DECODE: JURNAL PENDIDIKAN TEKNOLOGI INFORMASI
P-ISSN: 2775-2984 | E-ISSN: 2775-1813

Vol. 4, No 3, November 2024, Hal: 881-886
Doi: http://dx.doi.org/10.51454/decode.v4i3.602
https://journal.umkendari.ac.id/index.php/decode

Analysis of Information Security Readiness Using the Index KAMI

Suryanto Nugroho[1*], Tri Rochmadi[2]

[1]Department of Informatics, Institut Teknologi Sains dan Kesehatan PKU Muhammadiyah Surakarta, Indonesia.
[2]Department of Information Systems, Universitas Alma Ata, Indonesia.

Article Info

Keywords:

Index KAMI;
Information Security;
Information Security Framework;
ISO 27001:2013;
Measuring Readiness.

Article History:

Submitted: June 03, 2024
Accepted: October 22, 2024
Published: October 23, 2024

Corresponding Author:
Suryanto Nugroho
Email: suryanto@itspku.ac.id

Abstract: Hospitals are institutions that store sensitive data. Information security needs to be implemented and audited regularly. Evaluation of information security can use the KAMI Index to determine the readiness of the application of information technology in terms of information security. Research shows that PKU Muhammadiyah Surakarta scores 31 on the electronic system assessment and 356 on the five implementation aspects. These results indicate that PKU Muhammadiyah Surakarta is in a position to implement the framework, so it is necessary to develop both technical and non-technical to be more prepared to face the digitalization era. The results of this study indicate that the KAMI index can be used as a tool and method in measuring information security readiness towards ISO 27001:2013. Based on the evaluation of the level of information security at PKU Muhammadiyah Surakarta, it is in the high category with a score of 31. The assessment of the five aspects gets a score of 356, so it is still at the stage of fulfilling the basic framework and at maturity levels I+ to II. PKU Muhammadiyah Surakarta should regularly evaluate its information security to assess progress in the five key areas outlined in the ISO 27001/SNI information security standards.

INTRODUCTION

Digitization or the use of computer equipment today cannot be separated because it is the demands of the times and many benefits that can be used for work efficiency and service improvement as well as reducing the risk of medical errors (Fatima & Colomo-Palacios, 2018), and everything is required to be fast and accessible (Ratnasari et al., 2021). Using computers and digitization is also intended to achieve the vision, mission, and good governance, namely being able to be assessed and evaluated (Riadi et al., 2020). Evaluation is needed to know the process of making decisions about the quality of objects or activities by considering values based on data and information collected, analyzed, and systematically (Nurhasanah & Harahap, 2022). A form of digitization in the health sector, leaving work related to information security because data and information related to privacy or personal data issues will gradually become large or the term big data (Lei Xu et al., 2014). The reason is that during the COVID-19 pandemic, there was an alleged theft of data leaks, which were then sold on dark web forums, which contained data obtained from patients to hospitals as an administrative requirement (Shojaei et al., 2024). On this basis, information security in hospital institutions or agencies is a critical system (Saut Siagian, 2016) because, in addition to containing privacy data, it also contains medical history data; of course, this is also a threat in itself if it is used for a crime under the pretext of providing false information that scares confiscation.

Information security in hospitals is an important thing that must be protected. Besides, it is also needed to increase public trust in the agency and prevent the use of data from irresponsible persons (Wijaya, 2021). This information security concerns elements of the CIA (Confidentiality, Integrity, and Availability), i.e., data that has been submitted by patients to the hospital must be kept confidential, the data is maintained in its originality without unilateral changes, and is easily accessible again because it is available in a sound system(Savitri et al., 2024). The CIA element in information security must be obeyed because cyber crimes are extensive, such as ARP Spoofing, which individuals can use to steal wifi account data who want to connect to the agency network (Tawar et al., 2022).

In today's digital age, organizations face increasing threats from cyberattacks, data breaches, and various security vulnerabilities. Ensuring a robust level of information security is critical to protecting sensitive data, maintaining operational continuity, and building trust with stakeholders. The KAMI Index, version 4.2 (BSSN, 2021), offers a standardized and comprehensive framework for evaluating an organization's information security posture, enabling both self-assessment and compliance with best practices. If there is an incident, a digital forensic investigation can be carried out, namely the investigation process, if there is confusion or a crime with computer equipment. (Rochmadi et al., 2020) from digital identification (Rochmadi, 2019). While the primary focus of this study is to evaluate the level of information security using the KAMI Index version 4.2, the contribution extends beyond merely measuring technical security metrics. This evaluation also emphasizes the human factor in information security, recognizing that security is not only about technology but also about user behavior and organizational culture (Glaspie & Karwowski, 2018). As Indonesia's digital landscape expands, the importance of digital literacy and information security has become increasingly evident. The growing number of theft cases and the spread of hoaxes demonstrate the vulnerabilities associated with the user element in information security (Tinmaz et al., 2022). Although numerous studies have focused on technical solutions to improve security, recent research emphasizes the critical need for a holistic approach incorporating technological advancements and the human factors influencing security outcomes (Tawar et al., 2022). This holistic approach is the key to a robust and effective information security strategy.

Current frameworks for evaluating information security, such as the KAMI Index, primarily focus on the technical aspects of security measures. However, recent studies highlight that user behavior and digital literacy play a significant role in maintaining a secure environment (Savitri et al., 2024). Without addressing these behavioral components, investments in technology alone may prove insufficient. Despite recognizing this need, more comprehensive studies must combine technological assessments with user practices and digital literacy evaluations in Indonesia's unique challenges.

This study contributes to state-of-the-art research by expanding the scope of the KAMI Index evaluation to include technical security measures and the impact of user behavior and organizational culture. By addressing both dimensions, the research aligns with the current understanding that security frameworks must integrate technological and human factors to be truly effective. Furthermore, it responds to the specific needs of Indonesia, where digital literacy is still developing, and the widespread occurrence of security breaches is often linked to the user element (Shojaei et al., 2024).

The research fills a critical gap by offering practical insights into how organizations can enhance information security through technological advancements and fostering a digital literacy and security awareness culture (Lei Xu et al., 2014). This approach provides a more comprehensive and adaptable framework for improving security in Indonesia, reflecting the latest advancements in both technology and user-centric security practices. These practical insights are invaluable for professionals and organizations seeking to bolster security measures.

METHOD

The research consists of three stages: data collection, assessment, and analysis (Figure 1).

Figure 1. Research stages

The IT manager of PKU Muhammadiyah Surakarta Hospital conducted the data collection process, conducting interviews and filling out questionnaires. The IT manager was appointed as a resource person to obtain valid information about the actual situation at PKU Muhammadiyah Surakarta so that the assessment results would be more objective.

The data was obtained and assessed using the US Index based on SNI ISO/IEC 27007 criteria. The criteria include the category of the electronic system used, governance, risk management, framework, information asset management, information technology and security, and supplement. At this point, the supplement is an additional measure for the security aspect of third-party involvement, including using the cloud, which creates new data-related risks (BSSN, 2021).

The KAMI Index (Keamanan Informasi), developed by the Indonesian National Cyber and Encryption Agency (BSSN), is a comprehensive tool for assessing the maturity level of information security within organizations. Version 4.2 of the KAMI Index offers a standardized method to evaluate how well an organization implements security measures in line with national and international information security frameworks. The index evaluates multiple aspects of information security, including policy, governance, risk management, and technical controls, making it an ideal tool for organizations like PKU Muhammadiyah Surakarta.

The KAMI Index measures information security maturity through a structured assessment of several key domains: governance and organizational structure, information security framework, risk management, security technology, incident management, and compliance and awareness. Each domain contains specific criteria that evaluate the organization's current security practices. Points are awarded based on the level of implementation, from primary to advanced practices, across these areas. The scores are then aggregated to provide an overall maturity rating, indicating the organization's readiness and resilience in managing information security risks. This comprehensive approach ensures a balanced evaluation of technical controls and governance aspects.

The KAMI Index is used because it provides a comprehensive and standardized framework specifically tailored for organizations in Indonesia, allowing for a holistic evaluation of information security maturity. It covers critical areas such as governance, risk management, technology, and compliance, ensuring that both technical and organizational aspects of security are assessed. Its localized focus makes it highly relevant to Indonesia's regulatory and cybersecurity landscape. Most

importantly, its ability to benchmark performance and identify gaps empowers organizations like PKU Muhammadiyah Surakarta to proactively address potential security issues.

RESULTS AND DISCUSSIONS

The processed data consisted of 194 questions, which were divided into three major categories, namely: the category of electronic systems, the category of completeness and maturity of information security, and the category of supplements. The electronic system category has a classification of readiness status based on its level (Table 1).

Table 1. Category electronic system

Score	Category
10 – 15	Low
16 – 34	High
35 – 50	Strategic

The results of the comprehensive electronic system category assessment, which consists of 10 questions, are at a score of 31, so PKU Muhammadiyah Surakarta is in the high category. This assessment was conducted with utmost diligence and thoroughness, ensuring the accuracy of the results. The measurement is continued in the category of completeness and maturity of information security, which consists of 131 questions and is divided into five aspects.

The governance measure scored 81, indicating a maturity level at level II. This is a significant step forward in our information security journey. Risk management has a score of 30, maturity level I+, information security framework score of 47, maturity level I+, asset management score of 132, maturity level II, and technology and information security score of 66, maturity level II (Table 2). These scores demonstrate our continuous efforts to improve and strengthen our information security measures.

Table 2. Completeness application Index KAMI

Aspect	Score	Maturity Level
Governance	81	Level II
Risk Management	30	Level I+
Information Security Framework	47	Level I+
Asset Management	132	Level II
Information Technology and Security	66	Level II
Total	**356**	**Level I+ s/d II**

Based on the data in Table 2, PKU Muhammadiyah Surakarta is in maturity level I+ to II with a score of 356. These results indicate that PKU Muhammadiyah Surakarta's final evaluation of readiness status fulfills the basic framework, as seen in the level of readiness in Table 3.

Table 3. Information security readiness level

Low		Score		Readiness Status
10	15	0	174	Not feasible
		175	312	Fulfillment of the Basic Framework
		313	535	Pretty good
		536	645	Well
High		**Score**		**Readiness Status**
16	34	0	272	Not feasible
		273	455	Fulfillment of the Basic Framework
		456	583	Pretty good
		584	645	Well

Strategic		Score		Readiness Status
35	50	0	333	Not feasible
		334	535	Fulfillment of the Basic Framework
		536	609	Pretty good
		610	645	Well

Source: Index KAMI BSSN (BSSN, 2021)

The evaluation results can also be seen in the graph (Figure 2), which shows a striking evaluation value at its high level in asset management and governance. Other aspects still need to achieve ISO 27001/SNI compliance. Of the five aspects, the average is still in the essential framework category.

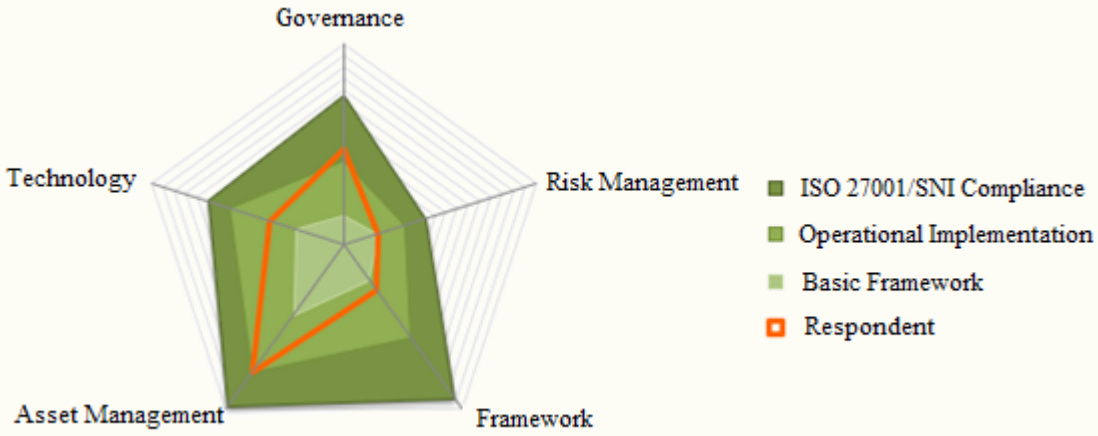

Figure 2. Spider Graph Analysis Results

In addition, additional aspects also show unbalanced values. Secure third-party engagement by 36%, security of cloud infrastructure services by 60%, and personal data protection by 58%.

Table 4. Additional Aspects of Implementation index KAMI

Aspect	Score
Third-Party Engagement	36%
Cloud Infrastructure Services	60%
Personal Data Protection	58%

PKU Muhammadiyah Surakarta needs to swiftly enhance its information security to adapt to the Fourth Industrial Revolution, which is marked by extensive computerization (Ahsan & Siddique, 2022). Urgent measures are necessary, particularly in the realms of technology and risk management, to combat cybercrime, especially the persistent and widespread threat of Cross-Site Scripting (XSS) (Wibowo, 2021).

CONCLUSIONS

Based on the evaluation of the level of information security at PKU Muhammadiyah Surakarta, it is in the high category with a score of 31. The assessment of the five aspects gets a score of 356, so it is still at the stage of fulfilling the basic framework and at maturity levels I+ to II. PKU Muhammadiyah Surakarta should regularly evaluate its information security to assess progress in the five key areas outlined in the ISO 27001/SNI information security standards. Additionally, further research could explore alternative frameworks for security management. Employing various measurement tools is crucial for obtaining more accurate results.

REFERENCES

Ahsan, M. M., & Siddique, Z. (2022). Industry 4.0 in Healthcare: A systematic review. *International Journal of Information Management Data Insights*, *2*(1), 100079. https://doi.org/10.1016/j.jjimei.2022.100079

BSSN. (2021). *Konsultasi dan Assessment Indeks KAMI*. https://www.bssn.go.id/indeks-kami/

Fatima, A., & Colomo-Palacios, R. (2018). Security Aspects in Healthcare Information Systems: A Systematic Mapping. *Procedia Computer Science*, *138*, 12–19. https://doi.org/10.1016/j.procs.2018.10.003

Nurhasanah, S., & Harahap, A. A. (2022). Evaluasi Tingkat Kesiapan Pengguna Sistem Single Sign On Pada Portal Universitas Alma Ata Menggunakan Metode Technology Readiness Index (TRI). *Indonesian Journal of Business Intelligence (IJUBI)*, *5*(1), 1. https://doi.org/10.21927/ijubi.v5i1.2126

Ratnasari, A., Harahap, A. A., Anshori, A. A., & Alam, M. (2021). Adopting task technology fit model on e-voting technology. *International Journal of Informatics and Communication Technology (IJ-ICT)*, *10*(2), 148-158. https://doi.org/10.11591/ijict.v10i2.pp148-158

Riadi, I., Riyadi Yanto, I. T., & Handoyo, E. (2020). Cyber Security Analysis of Academic Services based on Domain Delivery Services and Support using Indonesian E-Government Ratings (PEGI). *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *4*, 263–270. https://doi.org/10.22219/kinetik.v5i4.1083

Rochmadi, T. (2019). Deteksi Bukti Digital Pada Adrive Cloud Storage Menggunakan Live Forensik. *Cyber Security dan Forensik Digital*, *2*(2), 65-68. https://doi.org/10.14421/csecurity.2019.2.2.1455

Rochmadi, T., Wicaksono, Y., & Nisa, N. D. (2020). Digital evidence identification of Android device using live forensics acquisition on cloud storage (iDrive). *International Journal of Computer Applications*, *175*(26), 40-43.

Savitri, R., Firmansyah, Dworo, & Hasibuan, M. S. (2024). Information Security Measurement using INDEX KAMI at Metro City. *Journal of Applied Data Sciences*, *5*(1), 33–45. https://doi.org/10.47738/jads.v5i1.152

Siagian, S. (2016). Analisis Ancaman Keamanan Pada Sistem Informasi Manajemen Di Rumah Sakit Rimbo Medica Jambi 2015. *Scientia Journal Stikes Prima Jambi*, *4*(4), 371–375.

Shojaei, P., Vlahu-Gjorgievska, E., & Chow, Y. W. (2024). Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers, 13*(2), 41. https://doi.org/10.3390/computers13020041

Tawar, T., Riadi, I., Siregar, A. A., & Pratiwi, A. G. (2022). Security on Charity Crowdfunding Services using KAMI Index 4.1. *Engineering Science Letter*, *1*(01), 15-19. https://doi.org/10.56741/esl.v1i01.61

Wibowo, R. M., & Sulaksono, A. (2021). Web vulnerability through Cross Site Scripting (XSS) detection with OWASP security shepherd. *Indonesian Journal of Information Systems*, *3*(2), 149-159. https://doi.org/10.24002/ijis.v3i2.4192

Wijaya, Y. D. (2021). Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) Iso/Iec 27001:2013. *Jurnal Sistem Informasi Dan Informatika (Simika)*, *4*(2), 115–130. https://doi.org/10.47080/simika.v4i2.1178

Xu, L., Jiang, C., Wang, J., Yuan, J., & Ren, Y. (2014). Information Security in Big Data: Privacy and Data Mining. *Ieee Access*, *2*, 1149-1176. https://doi.org/10.1109/access.2014.2362522