Journal of Information Systems and Informatics
Vol. 6, No. 4, December 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i4.949 Published By DRPM-UBD

Information Security Evaluation at Hospital Using Index KAMI 5.0 and Recommendations Based on ISO/IEC 27001:2022

I Nyoman Adi Artha Wibawa[1], Anak Agung Ngurah Hary Susila[2], Muhammad Alam Pasirulloh[3]

[1,2,3]Information Technology Department, Udayana University, Bali, Indonesia
Email: [1]adi.artha043@student.unud.ac.id, [2]harysusila@unud.ac.id, [3]muhammad.alam@unud.ac.id

Abstract

Bali Mandara Regional Hospital integrates information technology into its healthcare services, but ransomware attacks pose significant risks to data security. In accordance with the 2016 Indonesian Ministry of Communication and Informatics regulation, Electronic System Operators (PSE) are required to ensure information security, emphasizing confidentiality, integrity, and availability. To support this, the National Cyber and Crypto Agency introduced the Index KAMI, an evaluation tool aligned with ISO/IEC 27001 standards. This study evaluates the hospital's information security using Index KAMI 5.0, yielding a score of 177, which classifies its readiness as "Not Eligible" for ISO 27001 compliance. Recommendations for improvement include establishing clear governance policies, implementing systematic risk management, enhancing asset management with integrated inventories, and strengthening data protection through access control and encryption. Additional measures involve improving physical security with surveillance systems and fostering stronger vendor relationships through binding SLA agreements. By adopting these measures, Bali Mandara Regional Hospital can enhance its security system, protect patient data, and achieve compliance with international standards.

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

1. INTRODUCTION

The swift advancement of information and communication technology has significantly impacted various sectors. This advancement has influenced healthcare facilities and transformed many aspects of human life. Organizations and companies across different fields must continually adapt and implement technological advancements to remain relevant and efficient. In the healthcare sector, the use of IT has evolved over time, with healthcare facilities increasingly relying on IT to improve the quality of patient care. The integration of IT in healthcare services has been driven by the need to enhance efficiency. However,

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

this shift has also introduced new challenges, particularly related to information security. Ransomware has become a growing concern, specifically on healthcare and medical institutions [1].

The increasing trend of data breaches has made information security a critical concern. In Indonesia, healthcare data theft has been a recurring issue. For instance, in 2020, the personal data of 230,000 COVID-19 patients was reportedly stolen and sold, causing both material and psychological harm, including potential social discrimination. Similarly, in January 2022, allegations surfaced of a 720 GB breach of patient medical records from several hospitals, later sold on the Raid forums platform [2].

Bali Mandara Regional Hospital was established under Law No. 44 of 2009 on hospitals and Law No. 23 of 2014 on Regional Government, to provide services to the public based on Pancasila, emphasizing humanity, ethics, professionalism, justice, equality, non-discrimination, patient safety, and social responsibility. The hospital has leveraged IT in its healthcare services, employing various information systems such as the Hospital Information System (SIM-RS), Patient Registration System, and others. However, according to interviews, during the system development phase at Bali Mandara Regional Hospital, a ransomware attack threatened the information stored within its systems.

Based on the 2016 regulation from the Ministry of Communication and Informatics of the Republic of Indonesia regarding Information Security Management Systems, Electronic System Operators (PSE) must implement security measures to safeguard the confidentiality, integrity, and availability of information. To enhance the quality of information security, the National Cyber and Crypto Agency introduced the Information Security Index (Index KAMI), as a tool to evaluate the level of readiness in alignment with the requirements of the standard [3]. On the other hand, Bali Mandara Regional Hospital has never conducted an information security evaluation since it began utilizing information systems in healthcare services.

The latest version of the Index KAMI, 5.0, references the international standard ISO/IEC 27001:2022 in evaluating information security. The ISO/IEC 27001:2022 standard outlines specific controls designed for managing information security systems, addressing critical aspects such as equipment maintenance, data backup, malware prevention, and network protection. Adopting these standards enables healthcare institutions to implement comprehensive measures that protect patient data, maintain data accuracy, and ensure adherence to regulatory requirements [4].

Several studies have applied information security frameworks for governance improvement. Research by [5] used Index KAMI 4.2 and ISO/IEC 27001:2013 at Department of Communication and Informatics or Office of Communication and Informatics Gianyar, resulting in a Level I score with recommendations. Study by [6] assessed PUSDATIN, scoring electronic systems at 39 and security at 394 (Level I+), and recommended ISO 27001. Study by [7] evaluated a tech startup with Index KAMI 4.0, rating security as "Inadequate" (Levels I-I+), suggesting ISO 27001:2013 improvements. Work by [8] in Minahasa Regency found "High" electronic systems but insufficient security (score 264) for ISO 27001 compliance. The others one by [9] used Index KAMI 3.1 to assess PIP Semarang, scoring 238 and recommending early-stage security improvements.

Bali Mandara Regional Hospital holds a significant responsibility in managing patient data and health information, highlighting the importance of evaluating the maturity of their information security practices and ensuring compliance with applicable security standards. Bali Mandara Regional Hospital faces several deficiencies in information security infrastructure, including ransomware threats, lack of formal evaluation since the implementation of the information system. Therefore, this study aims to use the Index KAMI 5.0 as a tool to evaluate information security at Bali Mandara Regional Hospital and provide recommendations based on ISO/IEC 27001:2022. This study will offer a comprehensive perspective on information security at Bali Mandara Regional Hospital and serve as a foundation for developing effective improvement strategies.

2. METHODS

The stages of this research include a literature review, information gathering, data collection using the Index KAMI questionnaire, calculation of the questionnaire results, verification of the data, analysis of the results, and recommendations. This case study applies the Index KAMI as a qualitative descriptive method [10]. Created to support agency leaders in evaluating the comprehensiveness and maturity of their information security structures, rather than critiquing existing practices [11]. The process stages are illustrated in the flowchart in Figure 1.

The research stages include a literature review to deepen understanding of the Index KAMI and ISO/IEC 27001 identifying knowledge gaps from trusted sources. Information was gathered through interviews and observations. Interviews with the Head of SIMRS at Bali Mandara Regional Hospital provided insights into the current state of the hospital's information security, while observations assessed its actual conditions.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

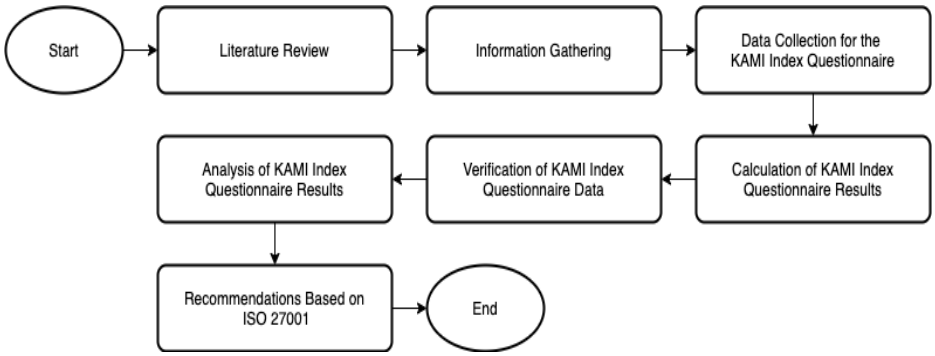

Figure 1. Research Stages

The information gathering stage involved interviews, observations, and the use of the Index KAMI questionnaire to assess the hospital's information security readiness. Interviews were conducted with the Head of the SIMRS Department at Bali Mandara Regional Hospital to obtain insights into the current information security conditions, while observations allowed for a direct assessment of the hospital's environment. To manage responsibilities and roles effectively during the data collection phase, the RACI model (Responsible, Accountable, Consulted, Informed) was employed. This management tool was used to map stakeholders for each process, enhancing the oversight and performance of the evaluation team [reference] [12]. Respondents for the Index KAMI questionnaire were selected based on the RACI Chart method, focusing on individuals with Responsible (R) and Accountable (A) roles, as they possessed the most comprehensive knowledge of the evaluated areas. Respondents were briefed on the questionnaire's purpose and content, focusing on eight key areas of the Index KAMI divided into two primary categories: Electronic Systems and Information Security, which encompass Governance, Risk Management, Information Security Framework, Asset Management, Technology, Personal Data Protection, and Supplementary Areas. The results of the questionnaire were processed using the predefined formula of the KAMI Index for Information Security. Each area was analyzed to calculate a final score, with the overall results summarized in Table 1, which displays the Electronic System Category Score.

Table 1. Electronic system category score

Category of Electronic System		Category of Information Security		Readiness Status
Low		Final Score		
10	15	0	247	Ineligible
		248	443	Compliance with the Basic Framework

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Category of Electronic System		Category of Information Security		Readiness Status
Low		**Final Score**		
		444	760	Fair
		761	916	Good
High		**Final Score**		**Readiness Status**
16	34	0	387	Ineligible
		388	646	Compliance with the Basic Framework
		647	828	Fair
		829	916	Good
Strategic		**Final Score**		**Readiness Status**
35	50	0	472	Ineligible
		473	760	Compliance with the Basic Framework
		761	864	Fair
		865	916	Good

The findings highlight four key assessment results, as illustrated in Figure 2. These results are visually represented in a six-axis radar diagram (Figure 3), providing an overview of the completeness level based on the evaluation. Readiness for ISO 27001 certification is achieved when the maturity level reaches at least level III+ with a "Fairly Good" readiness status, as depicted in Figure 4.

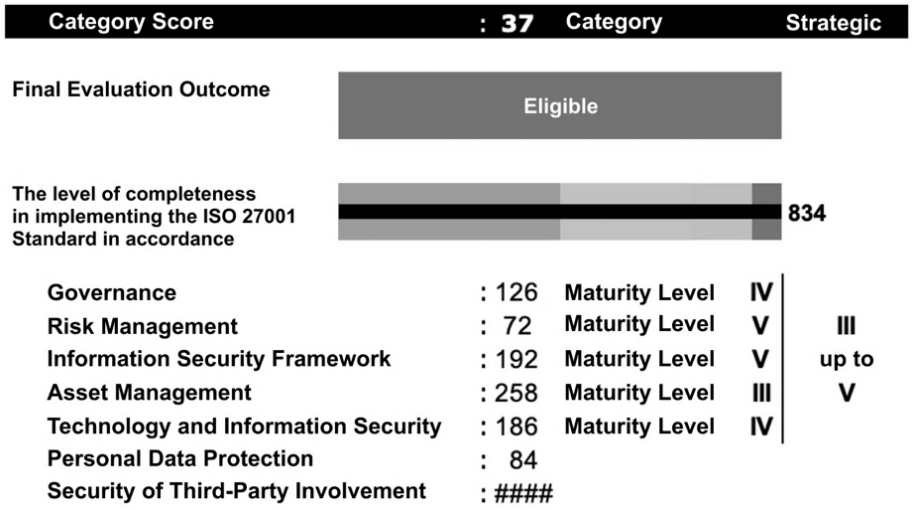

Figure 2. Table Display of Information Security Evaluation Results

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

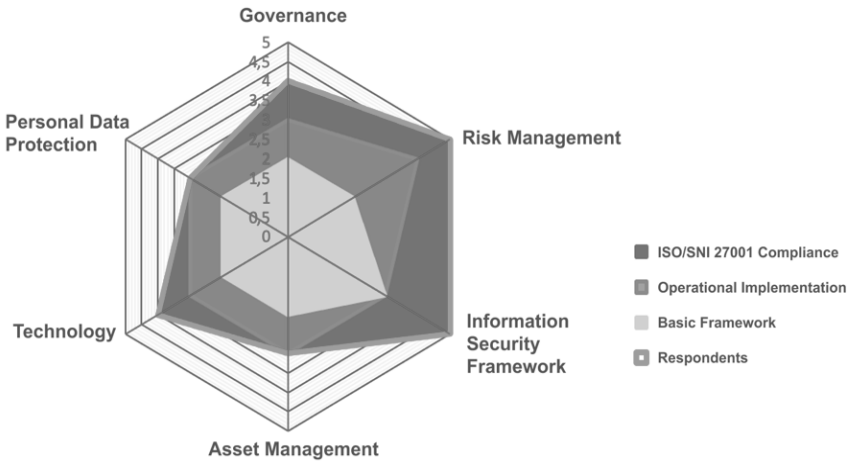

Figure 3. Radar chart display of information security evaluation results

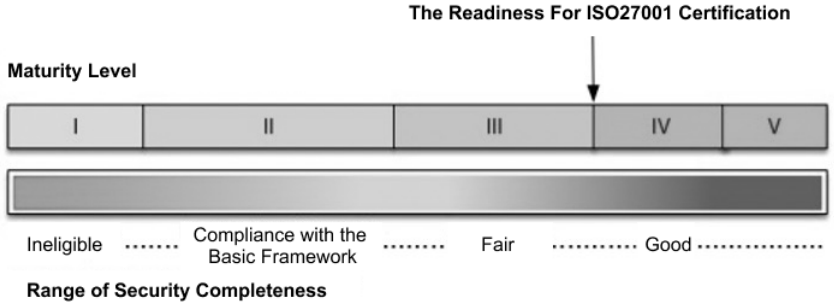

Figure 4. Level of readiness for ISO 27001 certification on the Index KAMI

The data verification stage aimed to ensure the accuracy of the questionnaire responses. Verification was conducted using a checklist to compare the respondents' answers with the actual conditions. The analysis phase involved providing questionnaire scores after verification and identifying issues in each area of the Index KAMI. These issues served as a reference for mapping with the controls of ISO/IEC 27001:2022. Recommendations were based on the information security evaluation, aligning each Index KAMI area with relevant controls from both frameworks. These recommendations were grouped according to the improvement of readiness status

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

3. RESULTS AND DISCUSSION

3.1 Index KAMI Assessment Result

The questionnaire results were calculated to determine maturity levels and final scores for each area in the Index KAMI. Final scores in each area are derived based on the Index KAMI guidelines, where each score level has different weightings. The calculation results for the Electronic System Category area are shown in Table 2.

Table 2. Calculation results for the electronic system category area

Category	Amount	Point	Total
Low	4	1	4
High	4	2	8
Strategis	2	5	10
		Total Score	22

From the total scores of implementation statuses, the Electronic System Category achieved a score of 22, placing "high" category. The Information Security Governance area was assessed by determining scores for each implementation status to analyze maturity levels. This area includes 22 questions, with response options ranging from 'Not Implemented' to 'Fully Implemented.' The area's total scores are presented in Table 3.

Table 3. Total score for the information security governance area

Execution Status	Category		
	1	**2**	**3**
Not Implemented	0	2	6
In Planning	7	5	0
In Progress/Partially Implemented	1	1	0
Fully Implemented	0	0	0
Not Applicable/Relevant	0	0	0
Total Score	**9**	**14**	**0**

The scores for Security Categories 1 and 2 totaled 23, which does not meet the criteria for Security Category 3 in the Information Security Governance area, rendering the evaluation for this category invalid according to the Index KAMI. An analysis of the maturity level will follow, with results presented in Table 4.

In Maturity Level II, the Information Security Governance area covers 8 questions in Security Category 1 and 5 in Category 2. A score of 21 was achieved, exceeding the minimum for this level but falling short of advancing to the next level, resulting in classification as Maturity Level I+.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 4. Maturity level in the information security governance area

Execution Status	Category	
	1	**2**
Not Implemented	0	0
In Planning	7	4
In Progress/Partially Implemented	1	1
Fully Implemented	0	0
Not Applicable/Relevant	0	0
Total Score	**9**	**12**

The evaluation of the Information Security Risk Management area involved calculating the scores for each implementation status to determine the final score, which aids in analyzing maturity levels. This area comprises 16 questions with response options including 'Not Implemented', 'In Planning', 'Partially Implemented', 'Fully Implemented', and 'Not Applicable'. The total scores for the Risk Management area can be seen in Table 5.

Table 5. Total scores for the risk management area

Execution Status	Category		
	1	**2**	**3**
Not Implemented	0	0	2
In Planning	10	4	0
In Progress/Partially Implemented	0	0	0
Fully Implemented	0	0	0
Not Applicable/Relevant	0	0	0
Total Score	**10**	**8**	**0**

The scores for Security Categories 1 and 2 did not meet the criteria to qualify for Security Category 3 in the Risk Management area, rendering the evaluation for this category invalid according to the Index KAMI. Consequently, the total evaluation score for the Risk Management area is 18. An analysis of the maturity level will follow, with results available in Table 6.

Table 6. Maturity level in the risk management area

Execution Status	Category
	1
Not Implemented	0
In Planning	10
In Progress/Partially Implemented	0
Fully Implemented	0
Not Applicable/Relevant	0
Total Score	**10**

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Maturity Level II in the Risk Management area includes 10 questions under Security Category 1. With a total score of 10, the results fall short of the minimum required for Maturity Level II, placing it in Maturity Level I.

The evaluation of the Information Security Governance Framework area involves calculating individual implementation status scores to derive a final score and facilitate maturity level analysis. This framework area consists of 32 questions, with response options indicating implementation status: 'Not Implemented,' 'In Planning,' 'Partially Implemented,' 'Fully Implemented,' or 'Not Applicable.' The total score results for the Information Security Governance Framework area are displayed in Table 7.

Table 7. Total score for the information security governance framework area

Execution Status	Category		
	1	**2**	**3**
Not Implemented	0	1	9
In Planning	11	7	0
In Progress/Partially Implemented	0	3	0
Fully Implemented	1	0	0
Not Applicable/Relevant	0	0	0
Total Score	**14**	**26**	**0**

Scores for categories 1 and 2 do not qualify for inclusion in category 3 of the Information Security Governance Framework area, rendering category 3 evaluation invalid in the Index KAMI. Consequently, the total evaluation score obtained in this area is 40, with the maturity level analysis shown in Table 8.

Table 8. Maturity level in the information security governance framework area

Execution Status	Category	
	1	**2**
Not Implemented	0	0
In Planning	8	2
In Progress/Partially Implemented	0	0
Fully Implemented	1	0
Not Applicable/Relevant	0	0
Total Score	**11**	**4**

For maturity level II in the Information Security Governance Framework area, there are 9 questions under category 1 safeguards and 2 questions under category 2. The total score of 15 surpasses the minimum for level II but falls short of the level II benchmark, thereby meeting the requirements only for maturity level I+.

The evaluation of the Information Asset Management area is performed by calculating individual implementation status scores to obtain a final score, which

aids in analyzing maturity levels. This area comprises 53 questions, with response options ranging from 'Not Implemented,' 'In Planning,' 'Partially Implemented,' 'Fully Implemented,' to 'Not Applicable.' The total score for the Information Asset Management area is shown in Table 9.

Table 9. Total score for the information asset management area

Execution Status	Category		
	1	**2**	**3**
Not Implemented	6	17	7
In Planning	14	1	0
In Progress/Partially Implemented	7	1	0
Fully Implemented	0	0	0
Not Applicable/Relevant	0	0	0
Total Score	**28**	**6**	**0**

The scores for safeguard categories 1 and 2 do not qualify for category 3 in the Information Asset Management area within the Index KAMI, making category 3 evaluation invalid. Consequently, the total evaluation score for this area is 34, with the maturity analysis presented in Table 10.

Table 10. Maturity level in the information asset management area

Execution Status	Category	
	1	**2**
Not Implemented	6	3
In Planning	14	1
In Progress/Partially Implemented	7	1
Fully Implemented	0	0
Not Applicable/Relevant	0	0
Total Score	**28**	**6**

In Maturity Level II, the Information Asset Management area includes 30 questions under category 1 and 5 under category 2. The total score achieved is 34, which does not meet the required minimum for Maturity Level II, thus it is classified at Maturity Level I.

The Technology and Information Security area is evaluated by calculating scores based on each implementation status, leading to a final score that helps assess the maturity level. This area comprises 35 questions with response options: 'Not Implemented,' 'In Planning,' 'Partially Implemented,' 'Fully Implemented,' and 'Not Applicable.' The final score for this area is presented in Table 11.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 11. Total score for the technology and information security area

Execution Status	Category		
	1	**2**	**3**
Not Implemented	7	8	7
In Planning	2	5	0
In Progress/Partially Implemented	5	1	0
Fully Implemented	0	0	0
Not Applicable/Relevant	0	1	0
Total Score	**12**	**20**	**0**

Scores from safeguard categories 1 and 2 did not meet the criteria needed for category 3, rendering category 3 ineligible for evaluation within the Index KAMI in the Technology and Information Security area. Consequently, the total evaluation score achieved for this area is 32, with the maturity analysis presented in Table 12.

Table 12. Maturity level in the technology and information security area

Execution Status	Category
	1
Not Implemented	7
In Planning	2
In Progress/Partially Implemented	5
Fully Implemented	0
Not Applicable/Relevant	0
Total Score	**12**

Maturity level II for the Technology and Information Security area comprises 14 questions in category 1. The resulting score of 12 is below the minimum threshold required for advancing to the next maturity level, placing the area in maturity level I. The evaluation of the Personal Data Protection area involves calculating scores for each implementation status to obtain a final score, which supports maturity level analysis. This area includes 35 questions with options: 'Not Implemented,' 'In Planning,' 'Partially Implemented,' 'Fully Implemented,' and 'Not Applicable.' The total score for this area is shown in Table 13.

Table 13. Total score for the personal data protection area

Execution Status	Category	
	1	**2**
Not Implemented	0	1
In Planning	1	11
In Progress/Partially Implemented	2	0
Fully Implemented	1	0
Not Applicable/Relevant	0	0
Total Score	**8**	**22**

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

The Personal Data Protection area comprises questions only within safeguard categories 1 and 2, resulting in an evaluation score of 30. Further maturity analysis can be found in Table 14.

Table 14. Maturity level in the personal data protection area

Execution Status	Category	
	1	**2**
Not Implemented	0	0
In Planning	1	2
In Progress/Partially Implemented	2	0
Fully Implemented	1	0
Not Applicable/Relevant	0	0
Total Score	**8**	**4**

Maturity level II in Personal Data Protection includes 4 questions in category 1 and 2 questions in category 2, yielding a score of 12. While this exceeds the minimum requirement for level II, it does not meet the score for advancing, placing it in maturity level I+. The evaluation of the Supplementary area is conducted by calculating the score for each implementation status, with the final result displayed as a percentage. This area includes 27 questions with options: 'Not Implemented,' 'In Planning,' 'Partially Implemented,' 'Fully Implemented,' and 'Not Applicable.' The total score calculation for this area is shown in Table 15.

Table 15. Total score for the evaluation of the supplementary area

Execution Status	Category
	1
Not Implemented	4
In Planning	23
In Progress/Partially Implemented	0
Fully Implemented	0
Not Applicable/Relevant	0
Total Score	**23**

The Supplementary area includes only questions within safeguard category 1. The score obtained in this area is 23, out of a maximum possible score of 81, resulting in an evaluation score of 28%.

3.2 Assessment Results

The overall evaluation scores are presented in two sections. The first section shows four key assessment results: the Electronic System Category Score, Final Evaluation Outcome, Level of ISO 27001 Standard Implementation per Category, and final scores with maturity levels for each area. The second section displays a six-axis radar diagram to illustrate information security readiness and completeness based on the achieved maturity levels.

Journal of Information Systems and Informatics
Vol. 6, No. 4, December 2024
p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

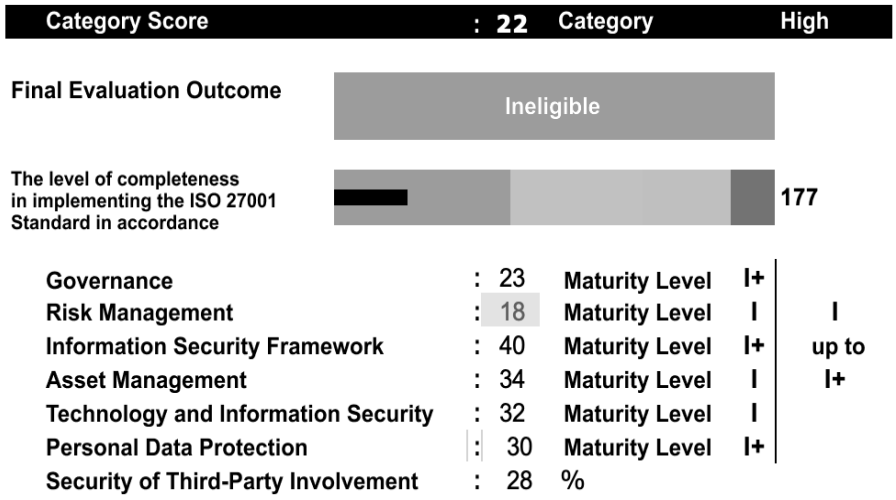

Figure 5. Table Display of Information Security Evaluation Results for RSUD Bali Mandara

Figure 5 shows the first evaluation section with four assessments. The Electronic System Category Score reached 22, classifying it as "high." The Final Evaluation Outcome, derived from the correlation of Electronic System and Information Security scores, indicates Bali Mandara General Hospital's status as "Ineligible" The third assessment reflects the ISO 27001 Standard Implementation Level at 177 (red zone). The fourth displays final scores and maturity levels across areas, placing Bali Mandara Hospital's information security maturity at Level I to I+.

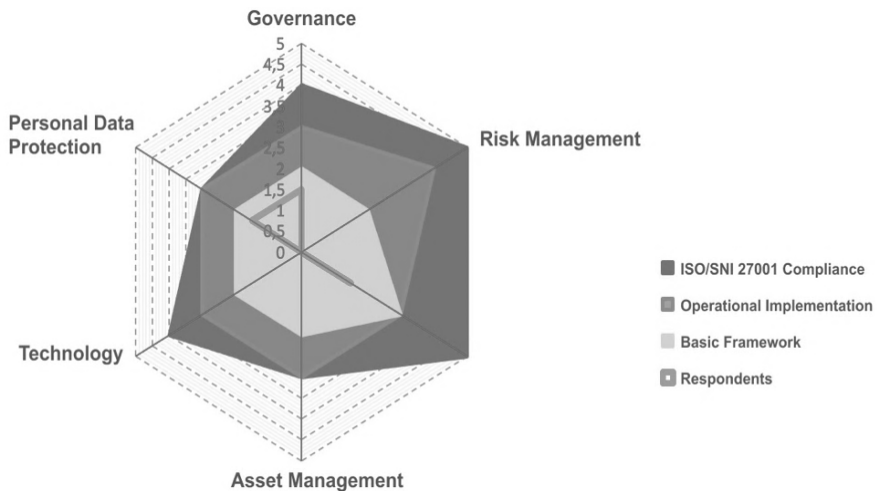

Figure 6. Radar Chart Display of Information Security Evaluation Results for RSUD Bali Mandara

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Figure 6 presents the second evaluation section as a six-axis radar diagram. The evaluation is shown as a bold red line ranging from 0 to 1.5, with three thresholds representing completeness levels (light to dark green for Levels 1 to 3). The result does not meet the light green threshold, indicating a foundational framework level.

3.3 Discussion

Based on the data collection and analysis of each evaluation area, it is evident that Bali Mandara Hospital does not yet meet the standards set by ISO/IEC 27001. Therefore, recommendations for improvement are necessary in the Information Security category, particularly concerning requirements marked as "In Planning" or "Not Implemented," aimed at enhancing information security effectiveness. These recommendations are based on a comparison with the controls outlined in ISO/IEC 27001:2022.

Information Security Governance area requires the implementation of controls focused on the development of security policies, the assignment of responsibilities, incident management, and risk assessments. Weak information security governance can lead to ambiguity in information security responsibilities, potentially resulting in slow or inappropriate decision-making. Recommendations include controls that serve as guidelines for improvement, specifically focusing on security policies, the assignment of responsibilities, incident management, and risk assessments, while also providing additional references for enhancements in this area, with an emphasis on governance policies and risk management strategies.

Information Security Risk Management area necessitates the implementation of controls aimed at improving risk assessment and mitigation strategies. Recommendations include guidelines that focus on risk management, assessment, and incident response. Without proper information security risk management, hospitals are vulnerable to threats such as ransomware, which can cripple a hospital's information systems. These controls emphasize establishing robust frameworks for identifying and evaluating risks while implementing effective incident management procedures, thereby underscoring the need for comprehensive governance policies to enhance organizational resilience against security threats.

Information Security Framework area requires the implementation of controls focused on establishing a robust governance structure for information security. The lack of a well-defined information security framework can hamper coordination between technical and management teams, which is essential for incident handling. Recommendations include controls that guide improvements in security policies, roles and responsibilities, risk management practices, and incident response protocols. These controls emphasize developing a solid framework for

managing information security risks, ensuring clear assignments of responsibilities, and fostering continuous improvement, ultimately enhancing the organization's resilience against security threats.

Information Asset Management area necessitates the implementation of controls aimed at effectively managing and safeguarding information assets. Without proper information asset management, hospitals cannot ensure the sustainability or security of patient data. Recommendations focus on establishing clear guidelines for asset classification and handling, ensuring appropriate access controls, and maintaining robust data protection measures. These controls emphasize the importance of assigning responsibilities for asset management, conducting regular audits, and implementing procedures for the secure disposal of assets.

Technology and Information Security area requires the implementation of controls focused on establishing effective governance frameworks for information security. Recommendations highlight the necessity of developing comprehensive security policies, defining roles and responsibilities, and ensuring regular communication regarding security practices within the organization. These controls emphasize the importance of risk assessment and management processes, along with continuous monitoring and evaluation of security measures.

The area of Personal Data Protection necessitates the implementation of controls that focus on safeguarding sensitive information and ensuring compliance with data protection regulations. Weak protection of personal data can lead to loss of patient trust and lawsuits. Recommendations emphasize the importance of developing clear policies for data handling, establishing protocols for data access and sharing, and implementing robust security measures to protect personal data from unauthorized access and breaches. Additionally, it is crucial to conduct regular assessments to identify and mitigate risks associated with data management.

Supplement area requires the establishment of comprehensive controls aimed at enhancing the overall security posture and ensuring the effective management of information security risks. Weaknesses in this area can result in undetected risks, particularly from third-party partners or physical security breaches that could impact the integrity of the hospital information system. Recommendations focus on developing policies that clarify governance structures, roles, and responsibilities, while also emphasizing the importance of incident response plans and the management of security-related activities. Moreover, it is essential to implement strategies for continuous monitoring and improvement of security measures, as well as to conduct regular assessments to identify and address vulnerabilities.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

4. CONCLUSION

The evaluation of information security readiness at Bali Mandara Regional General Hospital using the Index KAMI version 5.0 revealed a readiness status of "Ineligible" for ISO/IEC 27001:2022 compliance, with a total score of 197. While the Electronic System Category demonstrated a "high" score of 24 and the Technology and Information Security area showed progress in maintaining confidentiality, integrity, and availability, other areas such as Information Security Governance, Risk Management, the Security Framework, and Asset Management remain at basic maturity levels (I to I+). These findings highlight the need for substantial improvements, including the establishment of a dedicated security team, structured risk management programs, and comprehensive security policies. Furthermore, prioritizing network segmentation, enhancing personal data protection, and maintaining an updated asset inventory are critical steps. By implementing these recommendations, conducting regular audits, and increasing staff awareness, the hospital can strengthen its information security measures and align with ISO/IEC 27001:2022 standards, ensuring better protection of patient data and compliance with regulatory requirements.

REFERENCES

[1] A. Minnaar, "Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic," *Acta Criminologica: African Journal of Criminology & Victimology*, vol. 34, no. 3, Dec. 2021, doi: 10.10520/ejc-crim_v34_n3_a10.

[2] S. Sofia, E. T. Ardianto, N. Muna, and Sabran, "Analisis Aspek Keamanan Informasi Pasien Pada Penerapan RME di Fasilitas Kesehatan," *RAMMIK : Jurnal Rekam Medik dan Manajemen Informasi Kesehatan*, vol. 1, no. 2, pp. 94–103, Oct. 2022, doi: 10.47134/rammik.v1i1.29.

[3] R. Savitri, Firmansyah, Dworo, and M. S. Hasibuan, "Information Security Measurement using INDEX KAMI at Metro City," *Journal of Applied Data Sciences*, vol. 5, no. 1, pp. 33–45, Jan. 2024, doi: 10.47738/jads.v5i1.152.

[4] W. S. Basri and A. L. Ayu, "Risk Management in Information Systems: Applying ISO 31000:2018 and ISO/IEC 27001:2022 Controls at PMI's Central Clinic," *International Journal for Applied Information Management*, vol. 4, no. 1, pp. 1–13, Apr. 2024, doi: 10.47738/ijaim.v4i1.70.

[5] D. I. Khamil, G. M. A. Sasmita, and A. A. N. H. Susila, "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, pp. 1948–1960, 2022, doi: 10.35957/jatisi.v9i3.2310.

[6] P. Sundari and Wella, "SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)," *Ultima InfoSys : Jurnal Ilmu Sistem Informasi*, vol. 12, no. 1, pp. 35–442, 2021, doi: 10.31937/si.v12i1.1701.

[7] A. L. Maryanto, M. N. Al Azam, and A. Nugroho, "Evaluasi Manajemen Keamanan Informasi Pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks KAMI," *Jurnal SimanteC*, vol. 11, no. 1, pp. 1–12, 2022, doi: 10.21107/simantec.v11i1.14099.

[8] R. A. P. P. Gala, R. Sengkey, and C. Punusingon, "Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI," *Jurnal Teknik Informatika*, vol. 15, no. 3, pp. 189–198, 2020, doi: 10.35793/jti.v15i3.31597.

[9] D. D. Prasetyowati, I. Gamayanto, S. wibowo, and Suharnawi, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang," *Journal of Information System*, vol. 4, no. 1, pp. 65–75, 2019, doi: 10.33633/joins.v4i1.2429.

[10] V. I. Sugara, H. Syahrial, and M. Syafrullah, "Sistem Pemeriksa Keamanan Informasi Menggunakan National Institute Of Standards And Technology (Nist) Cybersecurity Framework," *Jurnal Ilmiah Ilmu Komputer dan Matematika*, vol. 16, no. 1, pp. 203–212, Jan. 2019, doi: 10.33751/komputasi.v16i1.1591.

[11] T. E. Wijatmoko, "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy," *Jurnal CyberSecurity dan Forensik Digital*, vol. 3, no. 1, pp. 1–6, May 2020, doi: 10.14421/csecurity.2020.3.1.1951.

[12] M. Zulvikri and M. Mukaram, "Optimalisasi Pengawasan Kinerja Karyawan Business Consultant PT XYZ : Implementasi Sistem RACI Melalui Project Google Spreadsheet," *Jurnal Riset Manajemen*, vol. 2, no. 4, pp. 197–207, Nov. 2024, doi: 10.54066/jurma.v2i4.2683.