Assessment of Information Security Readiness on Crowd funding System using KAMI Index 4.2

Ariqah Adliana Siregar
Department of Information System Universitas Ahmad Dahlan Yogyakarta of Indonesia

Imam Riadi
Department of Information System Universitas Ahmad Dahlan Yogyakarta of Indonesia

ABSTRACT
Technological developments are multiplying. The charity currently has a crowdfunding service. This service helps simplify the user management process. Security is a crucial issue to support and guarantee funders. This study aims to evaluate and provide recommendations for crowdfunding services to run safely and smoothly using the KAMI Index 4.2. This research consists of several steps, starting with observations made at charitable institutions and continued through focus group discussion activities to assess crowdfunding services' level of information security. Based on the assessment results, crowdfunding services at charities obtained a completeness level score of 165 and maturity levels I to I+, which indicates that the charity is still in its initial condition and has not implemented information security standards in managing crowdfunding services. The analysis of the calculation results is used as the basis for developing recommendations. Recommendations proposed to increase the value are carried out by compiling and implementing information security at the charity.

Keywords
Evaluation, Information, KAMI Index, Security, Crowdfunding.

1. INTRODUCTION
Information and Communication Technology development is currently experiencing rapid development[1]. Supported by computer networks, these technological advances allow information to be interwoven easily and quickly by anyone and anywhere. In Indonesia today, many organizations, both private and government, take advantage of the development of information technology[2]. The influence of Information and Communication Technology has made it an essential asset for individuals, the private sector, and the government [3].

Information is a valuable asset for organizations and agencies. This information becomes easy to attack or exploit by irresponsible parties[4]. Based on this, the organization or agency must be aware of information security related to integrity, availability, and confidentiality[5].

In an agency or organization that has utilized technology in business processes, it is necessary to have good governance. Information security is an important aspect and needs to be notice[6], believing that government will directly impact the organization because the government will hampered if a main object experiences problems, threats, damage, disruption, theft, and loss[7]. The National Standardization Agency (BSN) said that in implementing public services, good governance is needed, which discusses transparency, efficiency, accountability, and effectiveness in IT benefits. It is also explained in the Minister of Communication and InformationNumber 4 of 2007, which contains general guidelines for managing national Information and Communication Technology. This indicates that Information Technology Governance is crucial in implementing IT services[8].

One organization that has used information technology is Charity Organization. Charity Organization is a national-level zakat institution responsible for managing zakat funds, waqf, infaq, qurban and philanthropic funds[9]. The establishment of Charity Organization is intended as a zakat management institution with modern management that delivers zakat as part of solving social problems that continue to develop in society[10]. In fulfilling this program, Charity Organization has created an IT-based system to support its business processes, even though some platforms have not run optimally. One of these platforms is fundraising using the crowdfunding method. This method has a positive impact, namely making it easier for a person or organization to search for funds and a negative impact in the form of the vulnerability of the crowdfunding method to cybercrime and still being digitized in Charity Organization, so there are still minimal policies related to information security in the crowdfunding system.

The Minister of Communication and Information issued regulation No. 4 of 2016 related to the Technology Security Management System, explaining that every electronic system operator is required to carry out the security of information in the public interest, public services, and the smooth implementation of national security and defense. As a form of implementation of the applicable law, the Ministry of Communication and Information of the Republic of Indonesia hopes that every organization that uses electronic systems can carry out certifications related to information security. Therefore, it is necessary to carry out an assessment related to how information security is implemented in an organization. Several assessment tools can be used related to information security in educational institutions and public service organizations, for example by using ISO 27001:2013[11], COBIT, a combination of COBIT 4.1[12], ITIL V.3[13], ISO 27001 and KAMI Index.

The KAMI index is a measuring tool designed to assess and evaluate the level of maturity and completeness of implementation following the ISO/IEC 27001:2013 standard and provides an overview of information security governance within an agency or organization[14]. In its development, the KAMI Index continues to develop from the KAMI Index 1.0 until it was developed by the National Cyber and Crypto Agency (BSSN) to 4.2. There are quite striking differences in version 4.0, namely the addition of an evaluation area related to third parties, cloud services, and personal data protection [15]. At the same time, in the KAMI Index 4.2, there are not too many changes, only revisions and editorial additions by the National Cyber and Crypto Agency (BSSN).

Charity organizations are still relatively new to digitalization and must be aware that their Crowdfunding system can create gaps or risks. This crowdfunding system requires policies related to information security and risk management of information security. Furthermore, charity organizations also need a national assessment and standardization of data security information technology in this crowdfunding system to increase visitor confidence in conducting philanthropic activities.

2. LITERATURE STUDIES

Information Security

Information security, according to ISO 27001:2005, is protection related to information from various threats to minimize business risk, ensure business continuity, and maximize return on investment and business opportunities. Then information security, according to ISO 27001:2013, is an information security management system that maintains the integrity, confidentiality, and availability of information, applies risk management processes, and assures interested parties that risks are correctly managed[16]. Information security used in organizations aims to overcome obstacles and problems that arise both technically and non-technically[17].

Figure 1. CIA Triad

Figure 1 is information security with three aspects: confidentiality or confidentiality, integrity or integrity, and availability or availability. Confidentiality is an aspect that ensures that information and data owned by the company can be accessed only by authorized parties. Integrity or integrity as an aspect to maintain accuracy, ensure that the data held is not modified without the permission of the authorities, and the integrity of the information. Availability or availability as an aspect that guarantees the availability of information and data can be used by the rules when needed, whenever, and wherever [18].

Information Security Management System (SMKI)

An organization or agency requires an information security management system as a target to achieve the goals of the organization or agency by establishing, using, implementing, reviewing, maintaining, improving information security and minimizing risk, as well as ensuring the business continuity of an organization or agency proactively to limit the impact that will arise from security breaches [19]. The Information Security Management System (SMKI) must meet national and international standards that have been developed since 2005 by the International Organization for Standardization (ISO) so that the quality of the security provided can solve existing problems. The application of a process system within an agency, together with an analysis of the identification of each process and management, is referred to as the "process approach." In the ISMS, the process approach is presented following the ISMS standard, based on operating principles adopted from the ISO management system standard, commonly referred to as the Plan-Do-Check-Act (PDCA) process [20]. The following explains the Plan-Do-Check-Act process:

- Plan, in this process, will analyze, set overall goals and targets, also develop plans to achieve them.
- Do, in this process, will implement or carry out the plan that has been planned.
- Check, in this process, will monitor and measure the achievement in meeting the planned goals.
- Act, in this process, will improve activities that have not been following the plan, learn from previous mistakes, and improve activities to achieve better results.

Information Technology Risk

Risk is a process of activities carried out to determine opportunities for attacks or threats that can cause disruption of business processes and even failure of the goals of the agency or organization 16. Risk management is the process of achieving a balance of efficiency and realizing opportunities to gain profits and reduce losses and vulnerabilities[21]. An organization or agency thinks about data or information that is important and is a resource that can increase the value or image of the organization or institution. With this data and information, organizations or agencies need information security. Information security aims to minimize risk, guarantee business processes, and protect data from various dangerous threats such as data theft, viruses, and other attacks.

ISO/IEC 27001 as an ISMS Standard

ISO/IEC 27001 is a recommended international standard document for implementing an Information Security Management System (ISMS). ISO 27001 is a standard intended to assist organizations or agencies in maintaining and protecting the Information Security Management System (ISMS) and the security of company assets. ISO/IEC 27001 is a framework designed to apply to small and large-scale organizations or agencies that specify the need to create, implement, implement, monitor, analyze, and improve management regularly and maintain and document a Management System. Information Security (SMKI) [22].

Information Security Index Version 4.2 as an ISMS tool sequent Pages

The KAMI index is a tool or evaluation tool compiled by the Directorate of Information Security Team of the Ministry of Communication and Information Technology[23], which is used to analyze, measure, and evaluate the level of readiness for the application of information security in government agencies whose contents have been adjusted to the criteria in SNI ISO/IEC 27001[24]. not intended to analyze the feasibility or effectiveness of existing forms of security, but only as a tool to provide an overview of the condition of readiness, completeness, and maturity as well as the information security framework in the environment for organizational/agency leaders[25].

Organizations or agencies can use the KAMI index on a national scale and a small scale. The evaluation of the KAMI Index is recommended to be carried out by staff or officials with the responsibility and authority to manage information security within the organization or agency. The things it will evaluate in the KAMI Index focus on five areas: Electronic

Systems, Governance, Risk Management, Asset Management, Technology, and Information Security.

Before the quantitative assessment process, the initial stage is to classify the Electronic Systems used by agencies or organizations to organize the Electronic Systems used into certain "levels" or "sizes." The results obtained mean the dependence of an organization or agency on the role of Electronic Systems. Figure 2 shows the final score that will be adjusted to the readiness status of the agency or organization for information security.

Elelctronic System Categori				
Low		Final Score		Readiiness Status
10	15	0	174	Not Feasible
		175	312	Fulfillment of the basic framework
		313	535	Pretty good
		536	645	Good
High		Final Score		Readiiness Status
16	34	0	272	Not Feasible
		273	455	Fulfillment of the basic framework
		456	583	Pretty good
		584	645	Good
Strategic		Final Score		Readiiness Status
35	50	0	333	Not Feasible
		334	535	Fulfillment of the basic framework
		536	609	Pretty good
		610	645	Good

Figure 2. SE Category Matrix with KAMI index readiness status

Each category has questions based on the readiness to implement and secure information security following the ISO/IEC 27001:2013 standard. The grouping is explained as follows:

- The label "1" forms the basic framework for information security.
- The label "2" represents the consistency and effectiveness of implementing information security.
- The label "3" is a form of ability to improve information security performance which is adjusted to the minimum prerequisite readiness standard for ISO/IEC 27001:2013 certification.

This method's rating weights differ according to the completeness control label. Figure 3 is the score for each category.

	Security Status		
Security Status	1	2	3
Not done	0	0	0
In planing	1	2	3
In progress	2	4	9
Fully applied	3	6	6

Figure 3. The score value of control completeness label

Questions are categorized by maturity level, and applicability refers to the maturity level used by COBIT or CMMI. The maturity level is described as follows:

- Level I - Initial Condition
- Level II - Implementation of the Basic Framework
- Level III - Defined and Consistent
- Level IV - Managed and Scalable
- Level V – Optimal

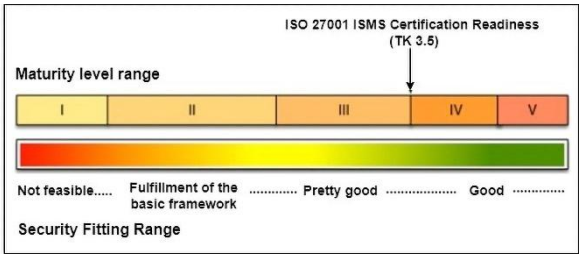

Figure 4. Maturity level and completeness of security

The KAMI index makes it easy by providing detailed descriptions with the addition of I+, II+, III+, and IV+ details. The minimum standard in readiness for certification in ISO/IEC 27001:2013 is at level III+. The following is Figure 4 regarding the status of completeness of security (bottom) and level of maturity of experience (top).

3. METHODOLOGY

In this research, there are several activities to complete this research. Figure 5 is the flow of activities carried out in this study.

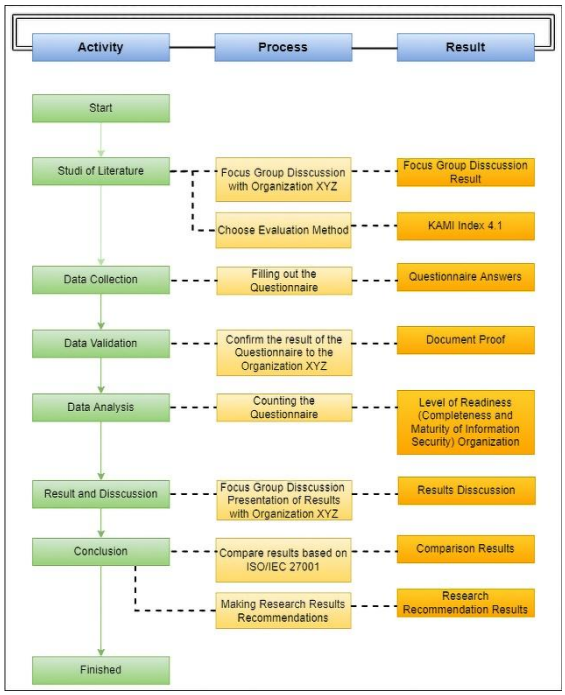

Figure 5. Research Methodology

Study of Literature

This literature study stage identified problems through focus group discussions with charities. This focus group discussion is more directed at stakeholders and IT staff at charities. After carrying out the discussion activities, several problems were found, such as some platforms not running well and still in development. In the crowdfunding system studied, information security has never been evaluated.

Data Collection

The data collection stage was carried out by filling out a questionnaire owned by the KAMI Index 4.2. This questionnaire was filled out through FGDs and filled in by stakeholders and IT staff at charitable institutions.

Data Validation

The data validation stage is carried out by re-confirming the answers that have been carried out in the previous step. The inspection is carried out with stakeholders and IT staff. At this stage, checking and related document reports are also carried out.

Data Analysis

The data analysis stage is carried out after the data is completely valid. The researcher will process the data in the form of a questionnaire with the formula in the KAMI Index 4.2.

Data Analysis

The data analysis stage is carried out after the data is completely valid. The researcher will process the data in the form of a questionnaire with the formula in the KAMI Index 4.2.

Results and Disscussion

The presentation of the results is the last stage in the research flow. At this stage the researcher has obtained, confirmed, processed, analyzed, and made recommendations following the results. Then the researcher will present the results and recommendations to the charitable institutions.

4. RESULT

Research on the maturity level of information security in the crowdfunding system of charitable institutions uses the KAMI Index evaluation tool version 4.2. The KAMI index has 194 questions divided into seven sections. A series of studies have been carried out, and the evaluation results are showed in Figure 6.

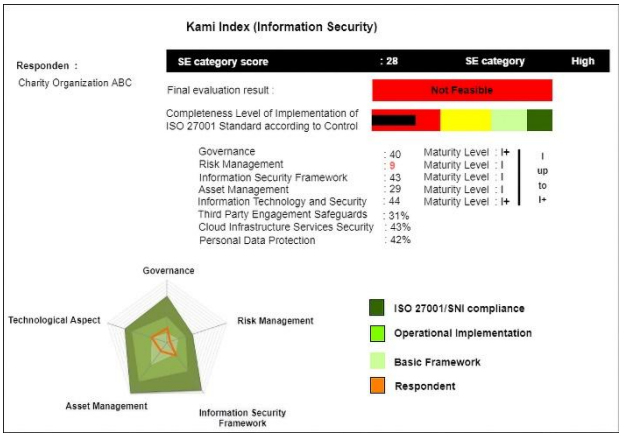

Figure 6. Evaluation results dashboard

In the radar diagram in Figure 6, the chart that forms the orange line pattern represents the condition of the SMKI in charity institutions based on the results of filling out questionnaires by the informants.

Electronic System Category

The Governance category is the second category in the KAMI Index that evaluates the level of governance in the system used. The Governance category is divided into 3 Control Categories with the label "1" having eight questions, the title "2" having eight questions, and the brand "3" having six questions. The maturity level assessment on the "3" label only gives results if all inquiries related to the "1" and "2" brands are filled with at least "Partially Applied." The Information Security Governance assessment in the crowdfunding system at charity received a total Information Security Governance evaluation score of 40 out of 22 questions with a maturity level status of I+. The minimum threshold for certification readiness for the expected maturity level is Level III+. Still, the information security governance results obtained are only valid at the I+ maturity level, which means they are in the initial condition.

Table 1. Electronic System Category Score

Electronic System Category Score	
Low	10-15
High	16-34
Strategic	35-50

Based on table 1, Information security management in the crowdfunding system, there is a reasonably large understanding of information security within the agency, documenting every task and responsibility for managing information security and maintaining compliance and has not defined a policy of criminal action against information security incidents.

Categories of Information Security Governance

The Governance category is the second category in the KAMI Index that evaluates the level of governance in the system used. The Governance category is divided into 3 Control Categories with the label "1" having eight questions, the brand "2" having eight questions, and the brand "3" having six questions. The maturity level assessment on the "3" label only gives results if all inquiries related to the "1" and "2" brands are filled with at least "Partially Applied." Table 2 is an assessment of Information Security Governance in charity's crowdfunding system. The minimum threshold for certification readiness for the expected maturity level is Level III+. Still, table 3 shows the results of the information security governance maturity level obtained that are only valid at the I+ maturity level, which means they are in the initial condition level.

Table 2. Level of Completeness Category Information Security Governance

Security Status	Maturity level						Total
	1	SK	2	SK	3	SK	
Are not done	0	0	0	0	0	2	0
In planning	1	2	2	3	3	3	8
In the application or partially applied	2	5	4	4	6	1	26
Thoroughly applied	3	0	6	1	9	0	6
Total score							**40**

Table.3Maturity Level of InformationInformation Security Governance

Control Category	Question	Score	Maturity Validation Level
II	13	17	I+
III	3	6	No
IV	6	0	No
Total	22	23	

Information security management in the crowdfunding system has a reasonably large understanding of information security within the agency, documents every task and responsibility

for managing information security and maintaining compliance, and has not defined a policy of criminal action against information security incidents..

Information Security Risk Management Category

The Risk Management category is the third category in the KAMI Index that evaluates the level of risk in the system used. The Risk category is divided into 3 Control Categories with the label "1" having ten questions, the brand "2" having four questions, and the brand "3" having two questions. . The assessment of the level of completeness on the "3" label only gives results if all inquiries related to the "1" and "2" brands are filled with at least "Partially Applied." Table 4 is an assessment of Information Security Risk that exists in the crowdfunding system at charities. The total value of the Information Security Risk evaluation is 9 out of 16 questions with maturity level I. Based on table 5 the management of Information Security Risk in the crowdfunding system is valid at maturity level I, which means in initial conditions. In this system, there is an understanding of the need for information security management, which needs improvement.

Table 4. Information Security Risk Category Completeness Level

Security Status	Maturity level						Total
	1	SK	2	SK	3	SK	
Are not done	0	2	0	4	0	0	0
In planning	1	7	2	0	3	0	7
In application or partially applied	2	1	4	0	6	0	2
Thoroughly applied	3	0	6	0	9	0	0
Total score							**9**

Table 5. Maturity Level of Information Security Risk Category

Control Category	Question	Score	Maturity Validation Level
II	10	8	No
III	2	0	No
IV	2	0	No
V	2	0	No
Total	16	8	

Information security risks in the crowdfunding system need to identify threats and weaknesses related to information assets, develop risk mitigation and mitigation measures, carry out periodic risk mitigation checks, and conduct regular assessments of the risk management framework to ensure/improve its effectiveness..

Categories of Information Security Management Framework

The framework category is the fourth category in the KAMI Index that evaluates the framework of the system used. The Framework category is divided into 3 Control Categories with the label "1" having 12 questions, the brand "2" having ten questions, and the brand "3" having seven questions. The assessment of the level of completeness on the "3" label only gives results if all inquiries related to the "1" and "2" brands are filled with at least "Partially Applied." Table 6 is the result of an assessment of the Information Framework that exists in the crowdfunding system at charities getting a total evaluation score of 43 out of 29 questions with maturity level I. Table 7 is the result of the maturity level of the Information Management Framework Area at maturity level I, which means it is in the beginning.

Table 6. Level of Completeness Category Information Security Framework

Security Status	Maturity Level						Total
	1	SK	2	SK	3	SK	
Are not done	0	3	0	4	0	2	0
In planning	1	4	2	0	3	2	4
In application or partially applied	2	2	4	2	6	1	12
Thoroughly applied	3	1	6	4	9	2	27
Total score							**43**

Table 7. Maturity Level Information Security framework categories

Control Category	Question	Score	Maturity Validation Level
II	11	8	No
III	13	11	No
IV	3	0	No
V	2	0	No
Total	29	19	

The information security framework in the crowdfunding system needs to define a secure system development policy, and it is necessary to control information system audits, verify reviews, and evaluate the continuity of information security

Categories of Information Asset Management

The Asset Management category is the fifth category in the KAMI Index that evaluates asset management on the system used. The Asset Management category is divided into 3 Control Categories with the label "1" having 24 questions, the brand "2" having ten questions, and the brand "3" having four questions. The assessment of the level of completeness on the "3" label only gives results if all inquiries related to the "1" and "2" brands are filled with at least "Partially Applied." Table 8 is the result of the assessment of Information Asset Management in the crowdfunding system at charities. The evaluation value is 29 out of 38 questions with maturity level I. Table 9 results of Information Asset management are valid at maturity level I, which means in initial conditions.

Table 8. Completeness Level of Information Security Asset Category

Security Status	Maturity Level						Total
	1	SK	2	SK	3	SK	
Are not done	0	13	0	7	0	3	0
In planning	1	3	2	1	3	1	5
In application or partially applied	2	8	4	2	6	0	24
Thoroughly applied	3	0	6	0	9	0	0
Total score							**29**

Table 9. Maturity Level of Information Asset Management Category

Control Category	Question	Score	Maturity Validation Level
II	29	13	No
III	9	4	No
Total	38	17	

Management of Information Security Assets in a crowdfunding system needs to protect all assets (offices, rooms, and facilities) from external environmental threats and ensure the procedures for intellectual property rights and access security are used.

Information Technology and Security Category

The Information Security Technology category is the sixth category in the KAMI Index that evaluates the technology in the system used. The Information Technology and Security category is divided into 3 Control Categories with the division of the label "1" there are 14 questions, the brand "2" has ten questions, and the brand "3" has two questions. The level of completeness assessment on the label "3" only gives results if all questions are related labels "1" and "2" are filled with at least "Partially Applied." Table XX is the result of assessing the Management of Information Technology and Security in the crowdfunding system at charities. The total value of the Information Technology and Security evaluation is 44 out of 26 questions with a maturity level status of I+. Table xx Information Technology and Security area are valid at maturity level I+ which means it is in the initial condition.

Table 10. Completeness Level of Information Security Technology Category

Security Status	Maturity Level						Total
	1	SK	2	SK	3	SK	
Are not done	0	5	0	4	0	2	0
In planning	1	1	2	1	3	0	3
In application or partially applied	2	7	4	3	6	0	26
Thoroughly applied	3	1	6	2	9	0	15
Total score							**44**

Table 11. Maturity Level of Information Technology and Security Category

Control Category	Question	Score	Maturity Validation Level
II	14	9	I+
III	11	12	No
IV	1	0	No
Total	26	21	

Information security technology in the crowdfunding system needs to carry out double protection on every system owned and control of malware and networks is needed to protect against the possibility of information vulnerabilities.

Supplement Category

The Supplement category is the seventh or final category on the KAMI Index. The evaluation results at the supplement stage showed that the maturity level for securing third-party involvement was 31%. Then for the security of cloud infrastructure services by 43%, and the last is personal data protection by 42%. The score obtained from the calculation of this supplement category does not affect the total score from part I to part VI in the KAMI Index assessment, which indicates the level of readiness and maturity of information security. Based on the KAMI index, the review of this supplement category aims to detect the emergence of new information security risks with the involvement of these three aspects.

5. CONCLUSION

The results of the assessment of the level of use of the Electronic System are 32 out of a total of 50. This shows that the crowdfunding system has entered the high category. The maturity level is at level I-I+. The minimum limit for ISO 27001 certification is III+. The story of completeness got a score of 165 which means that it is still in its initial condition. The focus of the following analysis should be to assess the organization's information security using other frameworks to generate data to support enterprise information security.

6. REFERENCES

[1] M. Yunella, A. D. Herlambang, and W. H. N. Putra, "Evaluation of Information Security Governance at the Malang City Communication and Information Office Using KAMI Index," *... Teknol. Inf. dan ...*, vol. 3, no. 10, pp. 9552–9559, 2020, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/6521.

[2] A. F. Manullang, C. Candiwan, and L. D. Harsono, "Information Security Assessment Using the Information Security Index (KAMI) at XYZ Institution," *Journal of Information Engineering and Educational Technology*, vol. 1, no. 2. p. 73, 2017, doi: 10.26740/jieet.v1n2.p73-82.

[3] M. R. Slamet, F. Wulandari, and D. Amalia, "Assessment of Technology Security in Electronic Learning Systems Using the Information Security Index at Batam State Polytechnic," *J. Appl. Bus. Adm.*, vol. 3, no. 1, pp. 162–171, 2019, doi: 10.30871/jaba.v3i1.1305.

[4] T. Informatika, U. Sam, R. Manado, J. Kampus, and U. Bahu, "Implementation of KAMI Index At Sam Ratulangi University," *J. Tek. Inform.*, vol. 12, no. 1, 2017, doi: 10.35793/jti.12.1.2017.17869.

[5] F. H. Purwanto and M. Huda, "Measurement of XYZ College Information Security Level Using Information Security Index (KAMI) Based on ISO/IEC-27001:2013," *J. VOI (Voice Informatics)*, no. 4, pp. 31–40, 2019, [Online]. Available: https://voi.stmik-tasikmalaya.ac.id/index.php/voi/article/view/162.

[6] J. Tukad and B. No, "Information Technology Security Level Assessment Using Information Security Methods (WE) And Vulnerability Assessment," *Jutisi J. Ilm. Tek. Inform. dan Sist. Inf.*, vol. 9, pp. 173–184, 2020.

[7] T. E. WIJATMOKO, "Evaluation of Information Security Using the Information Security Index (KAMI) at the Regional Office of the Ministry of Law and Human Rights Diy," *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 1, pp. 1–6, 2020, doi: 10.14421/csecurity.2020.3.1.1951.

[8] A. R. Riswaya, A. Sasongko, and A. Maulana, "Evaluation of Information Technology Security Governance Using KAMI Index for Preparation of Sni Iso/Iec 27001 Standard (Case Study: Stmik Mardira Indonesia)," *J. Comput. Bisnis, Vol. 14, No. 1, Juni 2020, 10-18 ISSN 1978-9629, ISSN 2442-4943*, vol. 14, no. 1, pp. 10–18, 2020.

[9] M. Ifas, "Analysis of Publications and Financial Statements Lazismu Based on PSAK No. 45 (Case Study of Lazismu Menteng, Central Jakarta)," *J. Ekon. Islam*, vol. 9, no. November 2018, pp. 46–74, 2018.

[10] R. A. Izdihar and T. Widiastuti, "The Role of the Surabaya Muhammadiyah Amil Zakat Institution (Lazismu) in Empowering Women MSMEs in Surabaya through the Utilization of Infaq and Shadaqah Funds," *J. Ekon. Syariah Teor. dan Terap.*, vol. 6, no. 3, p. 525, 2020, doi: 10.20473/vol6iss20193pp525-540.

[11] H. Hambali and P. Musa, "Analysis of Governance Security Management Information System Using Index Kami in Central Government Institution," *Angkasa J. Ilm. Bid. Teknol.*, vol. 12, no. 1, 2020, doi: 10.28989/angkasa.v12i1.563.

[12] D. Ariyadi, H. Kusbandono, and I. P. Astuti, "Recommended IT Infrastructure Improvements in Vocational Schools Based on Maturity Level Evaluation with the Cobit 4.1 Framework,"*J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 3, no. 1, p. 80, 2019, doi: 10.30645/j-sakti.v3i1.90.

[13] R. D. Pribadi, Y. Herry, A. I. Hadiana, and W. Witanti, "Measuring the Maturity Level of Information Technology Based on Itil V.3 at Jenderal Achmad Yani University,"*J. Ilm. Teknol. Inf. Terap.*, vol. IV, no. 1, pp. 11–17, 2017.

[14] E. R. Pratama, Suprapto, and A. R. Perdanakusuma, "Evaluation of Information Technology Security System Governance Using the KAMI Index and ISO 27001: A Case Study of KOMINFO East Java Province,"*J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 5911–5920, 2018, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/3465.

[15] N. Luh, P. Ning, and S. Putri, "E-Government Information Security Assessment Using the Information Security Index (Us) 4 . 0,"*J. Teknol. Inf. dan Komput.*, vol. 6, no. 2, pp. 238–244, 2020.

[16] Y. C. Yuze, Y. Priyadi, and . C.,"Analysis of Information Security Management Systems Using ISO/IEC 27001: 2013 and Recommendations for System Models Using Data Flow Diagrams at the Directorate of Higher Education Information Systems,"*J. Sist. Inf. Bisnis*, vol. 6, no. 1, p. 38, 2016, doi: 10.21456/vol6iss1pp38-45.

[17] R. Umar, I. Riadi, and E. Handoyo, "Information System Security Analysis Based on COBIT 5 Framework Using Capability Maturity Model Integration (CMMI),"*J. Sist. Inf. Bisnis*, vol. 9, no. 1, p. 47, 2019, doi: 10.21456/vol9iss1pp47-54.

[18] N. A. Widodo and and A. F. R. , R. Rizal Isnanto, "Planning and Implementation of Information Security Management System Based on Iso/Iec 27001:2005 Standard (Case Study in a National Private Bank)," vol. 4, no. 1, pp. 60–66, 2016.

[19] A. C. D. Tinungki, S. R. Sentinuwo, and S. Karouw, "Analysis of the Maturity Level of Information Security Application of the Bitung City Government Using the KAMI Index (Case Study: Office of Communication and Informatics ..."*Repo.Unsrat.Ac.Id*, pp. 1–8, 2021, [Online]. Available: http://repo.unsrat.ac.id/2963/.

[20] W. Apriandari and A. Sasongko, "Analysis of Information Security Management Systems Using Sni Iso / Iec 27001: 2013 in the Regional Government of Sukabumi City (Case Study: At Diskominfo Sukabumi City)," *Ilm. SANTIKA*, vol. 8, no. 1, pp. 715–729, 2018.

[21] N. Matondang, I. N. Isnainiyah, and A. Muliawatic, "Information System Data Security Risk Management Analysis (Case Study: XYZ Hospital),"*J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 2, no. 1, pp. 282–287, 2018, doi: 10.29207/resti.v2i1.96.

[22] W. C. Pamungkas and F. T. Saputra, "Evaluation of Information Security at SMA N 1 Sentolo Based on the Information Security Index (KAMI) ISO/IEC 27001:2013,"*J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 101, 2020, doi: 10.30865/json.v1i2.1924.

[23] M. I. Rosadi and L. Hakim, "Measurement and Evaluation of Yudharta University SIAKAD Security Using the KAMI Index,"*Explor. IT J. Keilmuan Apl. Tek. Inform. Univ. Yudharta Pasuruan*, vol. 7, no. 1, pp. 33–42, 2015.

[24] A. S. Anas, I. G. A. S. D. G. Utami, A. B. Maulachela, and A. Juliansyah, "KAMI index as an evaluation of academic information system security at XYZ university," *Matrix J. Manaj. Teknol. dan Inform.*, vol. 11, no. 2, pp. 55–62, 2021, doi: 10.31940/matrix.v11i2.2447.

[25] I. P. N. Hartawan and M. Sudarma, "ISMS Evaluation Using KAMI Index v.4 Based on ISO/IEC 27001:2013 (Case Study: Koperasi XYZ)," vol. 6, no. 2, pp. 4–7, 2021.