Matrix: Jurnal Manajemen Teknologi dan Informatika
Volume 11 Issue 2 Year 2021 Pages 55-62

DOI: http://dx.doi.org/10.31940/matrix.v11i2.2447
URL: http://ojs.pnb.ac.id/index.php/matrix

KAMI index as an evaluation of academic information system security at XYZ university

***Andi Sofyan Anas* [1]*, *I Gusti Ayu Sri Devi Gayatri Utami* [2], *Adam Bachtiar Maulachela* [3], *Akbar Juliansyah* [4]**

[1,2] *universitas Bumigora, Indonesia*
[3,4] *Universitas Pendidikan Mandalika , Indonesia*

*Corresponding Author: *andi.sofyan@universitasbumigora.ac.id*

Abstract: XYZ University is one of the universities that has used information technology to create quality service for students and the entire academic community. This Information technology service is managed by Information Technology and Communication Center (PUSTIK) which is responsible to carry out the development, management, service, and maintaining the security of information and communication technology. Good information technology governance should be able to maintain information security. Therefore, it is necessary to evaluate information system security especially the security of academic information systems. This information system security evaluation uses *Keamanan Informasi* (KAMI) Index which refers to the ISO/IEC 27001:2013 standard to be able to determine the maturity level of information security. An evaluation of five areas of the KAMI Index shows the Information Security Risk Management area gets the lowest score at 10 out of a total of 72. The result of the KAMI Index dashboard shows that the maturity level of each area of information security is at levels I and I+ with a total score of 166. This means that the level of completeness of implement ISO 27001:2013 standard is in the inadequate category.

Keywords: KAMI index, ISO/IEC 27001:2013, evaluation, security, information

History Article: Submitted 27 March 2021 | Revised 26 April 2021 | Accepted 17 May 2021

How to Cite: A. S. Anas, I. G. A. S. D. G Utami, A. B. Maulachela, A. Juliansyah, “KAMI index as an evaluation of academic information system security at XYZ university,” *Matrix: Jurnal Manajemen Teknologi dan Informatika*, vol. 11, no. 2, pp. 55-63, 2021.

Introduction

Until now, an organization still relies on information to help effectiveness and create quality services [1]. The implementation of Information Technology governance has now become a necessity and also a note in agencies, given the role of Information Technology which is currently increasingly important as a realization of good organizational or corporate governance [2]. Information technology governance should be able to maintain information security. According to Tata Sutabri in Edo Rizky Pratama, et al., Information is the most valuable data in the decision-making process [3]. Maintaining information security means protecting all information assets owned from threats that may arise, by taking into account the security factors of all supporting devices, networks, and other facilities that are directly or indirectly related to the information processing [4].

Educational institutions in Indonesia need to implement an information security system to safeguard their data to ensure security and authenticity. Information security is an effort to protect information assets from threats that may arise. The risk of data damage, loss, and exposure to unwanted parties is directly proportional to the increasing number of information stored, managed, and shared [5]. According to Husaini et al. In Prastiyawan et al. defines Risk as the probability of an event that can harm the company due to vulnerabilities and threats [6]. XYZ University is one of the educational institutions that has implemented an academic information system to provide information to students and the academic community. This Academic Information System is managed and developed by the Center for Information and Communication

Technology (PUSTIK). PUSTIK is responsible for carrying out the development, management, and services of information and communication technology. Information system security must be managed since the information system was built, not as a complement to the information systems [7].

Information security in the XYZ University academic information system is very necessary because it involves the data of all students, lecturers, and employees. Data that is not maintained, data integrity that cannot be maintained, affect the effectiveness and efficiency in providing and offering information to the academic community and disrupting the institution in achieving its institutional goals and strategies [8].

Because information system security is so important, a good policy with procedures is needed, including Asset management, human resource management, physical and environmental safeguards, logical security, information technology operational security, and incident handling in information security. Information system security evaluation must apply information system security audit techniques to ensure information system security meets standards and is following procedures. Evaluation is the process of evaluating objects by first taking measurements [9].

To be able to revise and improve the quality of information security of an institution, the Ministry of Communication and Information makes efforts one of which is to create an Information Security Index / Indeks Keamanan Informasi (KAMI) which is a tool to measure the level of maturity and completeness in information security. The KAMI index refers to the information security standard, namely ISO 27001 [10]. The KAMI index is not used to analyze the feasibility or effectiveness of information security, but as a tool that provides an overview of the readiness of an information security framework to leaders [11].

The specifications and requirements that must be met in building an Information Security Management System (ISMS) are regulated in ISO / IEC 27001. ISO 27001 is a standard that describes the management of information security in an organization. An overview of the needs of an organization in its efforts to implement information security concepts can be provided by ISO 27001 [12]. This standard is independent of information technology products, requires the use of a risk-based management approach, and is designed to ensure that selected security controls can protect information assets from various risks and assure the level of security for interested parties [10].

Based on the description that has been described, a study on the Evaluation of Academic Information Security Systems at XYZ University was carried out using the KAMI Index tool by referring to the ISO / IEC 27001: 2013 standard to be able to determine the maturity level of academic information system security.

Methodology

The stages carried out in this study are following this chart:

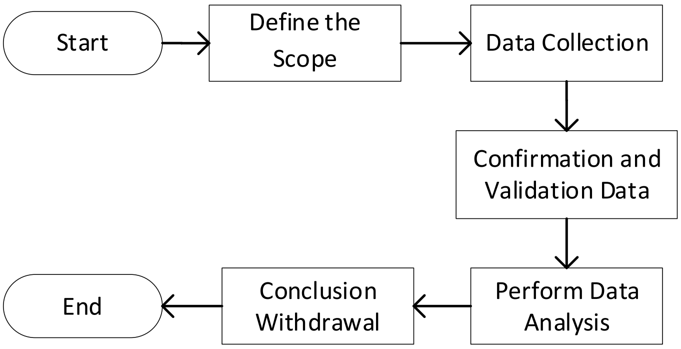


Figure 1. Research stages

Define the Scope

The research begins with defining the scope. XYZ University certainly understands the importance of information system security for campus success. Institutions or companies must pay attention to information system security because it can cause harm to the institution in the event of leakage and system failure [13]. The confidentiality and authenticity of the data and information processed will be maintained because of the good security of the information system. Therefore, it is necessary to evaluate information security to determine the maturity level of academic information system security at XYZ University using the KAMI index by referring to the ISO / IEC 27001: 2013 standard.

Data Collection

At the stage of data collection obtained from direct observation, filling out questionnaires, and interviews with competent parties on the object to be studied. Observations were made to determine the conditions of the existing security management for the system. So that later the results of the observations are used in determining the appropriate objective control. Furthermore, to obtain primary data, interviews were conducted with several managers related to academic information systems. Interviewed managers consisted of PUSTIK, Academic Administration (BAAK) and XYZ University Vice-Chancellor II (WR II).

Confirmation and Validation Data

Data confirmation and validation were carried out to check the authenticity and validity of the data obtained from the informants. This stage is carried out by the checklist method [14]. The checklist was carried out by respondents, namely the PUSTIK, BAAK, and WR II sections. This data validation was carried out concerning the five areas of the Index.

Perform Data Analysis

The next stage is data analysis to obtain evaluation results on the level of completeness of the application of the ISO 27001: 2013 standard. The data were analyzed using the existing formulation in the Information Security Index (KAMI Index) against the previously distributed questionnaires, so that the level of maturity and completeness of information security was obtained, which was then adjusted to ISO 27001: 2013 standards. Annex A or security control in the ISO / IEC 27001: 2013 structure consists of 14 domain areas, 35 objective controls, and 114 information security controls [10].

Areas in the KAMI Index, which are used to measure the maturity level of the ISMS at an institution, summarize the 14 domain areas in the ISO 27001 structure into 5 evaluation areas [3]. The relationship between the KAMI index and ISO 27001 can be seen in Figure 2 below.

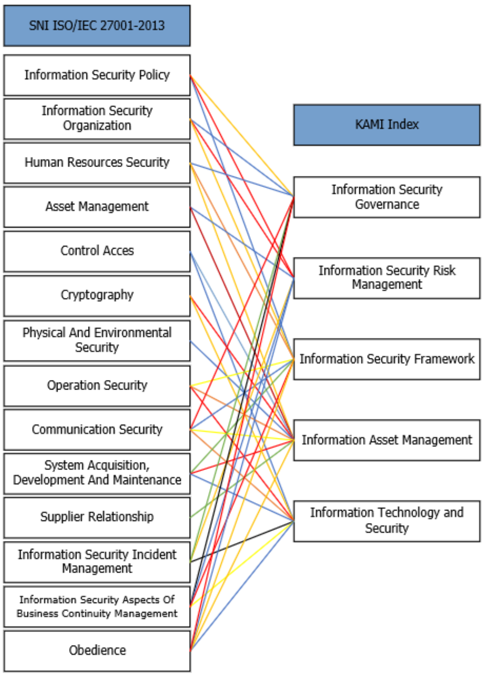

SNI ISO/IEC 27001-2013
Information Security Policy
Information Security Organization
Human Resources Security
Asset Management
Control Acces
Cryptography
Physical And Environmental Security
Operation Security
Communication Security
System Acquisition, Development And Maintenance
Supplier Relationship
Information Security Incident Management
Information Security Aspects Of Business Continuity Management
Obedience
KAMI Index
Information Security Governance
Information Security Risk Management
Information Security Framework
Information Asset Management
Information Technology and Security

Figure 2. KAMI Index relationship with ISO 27001 [3]

Conclusion

The last stage is to conclude the results of the data analysis that has been carried out. With this conclusion, we can find out the maturity level and feasibility of academic information system security at XYZ University.

Results and Discussions

The evaluation process is carried out by answering several questions from the following areas [10]:

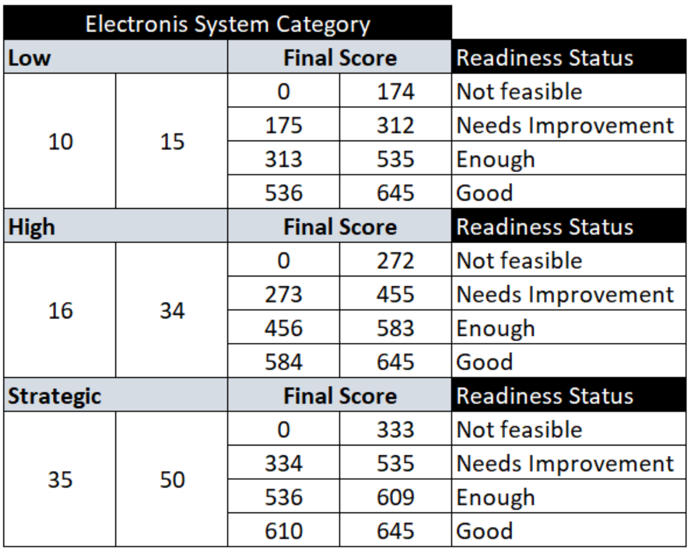
1. Information System Security Governance
2. Information Security Risk Management
3. Information Security Framework
4. Information Asset Management
5. Information Technology and Security.

The answer to each question is scored to generate an index score and is also used to display the evaluation results in the dashboard at the end of the process. The score for each question refers to the following Table 1.

Table 1. KAMI index score mapping

	Security Category		
Security Status	1	2	3
Is Not Done	0	0	0
In planning	1	2	3
In an application or partially applied	2	4	6
Applied thoroughly	3	6	9

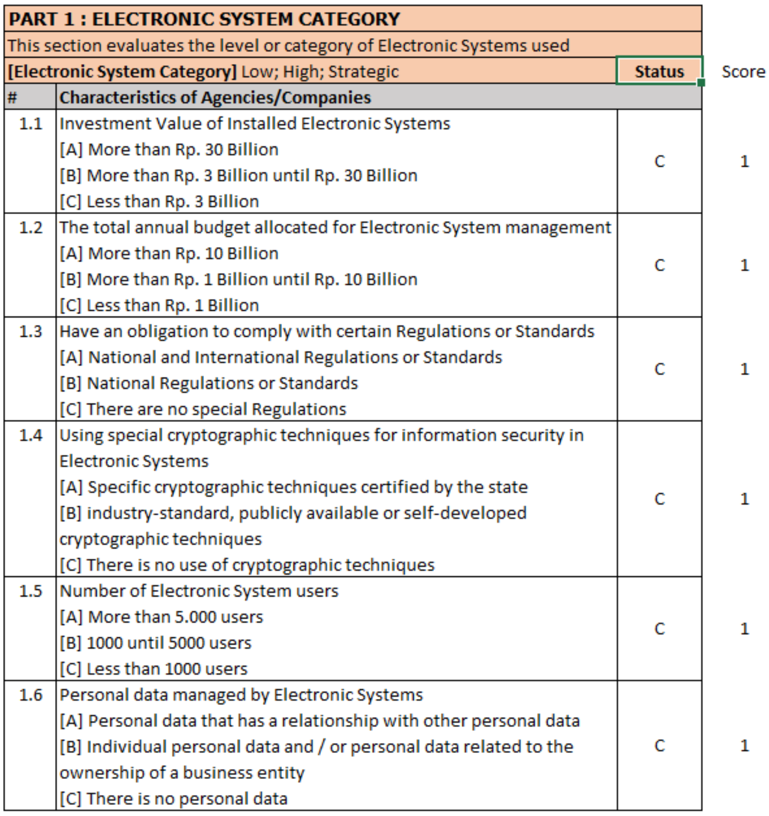
Before answering each question from the five evaluation areas on the KAMI index, first, the Electronic Systems category classification is carried out. Respondents must briefly describe the Electronic System in their work unit. It aims to classify the electronic systems used into certain levels, namely low, high and strategic [10]. The correlation between the Electronic System Category and the readiness status can be seen in Figure 3 below:



Electronis System Category				
Low		**Final Score**		**Readiness Status**
10	15	0	174	Not feasible
		175	312	Needs Improvement
		313	535	Enough
		536	645	Good
High		**Final Score**		**Readiness Status**
16	34	0	272	Not feasible
		273	455	Needs Improvement
		456	583	Enough
		584	645	Good
Strategic		**Final Score**		**Readiness Status**
35	50	0	333	Not feasible
		334	535	Needs Improvement
		536	609	Enough
		610	645	Good

Figure 3. Correlation matrix of electronic system categories and readiness status

The results of the assessment for the Electronic Systems category level at XYZ University can be seen in Figure 4 below:

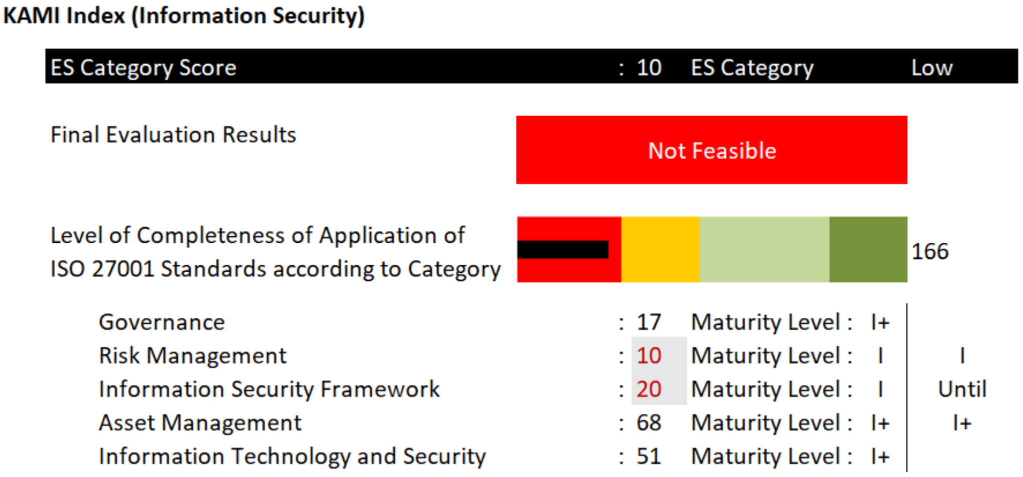


PART 1 : ELECTRONIC SYSTEM CATEGORY			
This section evaluates the level or category of Electronic Systems used			
[Electronic System Category] Low; High; Strategic		**Status**	Score
#	**Characteristics of Agencies/Companies**		
1.1	Investment Value of Installed Electronic Systems [A] More than Rp. 30 Billion [B] More than Rp. 3 Billion until Rp. 30 Billion [C] Less than Rp. 3 Billion	C	1
1.2	The total annual budget allocated for Electronic System management [A] More than Rp. 10 Billion [B] More than Rp. 1 Billion until Rp. 10 Billion [C] Less than Rp. 1 Billion	C	1
1.3	Have an obligation to comply with certain Regulations or Standards [A] National and International Regulations or Standards [B] National Regulations or Standards [C] There are no special Regulations	C	1
1.4	Using special cryptographic techniques for information security in Electronic Systems [A] Specific cryptographic techniques certified by the state [B] industry-standard, publicly available or self-developed cryptographic techniques [C] There is no use of cryptographic techniques	C	1
1.5	Number of Electronic System users [A] More than 5.000 users [B] 1000 until 5000 users [C] Less than 1000 users	C	1
1.6	Personal data managed by Electronic Systems [A] Personal data that has a relationship with other personal data [B] Individual personal data and / or personal data related to the ownership of a business entity [C] There is no personal data	C	1

Figure 4. Electronic system readiness status

From the results of the XYZ University Electronic System Category assessment, it was obtained a score of 10, so it was in the Low category because it was in the range of values 10-15. This low category means the importance of using Electronic Systems at XYZ University has not become a priority and there is still a lack of awareness about the importance of using Electronic Systems.

The next stage is to evaluate 5 areas on the KAMI index. Respondents did a checklist to confirm data by comparing the results of the questionnaire with the actual situation. From this checklist, the results of the level of completeness and security of information are obtained as shown in Figure 5 on the KAMI Index dashboard.



KAMI Index (Information Security)

ES Category Score : 10 ES Category Low

Final Evaluation Results — Not Feasible

Level of Completeness of Application of ISO 27001 Standards according to Category — 166

Governance	: 17	Maturity Level :	I+	
Risk Management	: 10	Maturity Level :	I	I
Information Security Framework	: 20	Maturity Level :	I	Until
Asset Management	: 68	Maturity Level :	I+	I+
Information Technology and Security	: 51	Maturity Level :	I+	

Figure 5. Information security maturity level

Based on Figure 5, it can be stated that the level of completeness of the application of the ISO 27001 Standard according to the electronic category gets a score of 166 with maturity levels at levels I to I +, and is in the red area which means the status is not feasible.

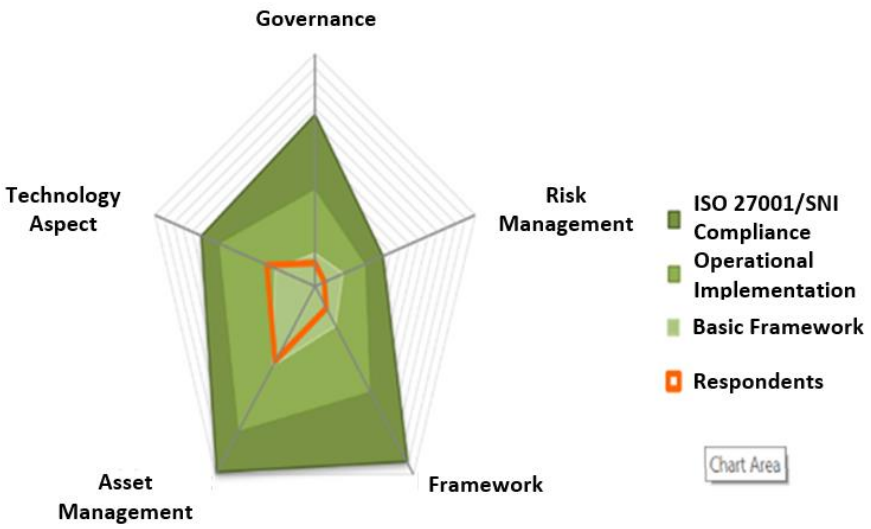


Figure 6. Radar diagram Information security maturity level

Based on the results of the radar diagram in Figure 6, the data is obtained from the calculation of the KAMI Index, showing the Red section or Red area (Respondents) on the bar chart is the security condition of the XYZ University academic information system. From the five areas of information security, it can be observed that the academic information system of XYZ University has a technological aspect that is in the operational implementation process area. Meanwhile, governance, risk management, framework, and asset management are in the basic framework area in the information system security management process.

The following is a description of the percentage maturity level of the five areas previously assessed using the KAMI Index Version 4.0:

Table 2. Percentage of information maturity level

Annotation	Governance	Risk Management	Framework	Asset Management	Security Technology
Max Score	126	72	159	168	120
Respondents	17	10	20	68	51
Percentage	13%	14%	12%	40%	42%

Based on Table 2 it can be described as follows:

1. In the Information Security Governance area, the respondent's score was 17 (13%) from a maximum score of 126. This score was obtained from 13 scores representing maturity level II, 4 scores representing maturity level III, and 0 scores representing maturity level IV. The Information Security Governance Area is classified into the status level of maturity level I + with a score of 13. Because it has exceeded the minimum maturity level, which is 12 but does not exceed the requirements to reach the minimum value of maturity level II, namely 36. The status of the maturity level of the security governance area This information relates to domain control areas A5 (Information Security), A7 (Human resource security) at ISO 27001: 2013.
2. In the Information Security Risk Management area, the respondent's score is 10 (14%) of the maximum score of 72, the score is 8 scores representing maturity level II, 2 scores representing maturity level III, 0 scores representing maturity level IV, and 0 The score represents the level of maturity V. The Information Security Risk Management Area is classified into the status level of maturity level I with a score of 8. Therefore it has not

exceeded the minimum maturity level of 14 and also does not exceed the requirements to reach a minimum value of maturity level II, namely 20. The relationship between the status of the maturity level of the information security risk management area with ISO 27001: 2013 is in the domain control areas A5 (Information Security) and A8 (Asset Management).

3. In the Information Security Management Framework area, it was found that respondents were 20 (12%) from a maximum score of 159, obtained from 10 scores representing maturity level II, 10 scores representing maturity level III, 0 scores representing maturity level IV, and 0 scores represent the level of maturity V. The Information Security Management Framework Area is classified into the status level of maturity level I with a score of 10. Therefore it has not exceeded the minimum maturity level of 15 and also does not exceed the requirements to reach a minimum value of maturity level II, namely 24. The relationship between the status of this area's maturity level with ISO 27001: 2013 is in the domain control areas A5 (Information Security), A11 (Physical and environmental security), and A12 (Operational security).
4. In the area of Information Asset Management, it was found that respondents were 68 (40%) from a maximum score of 168, where 50 scores represented maturity level II, 18 scores represented maturity level III. The Information Asset Management Area is classified into the status level of maturity level I + with a score of 50. Because it has exceeded the minimum maturity level, which is 25, it does not exceed the requirement to reach the minimum value of maturity level II, which is 62. The relationship between the status of the maturity level of the information asset management area with ISO 27001: 2013 there are domain control areas A7 (Human resource security), A8 (Asset Management), A11 (Physical and environmental security), and A12 (operational security).
5. In the area of Information Technology and Security, it was found that respondents were 51 (42%) from a maximum score of 120, obtained from 23 scores representing maturity level II, 28 scores representing maturity level III, 0 scores representing maturity level IV. The area or part of Information Asset Management is classified into the status level of maturity level I + with a score of 23. Because it has exceeded the minimum maturity level, which is 18 but does not exceed the requirements to reach the minimum value of maturity level II, namely 28. The relationship status of the maturity level of the technology area and information security with ISO 27001: 2013 is in the domain control areas A9 (access control) and A12 (operation security).

Conclusion

The conclusions that can be generated from this research on the evaluation of academic information system security using the KAMI Index and ISO 27001: 2013 are:

1. The results of the Electronic Systems category assessment at XYZ University get a score of 10 which means it is in a low category. This indicates that there is still a lack of interest in using electronic systems and low awareness of electronic systems.
2. The level of security and completeness of the application of the ISO 27001: 2013 standard according to the electronic category gets a score of 166, which means it is in the inappropriate category and at the maturity level I to I +. The Risk Management Area, Information Security Framework Area is at maturity level I, while the Governance, Asset Management, and Information Technology and Security areas are at maturity level I +. The cause of the low level of completeness and maturity of information security at the XYZ University Academic Information System has not implemented all security requirements or is still in planning.
3. Evaluation of the five areas of the KAMI Index shows that the Information Security Risk Management area gets the lowest score, 10 out of a total of 72, and is at maturity level I.
4. The results of the evaluation of the five KAMI index areas show a relationship with ISO 27001: 2013 in the domain areas A5, A7, A8, A9, A11, and A12.

Advice is given to researchers who will conduct information system security research using the KAMI index to provide recommendations based on ISO 27001: 2013. Recommendations are given by looking at what deficiencies exist in each area of the KAMI Index and comparing them with ISO 27001: 2013 controls.

Acknowledgments

With humility, the author would like to express his gratitude and appreciation to the Leaders and Academic Community of XYZ University, especially for the Vice-Chancellor II, the Head of BAAK, and the Head of PUSTIK, because for their help this research can be completed. And thank you for your cooperation during the author's research and data collection.

References

[1] D. Riani, *Audit Keamanan Sistem Informasi Akademik (SIAKAD) Universitas Lampung Menggunakan Standar ISO/IEC 27001*. Lampung: Universitas Lampung, 2018.

[2] M. Ikhsan, E. Darwiyanto, and D. D. J. Suwawi, "Audit keamanan sistem informasi akademik Sekolah Tinggi Farmasi Bandung berbasis risiko dengan menggunakan standar ISO 27001," *e-Proceeding Eng.*, vol. 3, no. 3, p. 5222, 2016.

[3] E. R. Pratama, Suprapto, and A. R. Perdanakusuma, "Evaluasi tata kelola sistem keamanan teknologi informasi menggunakan indeks KAMI dan ISO 27001: Studi kasus KOMINFO Provinsi Jawa Timur," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 5911–5920, 2018.

[4] F. A. Basyarahil, "Evaluasi manajemen keamanan informasi menggunakan indeks Keamanan Informasi (KAMI) berdasarkan ISO/IEC 2700:2013 pada Direktorat Pengembangan Teknologi Dan Sistem Informasi (DPTSI) ITS Surabaya," Jurnal Tekniks, vol. 6, no. 1, 2017.

[5] R. Sarno and I. Iffano, *Sistem Manajemen Keamanan Informasi*. Surabaya: ITS Press, 2009.

[6] D. A. Prastiyawan, A. Ambarwati, and E. Setiawan, "Analisis manajemen risiko layanan sistem manajemen dealer menggunakan COBIT 5," *Matrix J. Manaj. Teknol. dan Inform.*, vol. 10, no. 2, pp. 43–49, 2020.

[7] C. Chazar, "Standar manajemen keamanan informasi berbasis ISO/IEC 27001: 2005," *J. Inf.*, vol. VII, no. 2, pp. 48–57, 2015.

[8] D. Fitrianah and Y. G. Sucahyo, "Audit sistem informasi/ teknologi informasi dengan kerangka kerja cobit untuk evaluasi manajemen teknologi informasi di Universitas XYZ," *J. Sist. Inf.*, vol. 4, no. 1, p. 37, 2012.

[9] S. Arikunto, *Dasar-dasar Evaluasi Pendidikan*. Jakarta: PT Bumi Aksara, 2015.

[10] KOMINFO, Panduan Penerapan SMKI Berbasis Indeks KAMI, no. September, 2017. Jakarta: KOMINFO.

[11] Standar Nasional Indonesia and Badan Standardisasi Nasional, "Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan," 2009.

[12] BSN, *Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2005, IDT)*. Jakarta: BSN, 2009.

[13] Mufadhol, "Kerahasiaan dan keutuhan keamanan data dalam menjaga integritas dan keberadaan informasi data," *J. Transform.*, vol. 6, 2009.

[14] N. Arman, W. Hayuhardhika, and A. Rachmadi, "Evaluasi keamanan informasi pada dinas komunikasi dan informatika Kabupaten Sidoarjo menggunakan indeks Keamanan Informasi (KAMI)," *Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 6, pp. 5750–5755, 2019.