International Journal of Industrial Innovation and Mechanical Engineering

E-ISSN: 3047-4515
P-ISSN: 3047-4507

Review Articel

Evaluation of Information Security Based on KAMI Index and ISO/IEC 27001 at the XYZ Regency Communication and Information Office

Putu Pradiptha Dwipayani [1]*, Dwi Putra Githa [2], Muhammad Alam Pasirulloh [3]

[1,2,3] Universitas Udayana, Indonesia
* pradiptha.dwipa036@student.unud.ac.id

Jl. Raya Kampus Unud, Jimbaran, Kec. Kuta Sel., Badung Regency, Bali 80361

Abstract. Information security is one of the key aspects of protecting information assets. Referring to the Regulation of the Ministry of Communication and Informatics No. 4 of 2016, Electronic System Providers (PSE) are required to implement information security to safeguard public interests, public services, state administration, and national defense and security. Therefore, the XYZ Regency Communication and Information Office, as an Electronic System Provider, needs to conduct an evaluation of its information security. This study aims to assess the level of information security at the XYZ Regency Communication and Information Office using the KAMI Index version 5.0 and to provide improvement recommendations in accordance with ISO/IEC 27001:2022 controls. The KAMI Index is used as a standard evaluation tool for assessing information security readiness based on the Regulation of the National Cyber and Crypto Agency (BSSN) No. 8 of 2021. The evaluation results show that the XYZ Regency Communication and Information Office obtained a final score of 248, with a readiness status of "Not Eligible" to meet the ISO/IEC 27001:2022 standard. The maturity level of information security is in the range of Level I to II. Improvement recommendations are provided based on questionnaire results that do not yet meet the ISO/IEC 27001:2022 standards. These recommendations serve as a reference for the XYZ Regency Communication and Information Office to align its information security governance with the ISO/IEC 27001:2022 standard.

Keywords: Evaluation, Information Security, ISO/IEC 27001:2022, KAMI Index

1. INTRODUCTION

The advancement of technology opens new opportunities while simultaneously presenting challenges related to information security. In general, security is defined as a condition free from threats or risks. Meanwhile, information refers to processed or interpreted data that can be used in decision-making processes (Sutabri, 2012). Therefore, information security is a fundamental necessity and an organizational effort to protect its information assets (Yustanti et al., 2018).

One of the organizations that has implemented Information Technology (IT) is the XYZ Regency Communication and Information Office (Diskominfo). Diskominfo XYZ manages a data center that stores and processes information for all IT services. The information contained in this data center is highly valuable and critical, making confidentiality a top priority that must be secured with clear standards. Based on interviews, it was revealed that Diskominfo XYZ has not yet obtained ISO 27001 certification and has not conducted a specific evaluation of information security, despite having experienced security incidents involving access from foreign Internet Protocol (IP) addresses.

Referring to the Regulation of the Ministry of Communication and Informatics No. 4 of 2016 on Information Security Management Systems, Electronic System Providers (PSE) are required to implement information security measures to safeguard public interests, public services, state administration, and national defense and security. One of the efforts to enhance information security is through evaluation. According to the Regulation of the National Cyber and Crypto Agency (BSSN) No. 8 of 2021, Electronic System Providers (PSE) can conduct self-assessments using the KAMI Index as a

Received: March 16th, 2025
Revised: March 30th, 2025
Accepted: April 04th, 2025
Published: April 08th, 2025
Curr. Ver.: April 08th, 2025

standard evaluation tool to assess or analyze the level of information security readiness, ensuring confidentiality, authenticity, and integrity of information.

As an institution responsible for managing critical information, Diskominfo XYZ must prioritize information security. The loss or misuse of sensitive data could have serious consequences for individuals and potentially violate their privacy. Therefore, this study on Information Security Evaluation Based on KAMI Index 5.0 and ISO/IEC 27001:2022 at the XYZ Regency Communication and Information Office is necessary to assess the level of information security readiness and ensure compliance with ISO/IEC 27001:2022 standards.

2. STUDY LITERATURE

This study was conducted after analyzing several research articles used as references related to the implementation of the KAMI Index and the ISO/IEC 27001 standard. For example, Khamil et al. (2022) used the KAMI Index 4.2 and the ISO/IEC 27001:2013 standard to evaluate information security at the Gianyar Regency Communication and Information Office (Diskominfo). Additionally, Ramadhani et al. (2020) assessed information security at the Malang Regency Communication and Information Office using the KAMI Index 4.0 and the ISO/IEC 27001:2013 standard.

The primary difference between this study and previous research used as references is the application of the latest version of the KAMI Index, namely version 5.0, which was released in March 2023 by the National Cyber and Crypto Agency (BSSN), along with the most recent ISO/IEC 27001:2022 standard.

3. RESEARCH METHOD

Information Gathering Stage

The initial step in this research involved gathering information through interviews with the Head of the Cryptography and Statistics Division. The interviews aimed to obtain information regarding past information security issues at the XYZ Regency Communication and Information Office.

Literature Study Stage

The literature study process in this research involved searching for and studying fundamental theories as well as findings from previous studies related to information security governance, the KAMI Index, and ISO/IEC 27001.

Data Collection Stage

1. Respondent Selection

Respondents were selected based on their responsibilities within the institution, ensuring alignment with the questions in each category of the KAMI Index questionnaire (BSSN, 2023; Rahayu et al., 2017). Each respondent could be responsible for one or more categories in the KAMI Index questionnaire.

2. Questionnaire Completion

The selected respondents completed the questionnaire, which was designed in accordance with the KAMI Index 5.0. The questionnaire covered eight aspects, including:

- Electronic System Category
- Information Security Governance
- Information Security Risk Management
- Information Security Management Framework
- Information Asset Management
- Technology and Information Security
- Personal Data Protection
- Supplementary Aspects

Data Validation Stage

Data validation was conducted to ensure the accuracy of the questionnaire results compared to actual conditions. The validation technique used was a **checklist method**, which involved reviewing collected data and obtaining supporting evidence. The checklist verified responses where respondents answered "In Planning," "In

Implementation/Partially Implemented," or "Fully Implemented" within the evaluated aspects.

Data Analysis Stage

1. Questionnaire Result Calculation

The questionnaire results were calculated based on the KAMI Index Evaluation Tool User Guide. The calculations determined the scores for the Electronic System Category, Maturity Level, and Information Security Readiness Level.

The Maturity Level in information security includes five main levels, which have been expanded into nine levels with the addition of intermediate levels I+, II+, III+, and IV+ to provide a more detailed and refined assessment.

Table 1. Maturity Level Matrix

Maturity Level	Maturity Score for Each Area											
	Governance		Risk Management		Framework		Asset Management		Technology & Security		Personal Data Protection	
	Min	Achievement	Min	Achievement	Min	Achievement	Min	Achievement	Min	Achievement	Min	Achievement
II	12	36	14	20	15	24	39	88	18	28	8	16
III	8	14	4	8	56	84	83	118	68	92	36	48
IV	24	54	8	12	15	27	-		12	21	-	
V	-		12	18	12	18			-			

Source: KAMI Index Version 5.0 (2023)

The determination of the Maturity Level is based on the cumulative score in each area. If the cumulative score for a specific maturity level only reaches the minimum score, the Maturity Level will be upgraded to the **"+"** level of the previous Maturity Level.

Table 2. Readiness Level Status Matrix

Electronic System Category		Information Security Category		Readiness Status
Law		**Final Score**		
10	15	0	247	Not Eligible
		248	443	Basic Framework Compliance
		444	760	Fairly Good
		761	916	Good
High		**Final Score**		Readiness Status
16	34	0	387	Not Eligible
		388	646	Basic Framework Compliance
		647	828	Fairly Good
		829	916	Good
Strategic		**Final Score**		Readiness Status
35	50	0	472	Not Eligible
		473	760	Basic Framework Compliance
		761	864	Fairly Good
		865	916	Good

Source: KAMI Index Version 5.0 (2023)

The final evaluation result or Readiness Level is determined by the relationship between the final score of the Electronic System Category and the final score of the Information Security Category. Table 2 illustrates the correlation between the Electronic System Category and the Information Security Category.

2. Comparison of Evaluation Results with ISO/IEC 27001:2022

Based on the obtained results, the researchers will review the requirements of ISO/IEC 27001:2022 that have been met and those that have not. Recommendations will be provided for the unmet requirements. These recommendations serve as a reference for

the institution to align its current information security governance with ISO/IEC 27001:2022 standards**.**

4. RESULTS AND DISCUSSION

Data Collection

The data collection process was conducted by distributing the KAMI Index 5.0 questionnaire to obtain the Maturity Level and Readiness Level of information security at the XYZ Regency Communication and Information Office (Diskominfo).

Data Validation

The Electronic System Category requires supporting evidence for all question responses. The Information Security Category requires supporting evidence for responses with statuses of "In Planning," "In Implementation/Partially Implemented," as well as responses with the status "Fully Implemented." If there is no supporting evidence available in the Information Security Category, the status of the response will be downgraded to "Not Implemented."

Table 3. Validation Results of the KAMI Index Questionnaire

KAMI Index Area	Number of Questions Requiring Supporting Evidence	Number of Questions Without Supporting Evidence
Electronic System Category	10	10
Information Security Governance	22	13
Information Security Risk Management	16	15
Information Security Management Framework	22	20
Information Asset Management	36	17
Technology and Information Security	28	5
Personal Data Protection	9	6
Supplement	0	0

Results of Questionnaire Calculation

The calculation of the questionnaire resulted in a Readiness Score for the implementation of security measures in accordance with the completeness of controls in ISO/IEC 27001:2022 and the Maturity Level of the security implementation. Figure 1 shows the evaluation results of the KAMI Index areas, displaying four assessment results.

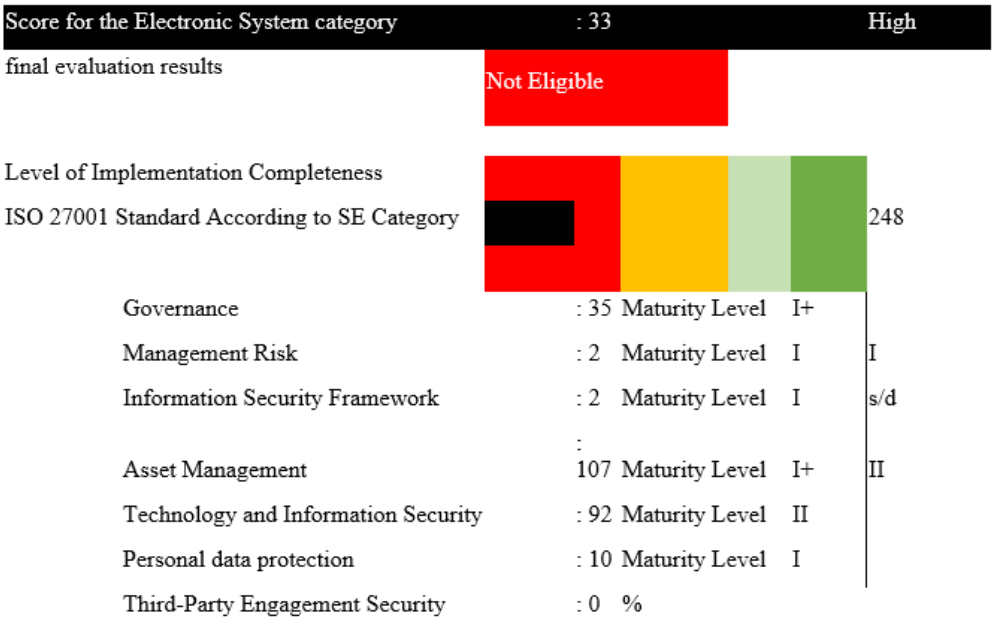

Figure 1. Evaluation Results of the KAMI Index Areas at the XYZ Regency Communication and Information Office

In the Electronic System Category, Diskominfo XYZ achieved a score of 33, categorized as High. For the Completeness Level of ISO/IEC 27001:2022 Standards Implementation, Diskominfo XYZ obtained a total score of 248, falling within the red area when summing the scores from each information security category. The final evaluation result for Diskominfo XYZ received a readiness status of "Not Eligible." Additionally, there were Maturity Level scores for each area of the Information Security Category, with Diskominfo XYZ's maturity level ranging from **Level I to II.** Based on the Maturity Level scores obtained, Diskominfo XYZ has not yet met the minimum evaluation score required to achieve Maturity Level III+.

Comparison and Recommendation of Analysis Results

Recommendations for improvement are provided based on the comparison with the controls in ISO/IEC 27001:2022. Improvement recommendations are made for the Information Security Category areas, specifically for questions with response statuses of "Not Implemented" and "In Planning," aimed at enhancing the effectiveness of information security measures.

1. **Information Security Governance**: There are 13 unmet requirements and 10 controls from ISO/IEC 27001:2022 that serve as references for developing improvement recommendations in the area of Information Security Governance.
2. **Information Security Risk Management**: There are 15 unmet requirements and 9 controls from ISO/IEC 27001:2022 that serve as references for developing improvement recommendations in the area of Information Security Risk Management.
3. **Information Security Management Framework**: There are 33 unmet requirements and 12 controls from ISO/IEC 27001:2022 that serve as references for developing improvement recommendations in the area of Information Security Management Framework.
4. **Information Asset Management**: There are 23 unmet requirements and 19 controls from ISO/IEC 27001:2022 that serve as references for developing improvement recommendations in the area of Information Asset Management.
5. **Technology and Information Security**: There are 12 unmet requirements and 7 controls from ISO/IEC 27001:2022 that serve as references for developing improvement recommendations in the area of Technology and Information Security.
6. **Personal Data Protection**: There are 27 unmet requirements and 9 controls from ISO/IEC 27001:2022 that serve as references for developing improvement recommendations in the area of Personal Data Protection.

In The Area of Supplement: There are 14 unmet requirements and 9 controls from ISO/IEC 27001:2022 that serve as references for developing improvement recommendations in the area of Information Security Governance.

5. CONCLUSION AND RECOMMENDATIONS

The XYZ Regency Communication and Information Office (Diskominfo) has conducted an information security evaluation using the KAMI Index version 5.0, achieving a score of 33 in the Electronic System Category, which falls within the "High" category, and a score of 248 in the Information Security Category, indicating that the Readiness Level is still "Not Eligible" to meet the ISO/IEC 27001:2022 standard. Based on the evaluation results, improvement recommendations have been formulated, referencing the controls in ISO/IEC 27001:2022.

The recommendations for improvement in the Information Security Governance area include conducting information security training programs. For the Information Security Risk Management area, one recommendation is to designate a risk management responsible person by defining roles according to the organizational structure. In the Information Security Framework area, a recommendation is to establish Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) in the disaster recovery planning for ICT services. For the Information Asset Management area, one recommendation is to implement regulations for secure software installation management. In the Technology and Information Security area, a recommendation is to enforce time-based access restrictions on systems and applications. For the Personal Data Protection area, one recommendation is to map the internal data processing flow and external data exchanges. Lastly, in the Supplement area, a recommendation is to form a dedicated team at the third party to manage service continuity processes.

Based on the results of the research conducted at Diskominfo XYZ, the suggestion is to strengthen the implementation of information security that has not yet met the ISO/IEC 27001:2022 standards by considering the improvement recommendations. Future research could also explore evaluations using other methods or frameworks to gain a more comprehensive and in-depth perspective on information security.

REFERENCES

(1). Bakhtiar, A. & Salsabila Hidayat, F. 2023, 'EVALUASI SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN PENILAIAN INDEKS KAMI v.4.2 PADA DINAS XYZ PROVINSI JAWA TENGAH', Industrial Engineering Online Journal, vol. 12, no. 4

(2). Barani, G.D.S. 2020, 'Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI (Keamanan Informasi) 4.0 (Studi Kasus : Dinas Komunikasi dan Informatika Provinsi Jawa Timur)', vol. 4, no. 9, hh. 3218-3224

(3). BSSN 2023, *Konsultasi dan Assessment Indeks KAMI*. Badan Siber dan Sandi Negara.

(4). Diva Ramadhani, N. 2020, 'Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)', Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 4, no. 5, hh. 1490-1490

(5). Firdani, A. 2019, 'Perencanaan Pengelolaan Keamanan Informasi Berbasis ISO 27001 menggunakan Indeks KAMI Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Rembang', Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 3, no. 6, hh. 6009-6015

(6). Gala, R.A.P.P. 2020, 'Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI', *Jurnal Teknik Informatika*, vol. 15, no. 3, hh. 189–198.

(7). Insan Khamil, D. 2022, 'Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 Dan ISO/IEC 27001:2013 (Studi Kasus: Diskominfo Kabupaten Gianyar)', *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no. 3, hh. 1946-1960

(8). Octaviani, S.I.D. 2019, 'Evaluasi Kesiapan Kerangka Kerja Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Batu Dengan Menggunakan Indeks KAMI', *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 3, hh. 2741-2745

(9). Pratiwi, H.A. & Wulandari, L. 2021, 'Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor', *Journal of Industrial Engineering & Management Research*, vol. 2, no. 5, hh. 146-163

(10). Rahayu, I., Miftach, F. & Haryatno 2017, *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI)*. Direktorat Keamanan Informasi & Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika.

(11). Rahmah, Y. 2020, 'Evaluasi Tingkat Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto dengan Menggunakan Indeks KAMI', *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 4, no. 3, hh. 840-847

(12). Shimels, T. & Lessa, L. 2023, 'Maturity of information systems' security in Ethiopian banks: case of selected private banks', *International Journal of Industrial Engineering and Operations Management*, vol. 5, no. 2, hh. 86–103.

(13). Sundari, P. & Wella 2021, 'SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)', *Ultima InfoSys : Jurnal Ilmu Sistem Informasi*, vol. 12, no. 1, hh. 35-42

(14). Sutabri, T. 2012, *Analisis Sistem Informasi*. Diedit oleh C. Putri. Penerbit Andi.

(15). Whitman, M.E. and Mattord, H.J. (2010) *Management of Information Security*. Edk 3. Course Technology.

(16). Wijatmoko, T.E. 2020, 'EVALUASI KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA KANTOR WILAYAH KEMENTERIAN HUKUM DAN HAM DIY', *CyberSecurity dan Forensik Digital*, vol. 3, no. 1, hh. 1-6

(17). Yustanti, W. *et al.* (2018) *Keamanan Sistem Informasi*. Zifatama Jawara.