as a percentage. All analysis results were then verified to ensure their conformity with the ISO/IEC 27001:2022 standard, supported by graphical visualizations and detailed calculations that reinforced the reliability of the evaluation results.

Formulation of Suggestions and Improvement Recommendations

The final stage involved formulating suggestions and improvement recommendations based on ISO/IEC 27001:2022 and aligned with the results of the conducted analysis. These suggestions and recommendations were provided and validated by Institution XYZ so they could be used as considerations and references for improving and developing the existing systems and IT infrastructure.

RESULTS AND DISCUSSION

Assessment of Electronic System (ES) Category Level

The first step involved assessing the Electronic System (ES) category level through interviews with relevant sources. This assessment was conducted to determine the extent of electronic system utilization at Institution XYZ. The results of the assessment are presented in Table 1.

Table 1. Results of Electronic System (ES) Category Level Assessment

Part I: Electronic System Category			
Number of Electronic System (ES) Questions:			**10**
Interview Results			
Implementation Status	**Number of Questions**	**Score**	**Total Score**
[A]	4	5	20
[B]	3	2	6
[C]	3	1	3
Total Score for Electronic System (ES) Category :			**29**
		Dependency Level :	**High**

Source: research data

Based on Table 1, a total score of 29 points was obtained, which falls into the "High" dependency level, indicating that the Electronic System (ES) plays a critically important role in supporting business processes, services, and daily operations at Institution XYZ.

Assessment of Six Information Security Areas and Supplements

This was followed by an assessment of the six information security areas. In this assessment, questions were posed according to each area being evaluated. The Information Security Index (KAMI) Version 5.0 comprises six evaluation areas with one supplementary category. Each question has four possible response statuses: "Not Implemented," "In Planning," "Partially Implemented," and "Fully Implemented," with an additional option, "Not Applicable/ Relevant," for specific conditions in certain questions. The assessment results are presented in Table 2.

Table 2. Results of All Evaluation Areas Assessment

Evaluation Area	Score	Number of Questions	Maturity Level
Information Security Governance	43	22	I+
Information Security Risk Management	34	16	I+
Information Security Management Framework	34	32	I
Information Asset Management	79	53	I+
Information Technology and Security	111	35	II
Personal Data Protection	46	16	I+
Supplement	6% = 0,19	27	-

Source: research data

Table 2 shows the lowest maturity level in the KAMI 5.0 Index evaluation is in the Information Security Management Framework area, with a score of 34 at Maturity Level I, whereas the highest maturity level is in the Information Technology and Security area, with a score of 111 at Maturity Level II.

The assessment results for the Supplement category indicate that the implementation of information security related to third-party involvement in service provision has not been fully executed at the work unit level of Institution XYZ. This limitation is due to the dominant role of the head office in managing systems, infrastructure, and information technology services, as well as the constrained operational authority of Institution XYZ in overseeing third-party information security aspects.

Analysis and Discussion of Assessment Results

After assessing all areas of the Information Security Index (KAMI) 5.0, the next step is to analyze the evaluation results for Institution XYZ based on the dashboard visualization displaying the scores for each assessment area.

Figure 3. Institution XYZ Assessment Dashboard

Source: research data

Based on Figure 3, the completeness level of the implementation of the ISO/IEC 27001:2022 standard at Institution XYZ obtained a score of 347 points, with the final evaluation result for information security readiness status being "Inadequate" and the maturity level ranging from I to II. This condition indicates that the maturity level of Institution XYZ has not met the minimum threshold standard for ISO/IEC 27001:2022 certification, which is Maturity Level III+, so systematic and sustainable efforts are needed to improve information security at Institution XYZ.

Formulation of Suggestions and Improvement Recommendations

Suggestions and improvement recommendations were formulated based on the ISO/IEC 27001:2022 standard and the assessment statuses of "Not Implemented" and "In Planning." A total of 97 recommendations were formulated for Institution XYZ according to its condition, and

validation was carried out with a representative from Institution XYZ confirming that all formulated suggestions and improvement recommendations align with the internal conditions of Institution XYZ. It is hoped that the entire evaluation process, along with the formulated suggestions and improvement recommendations, can serve as a guide for improving information security management within Institution XYZ.

Discussion

Analysis of Electronic System (ES) Category Level

The assessment results for the Electronic System (ES) category at Institution XYZ show a score of 29 points, classified as a high dependency level. This finding indicates that almost all operational activities, both in public services and internal business processes, are highly dependent on technology-based information systems. In the context of modern organizations, this condition is unsurprising, considering that digital transformation has become a primary foundation for improving service efficiency and speed. However, a high dependency level also carries significant risk consequences, especially if the system is not supported by adequate security management (Diva et al., 2020; Sugiantoro, 2025).

High dependency on electronic systems reflects that even minor system disruptions can significantly impact service continuity. This indicates that the electronic system at Institution XYZ has become a critical asset that not only supports but also determines the smoothness of organizational operations. Under such conditions, the information system is no longer complementary but has become the main infrastructure whose sustainability must be maintained. Therefore, the approach to system management should not focus solely on functional aspects but must also comprehensively cover security aspects (Beri, 2022; Wijaya, 2021).

From the perspective of information technology governance, a high level of dependency should be balanced with the organization's readiness to anticipate various potential risks. These risks may include system failures, cyber-attacks, and human errors that could disrupt operations. Thus, the results of this assessment serve as an initial indication that Institution XYZ requires a more comprehensive security strategy to maintain the stability of the system that serves as its operational backbone (Putri et al., 2022).

Furthermore, the distribution of scores in categories A, B, and C also shows variations in the level of electronic system implementation across different aspects. This indicates that, although dependency is generally high, not all system components are at the same optimal level. This disparity can potentially create security gaps if not identified and addressed systematically. Therefore, standardization efforts in electronic system management are needed so that all components can operate harmoniously and in an integrated manner (Afiansyah & Kadarwati Febriyani, 2023).

Analysis of Six Information Security Areas and Supplements

The evaluation results for the six information security areas show that most areas are still at the initial maturity levels, namely Levels I and I+. This condition illustrates that the implementation of information security at Institution XYZ is still at a basic stage and not yet optimally structured. Although some security practices have begun to be implemented, their execution is inconsistent and not supported by strong policies. This aligns with the findings of Bahary and Sugiantoro (2024), who state that many public sector organizations are still in the early stages of implementing information security.

The information security governance area obtained a score of 43 with a maturity level of I+, indicating that the organization has an initial awareness of the importance of information security. However, this awareness has not been fully translated into formal policies and structured monitoring mechanisms. In practice, weak governance can lead to a lack of clear direction in information security management, causing each work unit to operate partially without optimal coordination (Suyahman, 2025).

In the information security risk management area, the score obtained was also at Level I+, indicating that the risk identification and mitigation processes have not been carried out systematically. Risk management is an essential element of information security as it serves as the

basis for determining security priorities. Without effective risk management, organizations tend to be reactive in facing threats rather than proactive in preventing them (Putri et al., 2022).

The area with the lowest maturity level is the information security management framework, which is at Level I. This indicates that Institution XYZ does not yet have a clear structure of policies and procedures for managing information security. The absence of a mature framework can lead to inconsistencies in the application of security controls and make it difficult for the organization to conduct evaluations and implement continuous improvements. This condition is a serious concern because the framework is the main foundation of an information security management system (Anteng, 2026).

Conversely, the information technology and security area shows relatively better results with a maturity level of II. This indicates that, technically, Institution XYZ has begun to implement some security controls, such as using security software or network protection systems. However, this technical advantage is not yet balanced with adequate governance and policies, so its effectiveness is still limited. This condition is often observed in organizations that focus more on technical solutions without addressing managerial aspects (Jelita et al., 2024).

In the personal data protection area, the maturity level at I+ indicates that the management of sensitive data is not yet fully aligned with expected standards. In today's digital era, personal data protection is a crucial issue, especially for government agencies handling public data. Weaknesses in this aspect can lead to a loss of public trust and potential legal violations (Wibawa et al., 2024).

Meanwhile, the result for the supplement category, which only reached 6%, indicates that third-party involvement in information security is still very limited. This is due to the dominant role of the head office in system management, meaning work units have limited capacity to manage security aspects independently. This condition can become an obstacle in developing adaptive and locally responsive security systems (Hidayat & Bakhtiar, 2023).

Analysis of Information Security Maturity and Readiness Level

Overall, the evaluation results show that Institution XYZ obtained a total score of 347 points with a maturity level in the range of I–II and an "Inadequate" status. This result confirms that the implementation of information security at Institution XYZ is still far from the minimum standard set by ISO/IEC 27001:2022, which requires maturity Level III+. In other words, the organization is still in the early stages of building a structured and sustainable information security system (Anteng, 2026).

The "Inadequate" status is not just a label but reflects significant risks that could threaten the sustainability of systems and services. In this condition, the organization does not yet have adequate readiness to face increasingly complex cyber threats. This is reinforced by the fact that Institution XYZ has experienced phishing attacks, indicating that the existing security system has not been able to provide optimal protection (Puspitasari & Sutabri, 2023; Putra, 2021).

Upon further analysis, the gap between the high level of system dependency and the low level of security maturity is the main issue in this study. High dependency should be accompanied by a correspondingly high level of security, but in this case, there is an imbalance that could create significant risk. This condition is often referred to as the "high dependency–low security gap," which is a major challenge in organizational digital transformation (Afiansyah & Kadarwati, 2023).

Furthermore, the low maturity level indicates that information security implementation has not yet become a primary organizational priority. Contributing factors may include limited human resources, lack of understanding regarding information security, and the absence of specific policies governing it. Therefore, a paradigm shift is needed to view information security as a strategic investment rather than merely a cost burden (Suyahman, 2025).

The formulation of improvement recommendations in this study shows that many aspects need enhancement in the management of information security at Institution XYZ. The considerable number of recommendations reflects the complexity of the problems faced while also indicating that improvement efforts must be carried out gradually and sustainably. A systematic approach is needed to ensure that each recommendation can be implemented

effectively (Wibawa et al., 2024).

The recommendations formulated refer to the ISO/IEC 27001:2022 standard, which emphasizes the importance of integrating policies, procedures, and technical controls within an information security management system. Implementing this standard aims not only to improve security but also to build an organizational culture aware of the importance of information protection. Thus, successful implementation depends not only on technology but also on the commitment of all organizational elements(Jelita et al., 2024) .

Comparing these findings with Diva Ramadhani et al. (2020), who reported an average KAMI score of 312 for a district-level communications agency, Institution XYZ's total score of 347 is marginally higher, suggesting a slightly more advanced baseline implementation (Sugiantoro, 2025). Nevertheless, both institutions remain substantially below the ISO/IEC 27001:2022 certification threshold of Maturity Level III+. Jelita et al. (2024) similarly found that Indonesian government institutions applying KAMI 5.0 clustered between Levels I and II, confirming a systemic pattern rather than an institution-specific failure. Theoretically, these findings align with the Capability Maturity Model Integration (CMMI) framework, which posits that organizations progress through defined, managed, and optimized maturity stages sequentially. Institution XYZ's Level I–II range positions it in the Initial-to-Managed transition, indicating that while ad hoc security practices exist, they lack the formalization and consistency characteristic of higher maturity levels (Anteng, 2026). The disparity between higher scores in Information Technology & Security (Level II) and lower scores in the Information Security Management Framework (Level I) reflects what Suyahman (2025) terms "technical-governance decoupling" where organizations invest in technological solutions without commensurate investment in policy, training, and organizational structures. Practically, this study demonstrates that Information Security Maturity Assessment Using the KAMI Index 5.0 Based on ISO/IEC 27001:2022: A Case Study of a Government Agency Under the Ministry of Finance of the Republic of Indonesia, when combined with multi-source data collection and ISO/IEC 27001:2022-mapped recommendations, functions as an effective diagnostic and strategic planning tool for resource-constrained government institutions.

Validation of the recommendations by the institution indicates that the results of this study are relevant to actual field conditions. This is an added value because the recommendations provided are not merely theoretical but can be directly applied according to the organization's needs. However, the main challenge lies in the consistency of implementation, as changes in the information security system require time, resources, and strong management support (Hidayat & Bakhtiar, 2023). Overall, the resulting recommendations are expected to serve as a roadmap for improving the maturity level of information security at Institution XYZ. With proper implementation, the organization is expected to achieve a higher maturity level, thereby meeting international standards and increasing public trust in the services provided (Beri, 2022; Wijaya, 2021).

CONCLUSION

This study evaluated the information security maturity of Institution XYZ, a government agency under the Ministry of Finance of Indonesia, using the KAMI Index 5.0 framework aligned with ISO/IEC 27001:2022. The evaluation yielded a total score of 347 points, placing Institution XYZ at an Inadequate status with maturity levels ranging from I to II, confirming that the institution has not yet met the minimum ISO/IEC 27001:2022 certification threshold of Maturity Level III+.

The scientific contribution of this study lies in providing the first KAMI 5.0 baseline assessment for a sub-ministerial fiscal government institution in Indonesia, offering sector-specific benchmarking data and demonstrating the framework's diagnostic value in resource-constrained government settings. A total of 97 improvement recommendations were formulated and validated by institutional representatives, providing Institution XYZ with a structured, prioritized roadmap toward ISO/IEC 27001:2022 certification readiness. For policy, this study recommends that the Ministry of Finance mandate regular KAMI Index assessments for all subordinate agencies and establish dedicated information security functions within each work

unit. For practice, Institution XYZ should prioritize establishing a formal information security governance structure, followed by the development of a risk management framework and sustained personnel capacity building in cybersecurity.

This study is subject to several limitations. First, the case study design limits generalizability to other government agencies, as findings reflect the condition of a single institution at a specific point in time. Second, reliance on self-reported interview data introduces potential social desirability bias, which was partially mitigated through source triangulation and member checking. Third, institutional anonymization constrains scientific reproducibility. Future research should: (1) conduct longitudinal KAMI assessments to track maturity progress following the implementation of the recommendations generated in this study; (2) compare KAMI 5.0 assessments across multiple subordinate agencies under the Ministry of Finance to enable cross-institutional benchmarking; (3) integrate quantitative vulnerability scanning tools alongside KAMI qualitative assessments for a more comprehensive evaluation of security posture; and (4) examine the relationship between KAMI maturity levels and actual cybersecurity incident rates to validate the framework's predictive validity.

ACKNOWLEDGEMENT

The authors express gratitude to all staff members of Institution XYZ who participated in interviews, provided access to documents, and supported the field observations. Their cooperation was essential for collecting accurate and comprehensive data on the agency's information security practices.

AUTHOR CONTRIBUTION STATEMENT

M. Ihsan Alfani Putera led the study design, data collection, and analysis. Nana Aulia Tabita and Dwi Nur Amalia contributed to drafting the manuscript. All authors reviewed, revised, and approved the final manuscript, ensuring the accuracy and integrity of the research findings.

REFERENCES

Afiansyah, H. G., & Kadarwati, F. N. A. (2023). Penyusunan Kebijakan Pengamanan Dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 Dan ISO/IEC 27001:2022. *Info Kripto*, *17*(3). https://doi.org/10.56706/Ik.V17i3.81

Alrehili, A. A., & Alhazmi, O. H. (2023). ISO/IEC 27001 Standard: Analytical And Comparative Overview. *International Conference On Advances In Data-Driven Computing And Intelligent Systems*, 143–156.

Anteng, S. L. A. (2026). Peran ISO 9001 Dan ISO 27001 Dalam Meningkatkan Customer Satisfaction & Trust Di Perusahaan IT PT XYZ. *Prosiding Seminar Praktik Keinsinyuran VII Tema Peran Insinyur Profesional Dalam Reka Cipta Solusi Berkelanjutan Berbasis Environmental, Social, And Governance (ESG)*, 32.

Bahary, M. Syaiful, & Sugiantoro, B. (2024). Evaluasi Tingkat Keamanan Indeks Kami (Studi Kasus : Universitas X). *Cyber Security Dan Forensik Digital*, *7*(2), 90–94. https://doi.org/10.14421/Csecurity.2024.7.2.4634

Beri, N. (2022). *Paper_Beri Novriyadi - Beri Novriyadi*.

Diva R. N., Hayuhardhika N. P. W., & Dwi, H. A. (2020). *Evaluasi Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kabupaten Malang Menggunakan Indeks Kami (Keamanan Informasi)*. 4(5). http://J-Ptiik.Ub.ac.id

Firmansyah, F., & Nugroho, A. (2024). Analisis Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Versi 5.0. *Jurnal Borneo Informatika Dan Teknik Komputer*, *4*(2), 13–21.

Gupta, A., Gupta, S., Sharma, S., Singh, J., Ali, F., & Kwak, D. (2026). A Privacy Preserving Optimized Intelligent Security Framework For Smart Homes Using Zero Trust Architecture And Explainability. *Scientific Reports*.

Harahap, A. H. H., Andani, C. D., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan Cia Triad Dalam Keamanan Informasi Dan Data Untuk Pemangku Kepentingan Atau Stakholder. *Jurnal Manajemen Dan Pemasaran Digital*, *1*(2), 73–83.

https://doi.org/10.38035/Jmpd.V1i2.34

Hidayat, F. S., & Bakhtiar, A. (2023). Evaluasi Sistem Manajemen Keamanan Informasi Berdasarkan Penilaian Indeks Kami V. 4.2 Pada Dinas Xyz Provinsi Jawa Tengah. *Industrial Engineering Online Journal*, *12*(4).

Jelita, L. D. A., Al Azam, M. N., & Nugroho, A. (2024). Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 Dan ISO/EIC 27001:2022. *Jurnal Saintekom*, *14*(1), 84–94. https://doi.org/10.33020/Saintekom.V14i1.623

Leme, R. Da S., De Souza Pinto, J., Zanon, L. G., Sigahi, T. F. A. C., Moraes, G. H. S. M. De, Moro, S. R., & Anholon, R. (2026). Information Security Management: A Fuzzy Dematel Analysis Of The New Iso/Iec 27001:2022 Controls. *Information & Computer Security*, *34*(3), 413–434. https://doi.org/10.1108/Ics-10-2024-0269

Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information Security Governance In The Public Sector: Investigations, Approaches, Measures, And Trends. *International Journal Of Information Security*, *24*(4), 177.

Pathirana, A. I. W., & Wilenius, M. (2025). *ISO 27001 And Global Privacy Compliance*.

Puspitasari, D., & Sutabri, T. (2023). Analisis Kejahatan Phising Pada Sektor E-Commerce Di Marketplace Shopee. *Jurnal Digital Teknologi Informasi*, *6*(2). https://doi.org/10.32502/Digital.V6i2.5653

Putra, Y. V. F. (2021). Modus Operandi Tindak Pidana Phising Menurut UU ITE. *Jurist-Diction*, *4*(6), 2525. https://doi.org/10.20473/Jd.V4i6.31857

Putri, T. S., Mutiah, N. M., & Prawira, D. P. (2022). Analisis Manajemen Risiko Keamanan Informasi Menggunakan Nist Cybersecurity Framework Dan Iso/Iec 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat). *Coding Jurnal Komputer Dan Aplikasi*, *10*(02), 237. https://doi.org/10.26418/Coding.V10i02.54972

Rojabi, M. A. (2025). *Jejak Evolusi Iso 27001: Dari Awal Hingga Versi 2022*. Afdan Rojabi Publisher.

Souhoka, B. A., Fadillah, R. A., Fathan, M., Meldiansah, R., Mutakin, M. I., & Fauziyah. (2025). Analisis Strategi Pencegahan Phising Studi Kasus Pada Media Sosial Facebook. *Jurnal Sistem Informasi Galuh*, *3*(1), 10–22. https://doi.org/10.25157/Jsig.V3i1.4117

Sugiantoro, B. (2025). Evaluasi Tingkat Sistem Keamanan Teknologi Informasi Menggunakan Indeks Kami Dan Cobit 5 (Studi Kasus : Ponpes Demak). *Jurnal Media Informatika [Jumin]*. https://doi.org/10.55338/Jumin.V6i4.6492

Suyahman, S. (2025). Manajemen Dan Kebijakan Keamanan Informasi. *PT Solusi Administrasi Hukum*.

Wibawa, I. N. A. A., Susila, A. A. N. H., & Pasirulloh, M. A. (2024). Information Security Evaluation At Hospital Using Index Kami 5.0 And Recommendations Based On ISO/IEC 27001:2022. *Journal Of Information Systems And Informatics*, *6*(4), 3070–3086. https://doi.org/10.51519/Journalisi.V6i4.949

Wijaya, Y. D. (2021). Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013. *Jurnal Sistem Informasi Dan Informatika (SIMIKA)*, *4*(2), 115–130. https://doi.org/10.47080/Simika.V4i2.1178