Jurnal TAM *(Technology Acceptance Model)*
Jurnal TAM, Volume 16, Number 1, July 2025
E ISSN: 2579-4221; P ISSN: 2339-1103, pp. 52-57
Accredited SINTA 4 Number 225/E/KPT/2022
https://jurnal.ftikomibn.ac.id/index.php/JurnalTam/index

EVALUATION OF INFORMATION SECURITY USING THE INFORMATION SECURITY METHOD (KAMI) Case Study: UPT TIK UNIVERSITY MUHAMMADIYAH BENGKULU

Khairullah[1], RG Guntur Alam[2], AR. Walad Mahfuzi[3], Dedy Abdullah[4], Nora Fransiska[5]
[1,2,3,4,5]Informatics Engineering Study Programme, Universitas Muhammadiyah Bengkulu
[1,2,3,4,5]Kampus I, Jl. Bali, Kampung Bali, Teluk Segara, Kota Bengkulu, 38119
E-mail : khairullah@umb.ac.id[1], datuak73@yahoo.com[2], walad@umb.ac.id[3], dedy_abdullah@umb.ac.id[4], norafransiska05@gmail.com[5]

Article history:
Received: March 20, 2025
Revised: April 23, 2025
Accepted: May 16, 2025

Corresponding authors
khairullah@umb.ac.id

Keywords:
Evaluation;
Security;
Weakness;
Information.

Abstract
In the rapidly evolving digital era, educational institutions increasingly rely on information technology to manage data. However, information security is a critical issue because institutional data is an asset that is vulnerable to threats. This research aims to analyse how the OUR Index Method works in evaluating and measuring the level of information security at UPTIK. The methods used in this research include literature study to understand the concept of information security, primary data collection through interviews and questionnaires, and secondary data from policy documents and audit reports. Data analysis was conducted to compare the condition of information security at UPTIK with the standards set by OUR Index, which is based on SNI ISO/IEC 27001. The expected result of this research is a deeper understanding of the maturity level of information security at UPTIK, as well as the identification of weaknesses and potential risks. With this evaluation, it is expected that institutions can improve their information security posture, prepare for threats, and ensure that the security system implemented is in accordance with applicable standards. This research is expected to make a significant contribution to the management of information security in the educational environment, as well as a reference for other institutions that want to conduct similar evaluations.

I. INTRODUCTION

In this position, communication plays a very important role as one of the manifestations to fulfill human needs. Through communication, humans build themselves and their environment. Through communication, human civilization can advance, conversely, through communication, human civilization also declines. Through communication, human dignity can be raised and can also be plunged into despicableness beyond animals [1]. The implementation of IT in educational institutions has become commonplace. This implementation is intended to assist various functions in carrying out teaching and learning activities optimally, but of the many organizations that implement IT, the implementation of effective IT governance is still very small, especially in higher education institutions[2], [3].

Information is one of the most valuable assets for a higher education institution. Good information management will make universities have good managerial capabilities and increase the competitiveness of the university. Information security in theory is basically intended to guarantee the integrity of information, secure data confidentiality, availability of information, and ensure compliance with applicable regulations or laws. Information Technology (IT) helps organizations in various organizational business processes starting from activities related to the process, acquisition, compilation, storage and manipulation of data in various ways and procedures

to obtain quality and useful information in decision making[4]–[6].

Many tools can be used to evaluate information security, one of which is the Information Security Index or KAMI Index. The KAMI Index can help determine the condition of information security based on the SNI ISO/IEC 27001 criteria (Pratiwi & Wulandari, 2021). The use of the KAMI Index in measuring information security is a mandate from Permenkominfo No. 4 of 2016 concerning the Information Security Management System[7], [8].

Based on this, it is deemed necessary to secure the information owned, especially in the world of education that upholds noble values, and to realize this, it is first necessary to conduct an evaluation of information security using the KAMI index at UPTIK Universitas Muhammadiyah Bengkulu to find out the current picture of information security itself which is then continued with making recommendations for improvements to information security with the hope that the recommendations that have been made can be used as a consideration in improving the quality of information security at UPTIK Universitas Muhammadiyah Bengkulu so that it can always provide better services in the future and in ensuring effective utilization of Information Technology (IT) resources and minimizing losses or incidents due to misuse of available equipment or systems, either intentionally or unintentionally.

II. LITERATURE

2.1. Evaluation

The word evaluation is a loan word from English, namely "evaluation" which means assessment or estimation. Evaluation can be defined as a planned activity that aims to collect information, measure, and assess the success of a learning process or result[2], [9].

2.2. Information Security

Information security is a form of information protection and important elements, including systems and hardware, use, storage, and delivery of information. To be able to carry out protection, several work tools are needed such as policies, awareness, training, education, and technology. Meanwhile, the concept of information security according to ISO is an effort to protect information assets owned by an organization or company. This aims to ensure business continuity, minimize risks that may occur in the future and maximize the benefits obtained from investments and business opportunities[3], [10].

2.3 Information Security Index

The KAMI Index is an evaluation tool to analyze the level of information security readiness in government agencies. This evaluation tool is not intended to analyze the feasibility or effectiveness of existing forms of security, but rather as a tool to provide an overview of the readiness conditions (completeness and maturity) of the information security framework to agency leaders. The evaluation is carried out on various areas that are the target of information security implementation with a scope of discussion that also meets all aspects of security defined by the SNI ISO/IEC 27001:2009 standard[11].

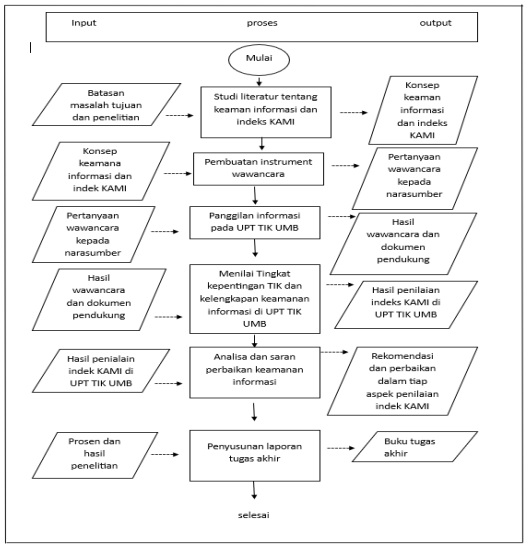
2.4 KAMI Index Evaluation Area

The KAMI Index helps institutions to see and assess the maturity level of the implementation of SNI ISO/IEC 27001:2022. The KAMI Index evaluates important areas including:

a) Information Security Governance
   This section evaluates the readiness of the form of information security governance along with the agencies/functions, duties and responsibilities of information security managers.
b) Information Security Management
   This section evaluates the readiness of the implementation of information security risk management as the basis for implementing an information security strategy.
c) Information Security Management Framework
   This section evaluates the completeness and readiness of the information security management framework (policies & procedures) and its implementation strategy.
d) Information Asset Management
   This section evaluates the completeness of security for information assets, including the entire cycle of using these assets.
e) Technology and Information Security
   This section evaluates the completeness, consistency and effectiveness of the use of technology in securing information assets.

III. RESEARCH METHODS

The methods used in this study include literature studies to understand the concept of information security, primary data collection through interviews and questionnaires, and secondary data from policy documents and audit reports. Data analysis was conducted to compare the condition of information security at UPTIK with the standards set by the KAMI Index, which is based on SNI ISO/IEC 27001. The following is the methodology that will be used during the study[1], [12], [13]



Assessing the Level of ICT Importance & Readiness

1. **Assessing the Level of ICT Importance**
   This stage is the initial step taken to conduct an assessment using the KAMI index, namely by first classifying the role of the ICT UPT of the University of Muhammadiyah Bengkulu. Grouping is used to assess the role of ICT in the institution into certain sizes, namely minimal, low, medium, high, and critical.
   From the results of the grouping, a general picture of the role of ICT in STIE Perbanas will be obtained. With this grouping, a mapping can be carried out on institutions that have the same ICT interest characteristics. The ICT Role Categories in question are as follows:
   a. Minimal
      The use of ICT within the defined scope is not significant, and its existence does not affect the ongoing work process.
   b. Low
      The use of ICT supports the ongoing work process, although not at a significant level.
   c. Medium
      The use of ICT is part of the ongoing work process, but its dependence is still limited.
   d. High
      ICT is an inseparable part of the ongoing work process.
   e. Critical
      The use of ICT is the only way to run strategic or national-scale work processes

2. **Analysis and Suggestions for Information Security Improvement**
   At this stage, suggestions and improvements will be made. After previously conducting an assessment with the KAMI index and knowing the results of each area contained in the KAMI index, the next stage is to make suggestions or recommendations for improvement in each part that is still lacking for the UPT ICT of the University of Muhammadiyah Bengkulu.

IV. RESULTS

The expected results of this study are a deeper understanding of the level of information security maturity at UPTIK, as well as identification of weaknesses and potential risks. With this evaluation, it is expected that institutions can improve their information security posture, prepare themselves for threats, and ensure that the security systems implemented are in accordance with applicable standards. This study is expected to provide a significant contribution to the management of information security in the educational environment, as well as being a reference for other institutions that wish to conduct similar evaluations.

4.1. Our Index Assessment Results Analysis

Based on the results of the score assessment per section, the following is an analysis of the results of the maturity level for all areas based on the level of score validity which can be seen in table 1.

Table 1 Validity Mapping Image Score 6 Aspects of KAMI Index

validitas	Tata kelola	Pengelolaan resiko	Kerangka kerja	Pengelolaan aset	teknologi	PDP
Tingkat Kematangan I No						
Validitas	-	-	-	-	-	-
Status	I+	I+	No	I+	I+	I+
Tingkat Kematangan II						
Validitas	No	No	No	No	No	No
Status	No	No	No	No	No	No
Tingkat Kematangan III No						
Validitas	No	No	No	No	No	No
Status	No	No	No	No	No	No
Tingkat Kematangan IV						
Validitas	No	No	No	No	No	No
Status	No	No	No	No	No	No
Status Akhir	I+ 2	I+ 2	I I	I+ 2	I+ 2	I+ 2

For the level of validity here is not to show whether the data is valid or not, but to show whether the score is valid or not to go to the next level of maturity. Based on table 1, it can be seen that the Governance score reaches the Validity level of maturity I+, followed by Risk Management, Asset Management, Technology Aspects, and PDP reaching the validity level of I+, then for the Framework does not reach the validity level of maturity I.

Table 2 Mapping Total SCORE 6 Aspects of KAMI Index

Indeks KAMI	Score	Level of Maturity
Part II: Information Security Governance	34	I+
Part III: Risk Management	22	I+
Part IV: Framework	24	I

Part V: Asset Management	81	I+
Part VI: Information Technology and Security	97	I+
Part VII: PDP	34	I+
Total Score	292	I/I+

Table 2 shows the results of measuring maturity levels II, III, V, VI, VII at the UPT ICT Muhammadiyah University of Bengkulu. To explain the rankings in the table above, the lowest order is section IV, while the highest is VI.

Table 3 Mapping All Aspects with Readiness Status

Score part I			Score Part II+III+IV+V+VI+VII		Readiness status
10	15	Low	0	247	Not feasible
			248	443	Basic Framework Compliance
			444	760	Pretty good
16	34	Tall	0	387	Not feasible
			388	646	Framework Compliance Basic Work
			647	828	pretty good
35	50	Strategis	0	472	Not feasible
			473	760	Basic Framework Compliance
			741	846	Pretty good

Table 3 shows the mapping between all parts of the KAMI Index where the higher the dependence on ICT or the more important the role of ICT to the agency's tasks, the more forms of security are needed. The following is a display of the KAMI Index radar diagram:

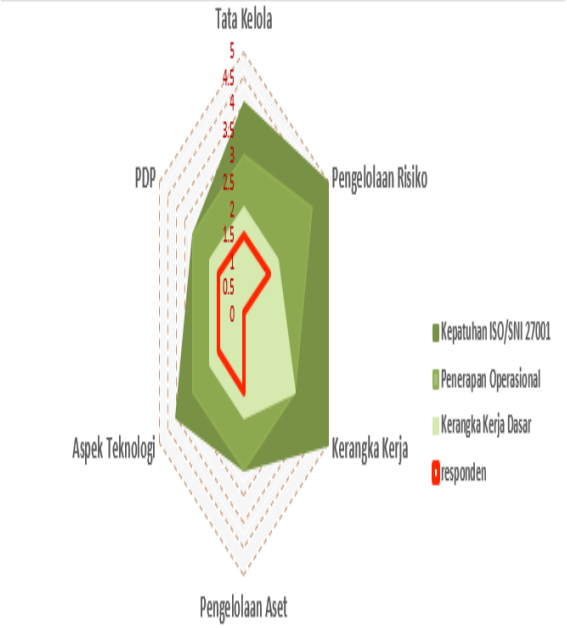


Figure 1 Radar Diagram After the assessment was carried out

The radar diagram in Figure 1 is a visual representation of the entire series of assessments that have been carried out using the KAMI Index. The value of each area is displayed in the red area. In the diagram, you can see a comparison between the readiness conditions as a result of the evaluation process with the existing completeness level reference. In the radar diagram, the background area shows the threshold for the completeness level (category) I to III (light green to dark green) of the KAMI Index. Based on the radar diagram in Figure 1, it can be seen that the smallest maturity level value of all scores is in the Risk Management area, followed by the Framework area, Governance area, PDP area, Asset Management area, and Information Technology and Security area.

Figure 2 Information Security at the ICT UPT of Muhammadiyah University of Bengkulu

For the value of each area summarized in Figure 2 shows how much completeness level of each area has been achieved at UPT ICT Universitas Muhammadiyah Bengkulu. The Completeness Status displayed by the Bar chart instrument in Figure 2 shows that the achievement is still in the red area and is still in the readiness status of "Not Eligible" with a total completeness value of 308 so that it is still not in accordance with the completeness of the control requested by the ISO / IEC 27001 standard. For the red area is still in the status of "Not Eligible", then the achievement in the yellow area is still "Needs Improvement", while the achievement of green color shows that the readiness status is "Good / Sufficient". Figure 2 also shows that the maturity level of the Framework at UPT ICT Universitas Muhammadiyah Bengkulu is still not good enough, while the maturity of information security is quite good because it has reached maturity level II.

Table 4 Characteristics of Maturity Level I

Level I – Initial Conditions (Reactive)
a. a. Beginning of understanding regarding the need for information security management
b. b. Implementation of security measures is still reactive, irregular, does not refer to the overall risk, without clear communication and authority flow and without supervision
c. c. technical and non-technical weaknesses are not properly identified.
d. d. Parties involved are not aware of their responsibilities.

Based on the results obtained from the analysis that has been done previously, it is concluded that the level of information maturity at the UPT ICT Universitas Muhammadiyah Bengkulu is at level I (First) Initial condition (Reactive) with the characteristics that have been explained in table 6.20. While the minimum limit that must be achieved to be able to carry out ISO certification is III.

4.2. Recommendations for Improvement of 6 Security Areas

Based on the analysis that has been conducted, the following are brief suggestions given to improve the six security areas of the Information Security Index (US):

a) Governance Area Recommendations

- Improve and fix several weaknesses in the information governance management system at the UPT ICT Universitas Muhammadiyah Bengkulu
- Prepare a formal information security policy document which is then published and communicated to all staff and related parties, who then carry out regular supervision, monitoring and evaluation periodically.
- Raise awareness of information security to all parties involved, either by holding training and socialization.

b) Risk Management Area Recommendations

- Implement and develop a Risk Management and Information Security Program.
- Prepare Disaster Recovery planning (DPR) In order to prevent risks and prepare internal parties optimally in facing threats and disasters

c) Framework Area Recommendations

- Improve information security management tools such as policies, procedures, and control controls.
- For information security management, improvements still need to be made in meeting the standardization of the information security framework.

d) Asset Management Area Recommendations

- Compile and Implement Information Asset Management Procedures
- Conduct a study on investment planning and evaluate the feasibility of the new system that will be implemented later.
-

e) Technology Area Recommendations

Implement standard configurations for system security for the entire system for information assets and network devices at the UPT ICT Universitas Muhammadiyah Bengkulu.

f) Personal Data Protection (PDP) Recommendations

Implement data encryption by changing text into text that cannot be understood by humans.

V. CONCLUSION

For the maturity level per area, it is known that the Governance area is at level I+, the risk management area is at level I+, the framework area is at level I, the asset management area is at level I+, the technology area is at level I+, and the PDP area is at level I+. Where the maturity level is still in the range of levels I to II, and the minimum limit that must be achieved in order to carry out ISO certification is III. These results show that most of the information security processes in the UPT ICT of the University of Muhammadiyah Bengkulu have not been carried out routinely and are not in accordance with existing standard procedures. Based on the ISO/IEC 27001:2022 standard, information security management at the UPT ICT of the University of Muhammadiyah Bengkulu still needs to be improved, especially in the Risk Management area which has the lowest score compared to other evaluation areas, followed by the Framework area and Governance Area

For further assessment, researchers should use the latest version of the Information Security Index (KAMI) research standard from the Ministry of Communication and Information in order to adapt to the development of needs, relevance and the latest technology. Detailed technical instructions are needed regarding the assessment process on the KAMI Index in order to understand the score obtained and to improve and develop the research process in the future.

REFERENCES

[1] S. Y. Yuliani, H. Heryono, A. Rosita, U. S. Zulpratita, E. A. Laksana, and F. Sulianta, "Information System Security Analysis at PT. TELKOM Using KAMI Index," *Int. J. Psychosoc. Rehabil.*, 2020.

[2] J. Jevelin and A. Faza, "Evaluation the Information Security Management System: A

Path Towards ISO 27001 Certification," *J. Inf. Syst. Informatics*, 2023.

[3] A. Supriyanto and others, "Alignment of KAMI Index with Global Security Standards in Information Security Risk Maturity Evaluation," *Cybern. Inf. Technol.*, 2025.

[4] R. Ismail, R. S. Pratama, S. Lestari, and Z. Safira, "Analisis Tingkat Keamanan Sistem Informasi Madrasah Tsanawiyah Negeri 2 Lampung Utara Menggunakan Metode Indeks KAMI," *J. Inf. Dan Komput.*, vol. 11, no. 2, 2023.

[5] S. F. Rahayu, D. Prawira, I. Rusi, and H. H. Nawawi, "Pengukuran Tingkat Keamanan Informasi Menggunakan Metode Indeks KAMI (Studi Kasus: Dinas Komunikasi dan Informatika Kota Pontianak)," *Coding J. Komput. dan Apl.*, vol. 9, no. 3, 2021.

[6] K. H. R and M. S. Hasibuan, "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan Indeks KAMI pada Tiyuh Pulung Kencana," *J. Digit. Lit. Volunt.*, vol. 2, no. 1, pp. 31–37, 2024.

[7] A. F. Manullang and L. Dwi Harsono, "Asesmen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) pada Institusi Xyz," 2017.

[8] G. Claudia and W. Wella, "ISO 27000 and KAMI Index: PT XYZ (Travel Agent)," *J. Ilmu Sist. Inf.*, 2025.

[9] W. K. Wardhani, B. Soewito, and M. Zarlis, "Information Security Evaluation Using Case Study Information Security Index on Licensing Portal Applications," *J. Inf. Syst. Informatics*, 2023.

[10] A. Kornelia and D. Irawan, "Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1," in *Jurnal Pengembangan Sistem Informasi dan Informatika*, 2021, vol. 2, no. 2.

[11] I. P. S. Syahindra and C. H. P. A. B. P. I., "Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi Xyz Menggunakan Indeks KAMI dan ISO 27005:2011," 2022.

[12] I. N. A. A. Wibawa, A. A. N. H. Susila, and M. A. Pasirulloh, "Information Security Evaluation at Hospital Using Index KAMI 5.0 and Recommendations Based on ISO/IEC 27001:2022," *J. Inf. Syst. Informatics*, 2024.

[13] P. P. Dwipayani, D. P. Githa, and M. A. Pasirulloh, "Evaluation of Information Security Based on KAMI Index and ISO/IEC 27001 at the XYZ Regency Communication and Information Office," *Int. J. Ind. Innov. Mech. Eng.*, 2025.