Online ISSN: 2622-4666 Print ISSN: 2356-3281
Jurnal Persada Husada Indonesia Vol. 13 No. 2 (Mei 2026) : 36-50

Analysis of the Readiness Level of Hospital Management Information System (HMIS) Security Based on the Kami Index 5.0 at RS X 2026

Agni Dika Seutiani[1], Fery Fadly[2]*

[1]Department of Medical Records and Health Information, Poltekkes Tasikmalaya, Indonesia
fery.fadly@dosen.poltekkestasikmalaya.ac.id
[2]Department of Medical Records and Health Information, Poltekkes Tasikmalaya, Indonesia,
agnidikass@gmail.com

*Corresponding Author: fery.fadly@dosen.poltekkestasikmalaya.ac.id

Abstract

Research Objective: The Hospital Management Information System (SIMRS) improves the quality and efficiency of hospital services. However, incidents of health data leakage still pose risks to the security of patient information. A preliminary study at X General Hospital showed that SIMRS has been implemented in all service units. Nevertheless, an assessment of information security readiness has never been conducted, so potential risks to patient data have not been clearly measured. This study aims to determine the level of information security readiness of the Hospital Management Information System (SIMRS) using the KAMI Index 5.0. **Methodology:** This study used a quantitative descriptive design. Respondents were selected using purposive sampling. Data were collected through observation of security procedures, the KAMI Index 5.0 questionnaire, and supporting interviews. Data analysis was conducted by calculating scores for each assessment area and determining the readiness level using the readiness matrix of the KAMI Index 5.0. **Results:** The electronic system category obtained a score of 21, which falls within the range of 16–34, indicating a high level of dependence on electronic systems. The overall readiness score was 554, categorized as "Basic Framework Fulfillment," indicating that security controls exist but are not consistently implemented. **Conclusion:** The hospital is still considered not ready because it has not reached the minimum score of 647 based on the KAMI Index 5.0. Therefore, improvements are needed, particularly in risk management, governance framework, and asset management to improve information security readiness.

Keywords: *Data Security, Hospital Management Information System (HMIS), Indeks KAMI 5.0.*

INTRODUCTION

The rapid development of information technology has created significant changes in healthcare services, requiring services to be able to adapt to these changes. Minister of Health Regulation No. 82 of 2013 requires every hospital to implement a Hospital Management Information System (SIMRS) as a system that integrates healthcare service processes and information management. The implementation of SIMRS must be supported by information security in its management to protect patients' personal and confidential data from loss or leakage (Christin et al., 2025). Ministry of Health Regulation No. 24 of 2022 stipulates that electronic medical records must comply with the principles of patient data and information security, namely Confidentiality, Integrity, and Availability. Information security in electronic systems can be managed by referring to the international standard ISO/IEC 27001:2022, which provides guidance for organizations to establish, implement, maintain, and improve information security management systems (Aristianto et al., 2025). Although standard ownership has been established, there have been many cases of data leaks both internationally and nationally, such as data leaks, data theft, and system lockouts demanding ransom. The large number of such cases shows the importance of knowing the readiness of information systems in facing cyber attacks and improving health data security.

International studies have demonstrated that healthcare organizations remain among the most

frequently targeted sectors for cyberattacks due to the high value of personal health information. Cybersecurity maturity assessments are increasingly used to evaluate organizational preparedness and identify security gaps before incidents occur.

National adaptation to international guidelines is carried out by the National Cyber and Crypto Agency (BSSN), which developed the KAMI 5.0 Index to determine the completeness of controls and maturity of information security based on the ISO/IEC 27001:2022 standard. The assessment results can be used as a basis for formulating improvement measures and setting priorities for enhancing information security. A number of previous studies have used the KAMI Index as an instrument to assess the level of information maturity, with the results showing that there is still a need for improvement in the area of security. The lack of readiness can pose a threat to health information security, which has the potential for leakage or misuse that can have a negative impact on both individuals and health facilities. Failure to meet data security readiness standards can pose a threat to the security of health information. Confidential and highly sensitive health data is at risk of being leaked or misused, which can have negative consequences for both individuals and healthcare facilities (Ahmad et al., 2025).

Preliminary study results show that X General Hospital has implemented SIMRS in all service units, so that patient data processing depends on the reliability of the information system. The hospital has implemented basic policies and procedures for patient data confidentiality, but has never conducted a comprehensive assessment of the level of electronic system security readiness. This situation indicates a non-compliance with regulatory requirements, as Government Regulation No. 71 of 2019 requires every Electronic System Operator to assess, control, and prove the security readiness of the electronic systems used to ensure they are reliable, secure, and accountable. Without measurable assessments, hospitals cannot ensure that their information security practices meet standards and are capable of protecting sensitive and private patient data. Research by Daniswara et al., (2023) confirms that periodic evaluation of security procedures is an important step in improving system resilience against data breaches.

These provisions require standardized and measurable assessment instruments, so that data security readiness is assessed using the KAMI Index, which is an official government instrument from BSSN designed to assess the completeness and maturity of information security implementation in electronic system operators, including hospitals. Therefore, this study aims to determine the level of information security readiness at X General Hospital using the KAMI Index version 5.0.

Although several studies have evaluated information security readiness using the KAMI Index in educational institutions, government agencies, and financial sectors, evidence regarding the implementation of KAMI Index 5.0 in hospital settings remains limited. Hospitals manage highly sensitive personal health information and are increasingly exposed to cybersecurity threats. Therefore, assessment of information security readiness in healthcare organizations remains an important research priority.

METHODS

This study uses a descriptive quantitative research design to assess the level of security readiness in the Hospital Management Information System through the KAMI 5.0 Index assessment score developed by BSSN. The study was conducted at X Hospital in Tasikmalaya City from December to February 2026. The Chief Information Officer (CIO) was selected as the sole respondent because this position is responsible for information technology governance, information security implementation, policy development, risk management, and strategic decision-making related to HMIS operations. Furthermore, the KAMI Index assessment requires respondents who possess comprehensive knowledge of organizational information security practices. To minimize subjectivity, questionnaire responses

were verified through document review, direct observation of information security practices, and supporting interviews with relevant personnel.

Data collection was conducted through questionnaires, supporting data observation, and supporting interviews. The study involved eight variables adjusted to the KAMI 5.0 assessment areas, namely Electronic Systems Category, Information Security Governance, Information Security Risk Management, Information Security Framework, Information Asset Management, Information Technology and Security, Personal Data Protection, and a supplement on third-party involvement risk. Data analysis was conducted by calculating the scores of the electronic systems to be categorized according to the KAMI 5.0 Index matrix, calculating the control completeness area scores, calculating the information security maturity status, and presenting the information security readiness level calculated from all areas to obtain a final score to be entered into the readiness level matrix and presented in a spider chart and horizontal bar chart.

RESULT

The research results obtained scores in each assessment area of the KAMI 5.0 Index. The collected data was automatically calculated in the KAMI 5.0 Index Excel spreadsheet using the answers specified in the guidelines.

Electronic Systems Category

The coverage area of the electronic system category is calculated based on the scores obtained in the questionnaire. The scores show the category of dependence on electronic systems obtained.

Table 1. Score Elektronic System Category

Category	Amout	Point	Total
Low	5	1	5
High	3	2	6
Strategic	2	5	10
Total Score			**21**

Based on Table 1, the assessment results for the electronic system category show a score of 21. This score falls within the range of 16-34, which is classified as a High level of dependency. The high level of dependency on the system indicates that hospital operations are highly dependent on the availability, reliability, and security of the electronic system. Based on the KAMI Index guidelines, electronic system operators with a high level of dependency are required to implement information security standards, including SNI ISO/IEC 27001 and other cybersecurity standards established by BSSN and relevant ministries.

Control Completion and Maturity Level
Information Security Government

Table 2. Information Security Governance Maturity Score Implementation Status

Variable	Frequency		
	I	**II**	**III**
Not Done	0	0	4
In Planning	0	1	0
In Implementation or Partially Implemented	0	1	0

Fully Implemented	8	6	2	
Not Applicable/Relevant	0	0	0	
Total Score	**24**	**42**	**18**	**=84**

The results of the completion of the Information Security Governance area yielded a score of 84, which meets the requirement that the implementation scores for categories 1 and 2 exceed the minimum score for category 3, which is 48, and the fulfillment status for stage 1 is "OK." Therefore, the assessment status for category 3 of the Information Security Governance area is declared valid in the KAMI index calculation.

Table 3. Information Security Governance Maturity Score Implementation Status

Variable	Frequency			
	I	**II**	**III**	
Not Done	0	0	4	
In Planning	0	1	0	
In Implementation or Partially Implemented	1	0	0	
Fully Implemented	12	2	2	
Not Applicable/Relevant	0	0	0	
Total Score	**52**	**14**	**18**	**=84**

Maturity status III is determined based on a score of 14, which meets the requirement that it exceeds the maturity level III achievement score and the validity of maturity level III is "Yes". The validity status of Yes is obtained because it meets the requirements, namely a maturity level score of II with a total of 52 exceeding the maturity threshold of 43.2, as well as a category 3 assessment that is declared valid because it meets the requirements at the control completeness stage. Thus, the maturity level calculation can be raised to maturity level III, which means it is defined and consistent.

Risk Management Area

Table 4. Risk Management Control Area Completeness Score Implementation Status

Variable	Frequency			
	I	**II**	**III**	
Not Done	3	0	0	
In Planning	1	1	2	
In Implementation or Partially Implemented	3	0	0	
Fully Implemented	3	3	0	
Not Applicable/Relevant	0	0	0	
Total Score	**16**	**20**	**2**	**=36**

The results of the Information Security Risk Management assessment for Categories 1 and 2 yielded a score of 36. The score for Category 3 cannot be added because it does not meet the minimum score requirement for Category 3 implementation, which is 40. Therefore, this area is declared invalid.

Table 5. Risk Management Area Maturity Score Implementation Status

Variable	Frequency			
	I	**II**	**III**	**IV**

Not Done	3	0	0	0	
In Planning	1	0	0	2	
In Implementation or Partially Implemented	3	0	0	0	
Fully Implemented	3	1	2	0	
Not Applicable/Relevant	0	0	0	0	
Total Score	**12**	**8**	**12**	**0**	**=32**

Maturity status I+ was obtained because the score at maturity level II was 16, which was only slightly above the minimum score for maturity level II. In addition, the validity of maturity level III was "No," which prevented the maturity level from increasing. These two factors cause the maturity level to drop and be set at maturity level I+, which defines that it is still in its initial stage.

Information Security framework Area

Table 6. Security Framework Control Area Completeness Implementation Status

Variable	Frequency			
	I	**II**	**III**	
Not Done	0	0	1	
In Planning	1	3	2	
In Implementation or Partially Implemented	1	5	2	
Fully Implemented	10	3	5	
Not Applicable/Relevant	0	0	0	
Total Score	**33**	**44**	**0**	**=77**

The results of the completion of the Information Security Framework area produced a score of 77 in categories 1 and 2. This score meets the minimum score of 68 in category 3 but does not meet the requirements for stage 1 compliance, so the information security framework area is declared invalid in the KAMI index calculation.

Table 7. Information Security Framework Maturity Level Score Implementation Status

Variable	Frequency				
	II	**III**	**IV**	**V**	
Not Done	0	1	0	0	
In Planning	0	5	1	0	
In Implementation or Partially Implemented	3	4	0	1	
Fully Implemented	8	7	2	1	
Not Applicable/Relevant	0	0	0	0	
Total Score	**34**	**43**	**0**	**0**	**=32**

Maturity level II status was obtained because it met one of the requirements, namely that the maturity level II score of 34 was higher than the maturity level II achievement score, but it could not be upgraded to a higher maturity level because another requirement was not met, namely the validity of maturity level III, which had a status of "No." Therefore, only one requirement was met, and it was assigned a maturity level II status, namely the implementation of a basic framework.

Information Security Asset Management Area

Table 8. Information Security Asset Management Area Control Completeness Score Implementation Status

Variable	Frequency			
	I	II	III	
Not Done	0	2	3	
In Planning	0	4	0	
In Implementation or Partially Implemented	9	4	3	
Fully Implemented	22	9	1	
Not Applicable/Relevant	0	0	0	
Total Score	**76**	**78**	**0**	**=154**

The results of the assessment in the Information Asset Management area produced a score of 154 in categories 1 and 2. This score meets the minimum score of 130 in category 3 but does not meet the requirements for stage 1 compliance, so the information asset management area is declared invalid in the KAMI index calculation.

Variable	Frequency	
	II	III
Not Done	0	5
In Planning	1	3
In Implementation or Partially Implemented	5	7
Fully Implemented	26	6
Not Applicable/Relevant	0	0
Total Score	**102**	**52**

Maturity level II status was obtained because it met one requirement, namely that maturity level II with a score of 102 exceeded the maturity level II achievement score, but it could not be upgraded to a higher maturity level because another requirement had not been met, namely the validity of maturity level III, which had a status of "No." Therefore, it was assigned a maturity level II status, namely the implementation of a basic framework.

Information Technology and Security Area

Table 10. Information Technology and Security Control Completeness Score Implementation Status

Variable	Frequency			
	I	II	III	
Not Done	0	2	2	
In Planning	0	2	2	
In Implementation or Partially Implemented	0	4	1	
Fully Implemented	14	7	1	
Not Applicable/Relevant	0	0	0	
Total Score	**42**	**68**	**15**	**=125**

The results of the assessment in the Information Technology and Security area yielded a score of 125, meeting the requirement that the implementation scores for categories 1 and 2 must exceed the minimum score of 88 and that the fulfillment status for stage 1 is "OK." Therefore, the assessment status for category 3 in the Information Technology area is declared valid in the KAMI index calculation.

Variable	Frequency		
	II	III	IV
Not Done	0	2	2
In Planning	0	2	2
In Implementation or Partially Implemented	0	4	1
Fully Implemented	14	7	1
Not Applicable/Relevant	0	0	0
Total Score	**42**	**68**	**15**

Table 11 Technology and Security Maturity Score Implementation Status Category maturity level III+ is obtained from a maturity score of IV with a total score of 15, which is the same as the minimum score for maturity level IV. In addition, the validity of maturity level IV is "Yes," but it cannot be upgraded to maturity level IV because the score is not higher than the achievement score for maturity level IV. Therefore, the maturity level calculation can be upgraded to maturity level III+, which is defined and consistent.

Personal Data Protection Area

Table 12. Personal Data Protection Control Completeness

Variable	Frequency		
	II	III	
Not Done	**0**	**0**	
In Planning	**0**	**1**	
In Implementation or Partially Implemented	**0**	**1**	
Fully Implemented	**4**	**10**	
Not Applicable/Relevant	**0**	**0**	
Total Score	**12**	**66**	**=78**

The results from the Personal Data Protection area consist only of categories 1 and 2, resulting in a score of 78 and declared valid in this area.

Table 13. Personal Data Protection Maturity Score

Variable	Frequency	
	II	III
Not Done	0	0
In Planning	0	0
In Implementation or Partially Implemented	0	1
Fully Implemented	6	9
Not Applicable/Relevant	0	0
Total Score	**24**	**54**

Maturity status III was obtained from a maturity score of 54, which is higher than the score required to achieve maturity level III, and the validity of maturity level III was rated "Yes." The validity status of "Yes" is obtained because the maturity level II score of 24 is higher than the maturity threshold of 19.2, and other requirements are met in the assessment of category 3 completeness of control is declared valid, so that the maturity level calculation can be raised to maturity level III, which means it is defined and consistent.

Overview of Information Security Readiness Level

The level of information security readiness on the KAMI Index 5.0 is determined from the total score of the areas that are summed up and categorized in a predetermined matrix. The overview of information system security readiness is presented in two parts. The first part shows the main assessment results, namely the electronic system category score, the final evaluation results, the level of ISO 27001 standard implementation per category, and the final score with the maturity level in each area. The first part is presented in a horizontal bar chart and spider chart.

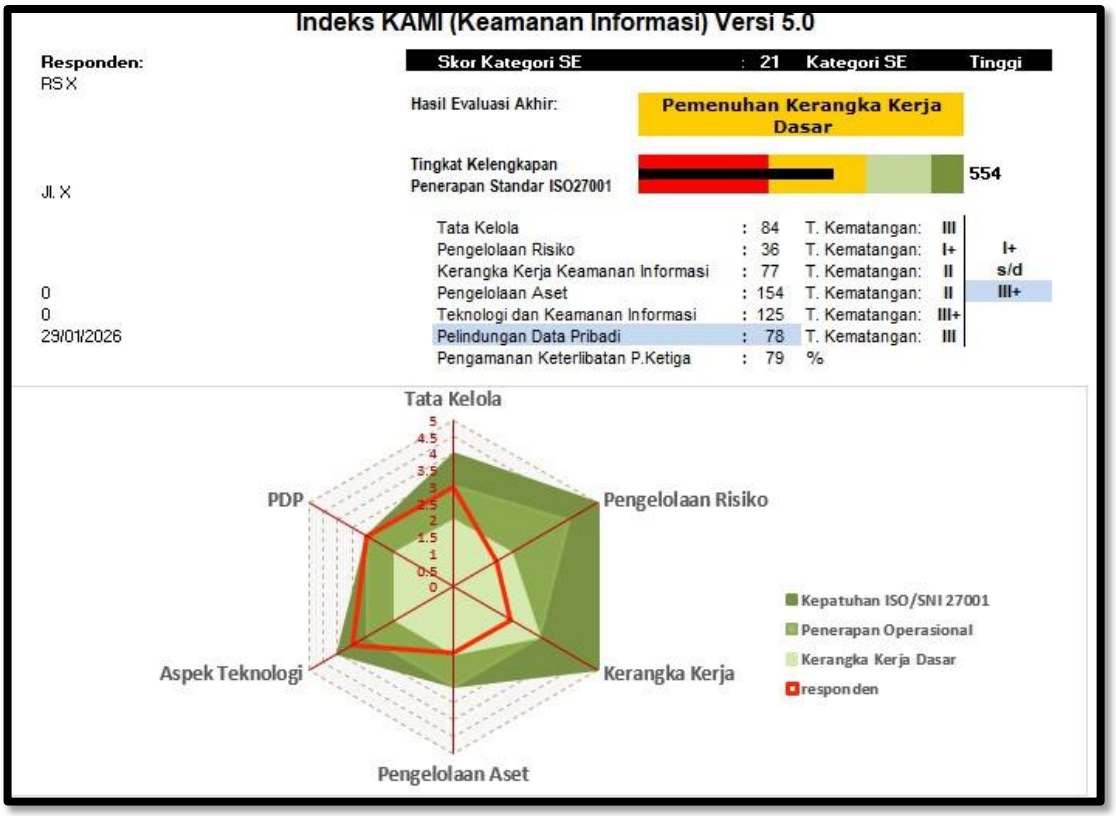

Figure 1. Overall Information Security Readiness Assessment Based on the KAMI Index 5.0 at RS X

These results define the security readiness of the hospital management information system (SIMRS) used at X General Hospital. The results show that the electronic system category score is 21 and is classified as having a "High" level of dependency. Therefore, the KAMI Index guidelines state that electronic system operators are required to implement SNI ISO/IEC 27001 or other security standards related to cybersecurity established by BSSN and other security standards with cybersecurity established by ministries or institutions.

The final evaluation results were obtained from the overall control completeness scores for each

area, which were adjusted to the KAMI index assessment matrix, whereby the control completeness score of 554 fell within the range of 388-646, meaning that the completeness score was included in the final evaluation results for Compliance with the Basic Framework. The results also show that the maturity level in all areas places the information security maturity level at X General Hospital at level I+ to III+.

DISCUSSION

Electronic System Category

The calculation results show a high level of dependence on information systems, describing that hospitals play a significant role in supporting health services. A high level of dependence illustrates that system disruptions, failures, and information security incidents have the potential to directly impact service continuity, service quality, and patient safety. The risks that arise are not only technical, but also operational and reputational. This condition is in line with the research by Simanullang et al., (2026), which states that the implementation of SIMRS significantly improves the effectiveness of service management and data integration in hospitals, but on the other hand also increases the level of vulnerability to information security threats if control is not implemented optimally. Based on the KAMI

Index guidelines, electronic system operators with a high level of dependency are required to implement information security standards, including SNI ISO/IEC 27001 and other cybersecurity standards set by BSSN and related ministries. Therefore, it is very important for electronic system operators in the high category to implement standardized SIMRS information security measures to reduce risks in the provision of health services.

Area Information Security Governance

The information security governance conditions at Hospital X show that roles and responsibilities related to information security have been documented and assigned to the head of IT as the person responsible for implementing the SIMRS, and that these responsibilities have been carried out consistently in accordance with the provisions assessed in the KAMI Index. In line with the research by Devlina et al., (2024) which states that institutions need to define roles and responsibilities so that all parties can clearly understand their obligations. Based on the KAMI index guidelines, level III indicates that information security policies, roles, responsibilities, and management mechanisms have been established, documented, and consistently implemented, thereby achieving operational implementation. This condition also demonstrates compliance with the requirements in ISO/IEC 27001:2022 chapters 5.2 (policy) and 5.3 (Organizational roles, responsibilities and authorities), which emphasize that policies regarding organizational roles, responsibilities, and authorities must be documented, communicated within the organization, and tailored to needs.

However, maturity level III in the governance area has not yet reached maximum maturity, and information security evaluation and improvement are still required in ISO/IEC 27001:2022 chapter 10.1 (continual improvement), which requires agencies to continuously improve the suitability, adequacy, and effectiveness of their information security management systems. The effectiveness of information security governance must be implemented periodically and through structured mechanisms. This is in line with the research by Akmal et al., (2025), which states that periodic evaluation and improvement of information security are necessary to maintain the readiness of the system in facing the dynamics of evolving data security threats.

Area Information Security Risk Management

Risk management at Hospital X is still carried out after an incident occurs, so there is no further identification for systematic risk recording and management, such as a risk register or risk treatment

plan for more systematic and planned risk control. This condition is in line with the research by Razaq & Muhammad, (2025) risk monitoring needs to be carried out in a more structured manner through the development of monitoring procedures and the establishment of clear risk metrics. Through this mechanism, organizations can identify deviations early on and take mitigation actions more quickly, so that risks can be controlled optimally.

The I+ maturity level obtained in the area of information security risk management indicates that risk management at Hospital X is still in its early stages. Based on the KAMI index guidelines, this maturity level shows that the implementation of security risk management is still limited, so the organization has the potential to experience delays in detecting risks before they develop into incidents.

The conditions in the risk management area at Hospital X are still not in accordance with ISO/IEC 27001:2022 in chapter 6.1.2 (Information security risk assessment), 6.1.3 (Information security risk treatment), which stipulates that organizations must define and implement a security risk assessment process that includes risk criteria, consistent risk assessment, risk identification, risk analysis, and risk evaluation. This condition is in line with the research by Nadanta et al., (2025) which states that institutions that do not yet have a formal risk management framework can experience difficulties in determining security priorities, suboptimal resource allocation, and the potential to face threats without structured mitigation. As explained in the study by Sri et al., (2025), a structured risk assessment can help anticipate evolving threats.

Area Information Security Framework

RS X has a number of SOPs and policies that formally support the implementation of information security. However, there are activities that are still not officially documented. In addition, performance evaluation and information security are still not consistently implemented. The maturity level II obtained in the information security framework area indicates that the maturity of implementation is still in the basic framework category. Based on the KAMI maturity level guidelines, security has been implemented, but there is some documentation that has not yet been formalized, so the level of information security maturity is not yet optimal. Rohmanto, (2025) research shows that hospitals with a low level of security management maturity generally have gaps in formal monitoring and evaluation processes, requiring improvements through policies, performance measurements, and periodic evaluations to support strategic objectives. In line with Radeta, (2025) notes that if system user training is not conducted on a scheduled basis and performance evaluations are not carried out periodically, there is a potential for a decline in information security controls.

This condition indicates that it still does not meet the requirements of ISO/IEC 27001: 2022 in chapter 7.5 (Documented Information), which states that every agency's information security management system must document all policies for the effectiveness of the management system, must ensure the creation and updating of documents, and must have written information controls to ensure that information remains available and adequately protected. In addition, section 9.1 (Monitoring, measurement, analysis, and evaluation) requires agencies to evaluate the performance and effectiveness of documented information security systems. Supported by Kurniawan (2021) research, it states that information technology security policies and procedures must be developed in an integrated manner that covers technical, managerial, and human aspects. This, periodic evaluations and reviews can be carried out as an effort to prevent security threats.

Area Information Asset Management

Asset security is carried out technically, one of which is through physical security measures, including regulations prohibiting the use of USB drives or flash drives on servers or devices, securing server rooms, installing CCTV, monitoring room temperature, and providing fire extinguishers. In

addition, information asset security is also implemented in the system, including a data backup mechanism with a 3-2-1 scheme, which means that three copies of the data are available, stored on two different media, and one copy is stored in the cloud. However, cloud service security is still limited to the initial assessment stage and is not yet supported by a risk evaluation mechanism and continuous monitoring of third-party service providers.

The maturity level in the area of information asset management is level II. This indicates that the completeness of information asset security and the asset usage cycle are still in the basic framework implementation stage. This condition shows that information asset management has been implemented technically, but has not been fully integrated into a formal framework that is documented and evaluated on an ongoing basis. If not improved, this condition has the potential to lead to uncontrolled asset life cycles, limited accountability in third-party service management, and increased exposure to risks to sensitive patient data.

Compliance with ISO/IEC 27001 has been achieved in several areas, such as in Appendix A5.9 (Inventory of information and other associated assets), which requires a documented inventory of assets and their owners, and in Appendix A7 (Physical controls), which complies with physical security requirements. However, there are still some areas that need improvement, such as in Appendix A5.23 regarding cloud services, which are still unstructured. These findings indicate that the main challenges in information asset management lie not only in technical aspects, but also in consistency and documentation, as reinforced by the research of Zaharatul et al., (2024), which shows that one of the main gaps in IT asset management is the lack of centralized asset documentation and weak monitoring of the asset life cycle from identification to disposal. making it a critical concern because poorly controlled disposal processes can increase the risk of sensitive data leaks.

Area Information Technology and Security

The implementation of information technology and security includes security measures such as Role-Based Access Control (RBAC), The implementation of role-based access control is part of the access control framework in information security and aligns with the research by Onotole, (2024), which states that restricting access based on roles and responsibilities can reduce potential exposure to sensitive data. Granting access rights, implementing access controls, setting passwords and entering OTPs, and 2FA access when accessing from outside the hospital building. This security measure is consistent with previous research showing that 2FA is effective in reducing the risk of unauthorized access resulting from compromised user credentials and in enhancing the system's resilience against account abuse (Azkiya et al., 2025). SIMRS security with external parties is also carried out through data encryption, user activity logging, data deletion management, and data backup or recovery. These security measures are crucial for enhancing the confidentiality of sensitive patient data, in line with the findings of Kumara et al., (2023), who noted that security measures involve the use of encryption and integrated access controls in the implementation of security protocols.

The maturity level in the area of technology and information security is at level III+. The III+ maturity level indicates that technology and information security have been defined and implemented consistently. This condition is in accordance with the ISO/IEC 27001:2022 standard in Appendix A8 (Technological controls), which requires every device to be configured in terms of access, access restrictions, secure authentication, activity logging, and control of the technology and network used. This is in line with the research by Yanty et al., (2024), which states that at maturity level III+, the effectiveness of security is evaluated periodically to ensure optimal information protection. Conceptually, this is in line with the principles of information security control in ISO/IEC 27001. The security measures implemented are well-defined and consistent, and their effectiveness is assessed periodically.

Area Personal Data Protection

The use and management of personal data is also reconfirmed with patients or their families for consent to access data and release information to third parties, namely BPJS and SATUSEHAT. This consent is given in the form of a signed general consent form or a photograph. However, the procedure for data destruction in the SIMRS system is unclear.

The maturity level in the personal data protection area is categorized as maturity level III. This maturity level is defined in the KAMI index guidelines as defined and consistent, achieving the highest maturity level in the Personal Data Protection area. This shows compliance with the ISO/IEC 27001:2002 standard in Appendix A5.34 (Privacy and protection of personally identifiable information), which states that there must be identification and control of compliance with requirements related to privacy preservation and personal data protection in accordance with applicable laws and regulations, as well as personal data contract requirements.

This condition is in line with the research Lestari, et al., (2025), which found a maturity level in the area of personal data protection, namely maturity level III, thus indicating that the system has been clearly defined and continuously complies with the laws and regulations related to personal data protection established by the government.

Hospital Management Information System (HMIS) Security Readiness

The SIMRS security readiness level of Hospital X based on the KAMI index calculation results shows a high level of dependence on electronic systems. However, the overall score in the areas of control completeness and maturity places the institution in the 'Basic Framework Compliance' category, with maturity levels in all areas ranging from I+ to III+. This condition indicates that although the use of electronic systems is very dominant in supporting hospital service operations, the level of information security readiness that has been implemented is not yet fully commensurate with the level of dependence. This condition is in line with the research by Nadanta et al., (2025), which states that institutions with a high level of dependence on electronic systems but are still in the basic framework implementation stage have the potential for information security gaps.

KAMI index assessment, which can be seen from the spider chart, shows that several areas still do not meet the standards because they are in the basic framework area. These areas include risk management, as risk management is still carried out reactively rather than preventively, and the information security framework, as some implementations are still carried out without official operational standards and are not yet documented. As a result, security mechanisms are not yet supported by comprehensive documented policies, procedures, or evaluations, requiring further evaluation to improve information security readiness.

The findings are consistent with previous studies conducted in universities, fintech organizations, and healthcare institutions using the KAMI Index framework, which generally reported readiness levels within the Basic Framework Fulfillment category and highlighted deficiencies in risk management and governance processes.

Although several domains achieved maturity level III, the overall readiness score remained below the minimum readiness threshold because the KAMI Index evaluates both maturity and completeness of control implementation. Critical areas such as risk management and information security framework were still categorized at lower maturity levels and had not fully met the required implementation criteria, thereby reducing the overall readiness score.

The use of self-assessment instruments may introduce subjective bias because responses depend on the respondent's knowledge and perception regarding organizational information security implementation. To reduce this risk, questionnaire findings were supported by observations and document verification.

CONCLUSION

The SIMRS security readiness assessed using the KAMI Index instrument shows that the electronic system used at RS X has a high level of dependency, where most service processes are highly dependent on the electronic system services used. However, the overall calculation results for the control completeness and maturity level are still in the Basic Framework Compliance category.

Therefore, it is recommended to improve readiness in the area of risk management by implementing risk analysis for the purpose of risk mitigation. In the area of information security framework, there are still policies that have not been fully documented and no periodic evaluation of the level of compliance, consistency, and effectiveness of information security implementation has been carried out. Therefore, hospitals need to conduct regular internal audits and strengthen operational documentation as a form of control and monitoring of policy implementation.

Priority improvements should focus on establishing a formal information security risk management framework, strengthening information security governance documentation, implementing regular internal security audits, conducting periodic staff cybersecurity training, and developing structured monitoring mechanisms for third-party service providers.

Author Contributions: Fery Fadly: Methodology, supervision, validation, review and editing; Agni Dika Seutiani: Conceptualization, data curation, investigation, formal analysis, and writing draft.

Funding: This research received no external funding.

Ethical Approval Statement: This study was conducted in accordance with ethical principles involving human participants. Ethical approval was obtained from the Ethics Committee of Komite Etik Penelitian Kesehatan (Approval Number: DP.04.03/F.XVIII.1.3.1/077/2026, Date: 20 February 2026).

Informed Consent Statement: The researcher first provided an explanation about the purpose, procedures, and aspects of the study to the participants before the research was conducted. After the explanation was given, written informed consent was obtained from all participants who agreed to be involved in the study.

Data Availability Statement: The data used in this study are available from the corresponding author upon reasonable request.

Acknowledgments: The author would like to thank the hospital and all respondents who participated in this study. Appreciation is also extended to colleagues and institutions that provided support during the data collection and manuscript preparation process.

Conflict of Interest: The author declares no conflict of interest.

References

Ahmad, A., Hastuti, J., Hijriatin, M., Indonesia Banda Aceh, S., & Tinggi Ilmu Administrasi Pelita Nusantara, S. (2025). Data Security Analysis in Electronic Health Information Systems. *Journal Informatic, Education and Management (Jiem)*, *7*(1), 1–11.

https://doi.org/10.61992/jiem.v7i1.107

Akmal, R. N., Tarwoto, Deni Dwi Susilo, Rouf, E. H., & Kodir. (2025). Evaluasi Keamanan Sistem Informasi Rumah Sakit: Metode Pengujian ISO 27001 di RS Khusus Mata Purwokerto. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *6*(1), 560–569. https://doi.org/10.35870/jimik.v6i1.1172

Aristianto, E., Hafizhuddin Hilman, M., & Yazid, S. (2025). Evaluating ISO Standards for Indonesian PDP Law Compliance: A Regulatory Mapping and Literature Review. *Scientific Journal of Informatics*, *12*(1), 145–158. https://doi.org/10.15294/sji.v12i1.21538

Azkiya, A., Budi, M., Ichsan, P., Putra, N. A., Hasibuan, F., Andrianti, R., & Maulana, I. (2025). *Analisis Sistem Autentikasi Dua Faktor (2FA) Dan Efektivitasnya Dalam Meningkatkan Keamanan Akses*. *2*(2), 196–202. https://doi.org/10.62671/jikum.v2i2.175

Badan Siber dan Sandi Negara (BSSN), "Indeks KAMI," [Online]. Available: https://www.bssn.go.id/indeks-kami/.

Christin, R., Lestari, S., Apriliya, R., & Widya, Stik. (2025). *Implementing Security Mechanisms in Hospital Information Systems: a Review*. *2*(1), 24–31.

Daniswara, M. C., Putrawanto, D. I., Najib, M., Achmadha, Z., Syaifullah Islami, M. C., & Mukaromah, S. (2023). Evaluasi Keamanan Informasi di Lingkungan Rumah Sakit: Pendekatan Audit ISO 27001 di RS Rahman Rahim Sidoarjo. *Journal of Digital Ecosystem for Natural Sustainability*, *3*(2), 64–69. https://doi.org/10.63643/jodens.v3i2.192

Deddy Kurniawan, D., & St Moh Rasyid Nagari Ketaping, J. H. (2021). Kebijakan dan Prosedur Keamanan Teknologi Informasi: Suatu Kajian Literatur. *Jurnal Ilmu Komputer Dan Sistem Informasi JIKSI*, *02*(03), 121–125. https://doi.org/10.61346/jiksi.v2i3.115

Devlina, L., Jelita, A., Noor, M., Azam, A., & Nugroho, A. (2024). *Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022*. *14*(1), 84–94. https://doi.org/10.33020/saintekom.v14i1.623

Kumara, I. N., Nanumura, U. A., & ... (2023). Enhancing Data Privacy of Medical Data through Encryption and Access Control. *International Journal of ...*, *6*(11), 38–43. https://journal.ijresm.com/index.php/ijresm/article/view/2851%0Ahttps://journal.ijresm.c om/index.php/ijresm/article/download/2851/2850Lestari, M., Puspita, M. E., Geasela, Y., Wijaya, A. F., Hiskiawan, P., & Vicky, V. (2025). Assessing Information Security Readiness in Indonesian Fintech Companies Using KAMI Index 5.0 Framework. *CogITo Smart Journal*, *11*(2), 271–280. https://doi.org/10.31154/cogito.v11i2.837.271-280

Nadanta, A. H., Farisi, H., & Brata, D. W. (2025). Analisis Evaluasi Indeks KAMI (Keamanan Informasi) 5.0 dalam Pengelolaan Keamanan Informasi di SMK Telkom Purwokerto. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *9*(8), 1–9. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/download/15233/6765

Onotole, E. F. (2024). End-to-End Encryption, Role-Based Access Controls, and Audit Logs in Safeguarding Electronic Health Records – A closer look at the features housing HER. *International Journal of Scientific Research and Engineering Trends*, *10*(6), 3103–3105.

https://doi.org/10.61137/ijsret.vol.10.issue6.629

Radeta, O. (2025). *Analisis Kematangan Tata Kelola It Pada Pengelolaan Keuangan Medical Check-Up Menggunakan Framework Cobit 5 Analisis Kematangan Tata Kelola It Pada Pengelolaan Keuangan Medical Check-Up Menggunakan Framework Cobit 5*. *3*(12).

Razaq, T. A., & Muhammad, A. H. (2025). Analisis Manajemen Risiko TI Berbasis COBIT 2019 Pada Lembaga Amil Zakat Nasional XYZ. *Jurnal Fasilkom*, *15*(1), 185–194. https://doi.org/10.37859/jf.v15i1.9093

Rohmanto, R. (2025). Pengukuran Tingkat Maturity Tata Kelola Sistem Informasi Rumah Sakit dengan Menggunakan Framework Cobit 4.1 (Studi Kasus: Rumah Sakit "A"). *Media Indormatika*, *8*(3),135–144. https://www.jurnal.masoemuniversity.ac.id/index.php/internal/article/download/1872/10 83

Simanullang, M. J., Adi, M., Aritonang, S., & Sinaga, F. M. (2026). *Analisis Keamanan Data Pasien pada Sistem Informasi Manajemen Rumah Sakit (SIMRS)*. 44–50. https://doi.org/10.58520/jddat.v5i1.98

Sri Fuji Muliati, Fidi Supriadi, & Dani Indra Junaedi. (2025). Strategi Manajemen Risiko Teknologi Informasi Berbasis Studi Literatur. *Jupiter: Publikasi Ilmu Keteknikan Industri, Teknik Elektro Dan Informatika*, *3*(2), 27–39. https://doi.org/10.61132/jupiter.v3i2.780

Yanty, T., Sinaga, M., Asril, E., Sistem, S., Fakultas, I., Komputer, I., & Lancang, U. (2024). *Evaluasi Keamanan Informasi Menggunakan Metode Indeks Keamanan Informasi (Studi Kasus : Universitas Lancang Kuning)*. 167–174.

Zaharatul, U., Asrianda, & Muhammad, F. (2024). Analisis Dan Pengelolaan Aset Teknologi Informasi Menggunakan Framework Cobit 2019. *Sports Culture*, *15*(1), 72–86. https://doi.org/10.25130/sc.24.1.6

