CoreID JOURNAL

Vol. 1 No. 3, November 2023 (90-95)
ISSN: 2987-6990
DOI: https://doi.org/10.60005/coreid.v1i3.23

Information Security Risk Measurement Using Information Security Index (KAMI) at the Information Technology and Database Center

Rifqi Syamsul Fuadi[1], Djajasukma Tjahjadi[2], Rini Astuti[3], Dhanny Setiawan[4]
[1,2,3,4] Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI

Article Info

Article history:

Received Sept 20, 2023
Revised Okt 30, 2023
Accepted Nov 18, 2023

Keywords:

Information Security Index (KAMI)
Information Security
Basic Framework Fulfillment
Risk Assessment

ABSTRACT

UIN Sunan Gunung Djati Bandung, as a rapidly growing higher education institution, faces significant challenges in ensuring information security. This research aims to improve information security at UIN Sunan Gunung Djati Bandung by applying the Information Security Index (KAMI). This method analyzes information security risks to identify potential threats, vulnerabilities, and possible impacts. The analysis revealed that security measures were already in place, but they also highlighted areas that require further attention. By achieving a final score of 415, signifying category II (Basic Framework Fulfillment), this research significantly contributed to understanding information security in higher education. Through the application of WE, this research not only provides a comprehensive overview of the status of information security at UIN Sunan Gunung Djati Bandung but also opens up opportunities to identify and address potential threats more effectively. Thus, the results of this study have important implications for improving information security and protection in higher education institutions and can be a valuable guide for similar institutions in their efforts to mitigate information security risks.

Corresponding Author:

Rifqi Syamsul Fuadi
Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI
Jl. Ir. Juanda 96 Bandung 40132
Email: rifqi.syams@gmail.com

1. INTRODUCTION

Universities are primarily responsible for providing services to the community to produce qualified and valuable human resources. To achieve this goal, universities must provide excellent, effective, and efficient academic services. To carry out these academic services, a supporting information system is crucial. The success of educational services in educational institutions depends on the effectiveness of information technology management practices [1], [2].

One of the threats in the digital environment is web defacement attacks, which target vulnerable websites or web servers to corrupt, modify, or delete web page content. Statistics show that such attacks occur with significant frequency. Information security is crucial to protect the information assets and infrastructure of universities [3].

In 2021, the academic sector, including universities, experienced the highest number of cases of web defacement attacks. Therefore, it is essential to adopt information security measures, such as an Information Security Management System (ISMS), to protect information assets from potential threats and disruptions[2].

The Information Technology and Database Center (PTIPD) is one of the technical implementation units (UPT) at UIN Sunan Gunung Djati Bandung. Initially, PTIPD consisted of two units, the IT Center and the Computer Center (Puskom), combined with simple tasks according to the institution's needs. Legally, the existence of Puskom was included in the Decree of the Minister of Religious Affairs No. 385 of 1993, dated December 29, 1993, concerning the Organization and Work Procedures of IAIN Sunan Gunung Djati Bandung.

Article 60 of the decree explains that Puskom is a supporting element of IAIN Sunan Gunung Djati Bandung in the field of computers [4], [5].

To improve the quality of administrative services, the Chancellor of IAIN, Sunan Gunung Djati Bandung, formed an implementation team to prepare the Computer Center Program. Due to the demands of the times that require fast and accurate information in 2011, the IT Center was established as a technical implementation unit for IT issues at UIN Sunan Gunung Djati Bandung. Then, in 2015, the Computer Center and IT Center were merged into one technical implementation unit called the Center for Information Technology and Database (PTIPD) [4].

This change in the name, duties, and functions of the data management and information technology implementing unit occurred in response to nationally applicable needs. Similar standards on the unit's name, duties, and functions are also applied to all State Islamic Religious Universities (PTAIN). For UIN Sunan Gunung Djati Bandung, the changes are regulated in the Regulation of the Minister of Religious Affairs of the Republic of Indonesia (PMA RI) Number 26 of 2015 concerning the Organization and Work Procedures of UIN Sunan Gunung Djati Bandung. In the PMA RI, PTIPD has the task of managing and developing management information systems, network and application development and maintenance, database management, other technology development, and network cooperation. A head appointed by the Rector leads PTIPD and is responsible to the Vice Rector II for General Administration, Planning, and Finance.

Amid the complexity of the university environment, State Islamic University (UIN) Sunan Gunung Djati Bandung is one of the institutions highly dependent on information technology. In this context, it is necessary to implement an information technology governance mechanism by the standards and vision-mission of the institution. Information security evaluation and management are vital in maintaining information integrity, confidentiality, and availability.

To improve the quality of information security, the Ministry of Information and Communication developed the Information Security Index (KAMI), which is used to evaluate the maturity level of ISO 27001 standard implementation in the information security governance [6]. KAMI implementation can help institutions achieve goals and create value through effective information technology governance.

2. METHOD

The KAMI Index, developed by the National Cyber and Crypto Agency (BSSN), is a guide used to analyze and evaluate the readiness level in implementing information security. The KAMI Index is a Microsoft Excel application. Various organizations, including government agencies, non-government agencies, national-scale organizations, and small and medium organizations can use it. Apart from that, this index can also be used by companies of various levels and sizes and multiple interests in using information technology in carrying out their business processes [7], [8].

The KAMI index is based on the criteria contained in the Indonesian National Standard ISO/IEC 27001:2013. In other words, the evaluation carried out using the KAMI index covers and fulfills all aspects included in the ISO 27001:2013 standard [3], [9], [10]

The KAMI Index functions as a tool to provide an overview of the state of information security readiness to agency leaders. Through analysis carried out by the KAMI index, information security is evaluated in terms of improvement, development, and implementation. The data resulting from this evaluation provides an overview of the readiness level in terms of completeness and maturity of the information security that has been implemented. Furthermore, the results of this evaluation can be used to compare and make improvements.

This research methodology uses a systematic qualitative method with a case study approach, which can be used as a guideline for researchers so that the results achieved do not deviate. The desired objectives can be carried out correctly and follow the predetermined goals. The methods used here are literature studies, problem identification, data collection, data analysis, and implementing information security evaluation guidelines with Indeks KAMI version 4.2 [10]–[12].

In doing this research, the author will look at the results from the literature study, namely the improvement recommendations obtained from the analysis carried out on the current IT process maturity level and the expected maturity level; several steps will be taken.

3. RESULTS AND DISCUSSION

A risk is an unavoidable event. Therefore, it is essential that we specifically manage it carefully. The interview process results indicate that PTIPD has never conducted an audit related to information security risks, which means that the risk management and management process has not been carried out. There is no application of specific standards related to information security risk management. When errors occur, or risks arise, PTIPD only adopts an acceptance or prevention approach to risks that could adversely affect the organization. Since the organization prioritizes goals other than financial gain, the most common risks to avoid are those that could be detrimental to customer satisfaction and consume valuable time.

3.1. Discussion of Analysis of Assessment Results Index KAMI

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

Table 1. Mapping the validity of information security completeness and maturity scores INDEX KAMI

Validity	System Manage	Management Risk	Framework	Management Asset	Technology
Maturity Level I					
Validity	Yes	Yes	Yes	Yes	Yes
Status	I+	I	I+	I	I
Maturity Level II					
Validity	No	Yes	No	Yes	Yes
Status	No	II	No	II+	II
Maturity Level III					
Validity	No	No	No	No	Yes
Status	No	No	No	No	III+
Maturity Level IV					
Validity	No	No	No	No	No
Status	No	No	No	No	No
I+					
Status Akhir	**I+**	**II**	**I+**	**II+**	**III+**

The validity level 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 maturity level.

Table 1 shows that the Governance area and Framework area scores reach the Maturity Validity Level I +, which means reaching Maturity Level I but not quite Maturity Level II. The risk management area is at maturity level II, and asset management is at maturity level II +, with the highest maturity level, namely the information security technology area.

Table 2 shows the results of measuring the information security maturity level for Sections II, III, IV, V, and VI at UIN Bandung.

Table 2. 5 Aspect Total Score Averaging Indeks KAMI

Indeks KAMI	Skor	Tingkat Kematangan
Bagian II: Information Security Governance	83	I+
Bagian III: Information Security Risk Management	44	II
Bagian IV: Information Security Management Framework	48	I+
Bagian V: Information Asset Management	129	II+
Bagian VI: Information Technology and Security	111	III+
Total Skor (II+III+IV+V+VI)	**415**	**I+ s/d III+**

Table 3 shows the mapping between all parts of Indeks KAMI where the higher the dependence on Electronic Systems or the more critical the role of Electronic Systems in the agency's tasks, the more forms of security are needed.

Table 3. Mapping of All Aspects with Readiness Status

Electronic Systems			Section Score II+III+IV+V+VI		Readiness Status
Section Score I					
0	12	Low	0	174	Poor
			175	312	Compliance with the Basic Framework
			313	535	Fair
			536	645	Good
25	36	Tall	0	272	Poor
			273	455	Compliance with the Basic Framework
			456	583	Fair
			584	645	Good
37	48	Strategic	0	333	Poor
			334	535	Compliance with the Basic Framework
			536	609	Fair
			610	645	Good

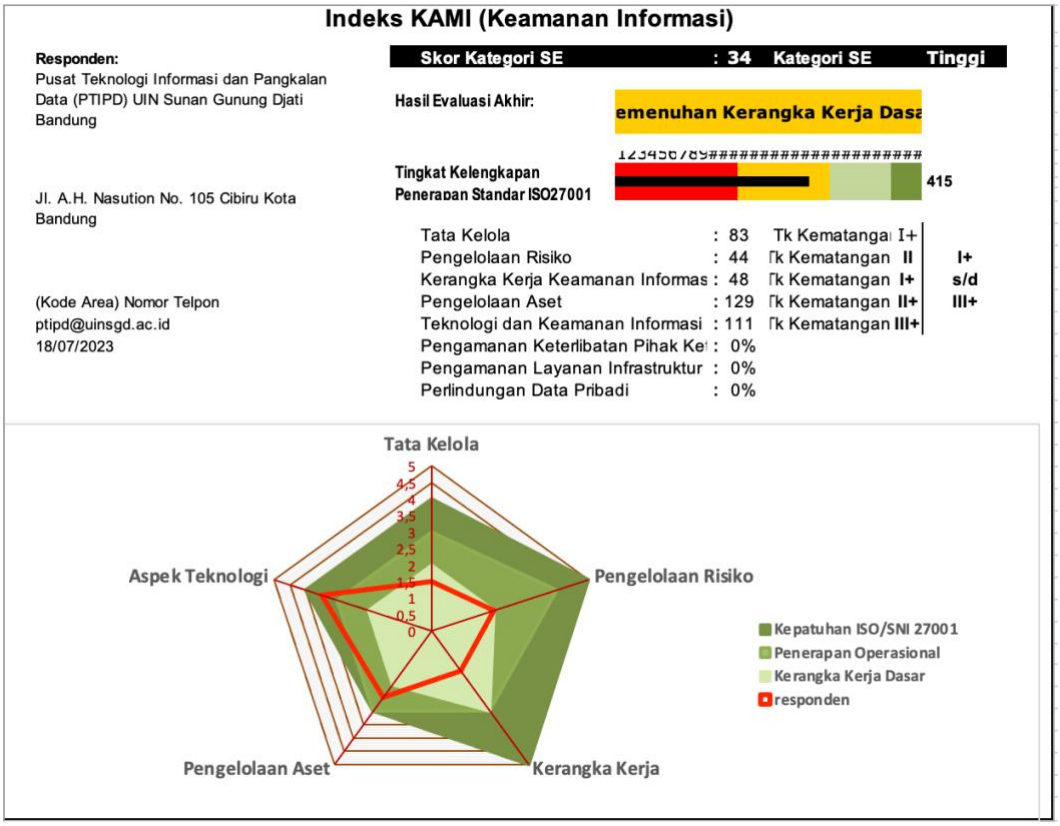

Figure 1. Indeks KAMI Assessment Dashboard at PTIPD UIN Bandung

Based on the Indeks KAMI assessment dashboard at PTIPD UIN Bandung Figure 2, it can be seen that the evaluation results are in yellow, which indicates that the level of information security at UIN Bandung is in Category II (Basic Framework Fulfillment). However, it should be noted that the minimum threshold required to obtain ISO certification is Category III.

3.2. Recommended Improvements 5 Security Area

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

1. Governance Area Recommendations

a) Improve and correct some weaknesses in the information security governance management system at UIN Bandung.

b) Develop a formal Information Security Policy Document, which is then published and communicated to all staff and related parties, who regularly conduct regular supervision, monitoring, and evaluation.

c) Increase information security awareness to all parties involved by conducting socialization, training, certification, etc.

2. Risk Management Area Recommendations

a) Develop and implement Risk Management and Information Security Systems/Programs.

b) Develop Disaster Recovery Planning (DRP) to minimize risks and prepare internal parties for threats and disasters optimally.

3. Framework Area Recommendations

a) Improving information security management tools such as information security management standards (ISMS), policies, procedures, and control controls such as forms and checklists.

b) For information security management, there is still a need for improvement in meeting the ISO / IEC 27001: 2005 standardization, especially in the information security framework documentation.

4. Asset Management Area Recommendations

a) Develop and implement information asset management procedures

b) Conduct a study on financial planning (investment) and evaluate the feasibility of the new system that will be implemented.

5. Technology Area Recommendations
   Establish a standard configuration for system security for the entire system for all information assets and network devices.

4. CONCLUSION

Based on the data from the assessment of the information security management area obtained, the risk management needs at UIN Sunan Gunung Djati Bandung have been protected quite well. This is evidenced by establishing the person in charge of risk management and escalating reporting on information security risk management status to the leadership level.

The implementation of information security governance at this time still needs to be improved to meet the organization's needs for information security because, from the results obtained, the majority are still in planning.

In the context of the information security completeness score obtained from the five areas in the Indeks KAMI of 415 out of a total overall score of 645 and being at level II of the Basic Framework, this may imply that the College has made reasonable efforts in developing a foundation for information security, identifying risks, and implementing basic controls. However, there is still room for further improvement, especially in optimizing the use of security technologies, measuring the effectiveness of controls, and conducting more in-depth risk assessments.

The following are some recommendations that can be given to improve information security in Higher Education Institutions that have reached level II in our Basic Framework Index:

a) Conduct regular training for staff and faculty on information security practices, including cyberattack prevention and secure password management.
b) Increase security awareness among students by holding regular training sessions or security awareness campaigns.
c) Conduct regular security audits and vulnerability testing to identify potential loopholes or security issues that may have been overlooked.
d) Implement recommendations from audits and testing to address potential findings.
e) Create a comprehensive information security plan with detailed control measures and mitigation actions.
f) Ensure that the risk management measures that have been implemented are continuously monitored and evaluated regularly to ensure their effectiveness.

Research related to information security still opens many opportunities for researchers because many aspects can be studied using various frameworks. This research is expected to be a bridge for further research. Future research is expected to be more specific, such as researching in the context of legal and compliance aspects and examining the relationship between information security in higher education and applicable legal regulations and regulations, such as personal data protection. How can universities comply with these regulations and protect data effectively? Analyze the impact of information security on college reputation, examine how information security incidents can affect college reputation, and how reputation management can be improved through a good information security strategy.

REFERENCES

[1] C. E. Gunawan and Fernando, "Pengukuran Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Studi Kasus di PUSTIPD UIN Raden Fatah Palembang," *J. Sist. Inf.*, vol. 4, pp. 121–132, 2018.
[2] A. Kornelia and D. Irawan, "Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1," *J. Pengemb. Sist. Inf. dan Inform.*, vol. 2, no. 2, pp. 78–86, 2021.
[3] E. Novianto *et al.*, "Keamanan Informasi (Information Security) pada Aplikasi Sistem Informasi Manajemen Sumber Daya Manusia," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 8, no. 1, pp. 10–15, Jan. 2023.
[4] "Struktur Organisasi UIN Sunan Gunung Djati Bandung - UIN Sunan Gunung Djati Bandung," 2021. [Online]. Available: https://uinsgd.ac.id/struktur-organisasi-uin-sunan-gunung-djati-bandung/. [Accessed: 07-Jun-2023].
[5] "Pusat Teknologi Informasi dan Pangkalan Data - UIN Sunan Gunung Djati Bandung." [Online]. Available: https://uinsgd.ac.id/pusat-teknologi-informasi-dan-pangkalan-data/. [Accessed: 13-Jun-2023].
[6] E. R. Pratama, "Evaluasi Tata Kelola Sistem Informasi Menggunakan Indeks KAMI dan ISO 27001,"

Universitas Brawijaya, 2018.
[7] BSSN, "Laporan Tahunan Monitoring Keamanan Siber 2021," Jakarta, 2021.
[8] R. A. Syarif and A. Nugroho, "Analisis Tingkat Kematangan Sistem Manajemen Keamanan Informasi Direktorat Jenderal Perbendaharaan Diukur Dengan Menggunakan Indeks Keamanan Informasi (Studi Kasus: Aplikasi Span)," *J. Info Artha*, vol. Syarif, R., pp. 69–80, 2016.
[9] J. Saptoro and G. Gunawan, "Pengaruh Budaya Organisasi, Teknologi Informasi, Dan Sistem Informasi Akuntansi Manajemen Terhadap Kinerja Manajerial PT. Propan Raya I.C.C Cab. Bandung," *JASa*, vol. 2, no. 4, 2018.
[10] I. Putu, S. Syahindra, C. H. Primasari, A. Bagas, and P. Irianto, "Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi XYZ Menggunakan Indeks KAMI dan ISO 27005 : 2011," *J. Teknoinfo*, vol. 16, no. 2, pp. 165–182, Jul. 2022.
[11] M. F. Husin, H. . Wowor, and S. D. . Karouw, "Implementasi Indeks Kami Di Universitas Sam Ratulangi," *J. Tek. Inform.*, vol. 12, no. 1, 2017.
[12] BSSN, "Konsultasi dan Assessment Indeks KAMI Versi 4.2," 2021. [Online]. Available: https://bssn.go.id/indeks-kami/. [Accessed: 14-Apr-2023].