Security on Charity Crowdfunding Services using KAMI Index 4.1

Manuscript received June 28, 2022; revised July 30, 2022

Tawar*
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
tawar@is.uad.ac.id

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
imam.riadi@is.uad.ac.id

Ariqah Adliana Siregar
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
ariqah1800016036@webmail.uad.ac.id

Adiniah Gustika Pratiwi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
adiniah1800016038@webmail.uad.ac.id

***Abstract*—Technological developments are multiplying. The ABC 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 research aims to evaluate and provide recommendations for crowdfunding services to run safely and smoothly using the KAMI Index 4.1. This research consists of several steps, starting with observations made at charitable institutions. The following process is through focus group discussion activities to assess the level of information security of crowdfunding services. The analysis of the calculation results is used as the basis for developing recommendations. Based on the assessment results, crowdfunding services at charities obtained scores of I to I+, this indicates that the charity is still in its initial condition and has not yet implemented information security standards in managing crowdfunding services. Recommendations proposed to increase the value are carried out by compiling and implementing information security at the charity.**

***Index Terms*—assessment, information, KAMI index, security, crowdfunding**

I. Introduction

Information and Communication Technology (ICT) 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 Information (KOMINFO) Number 41 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 ABC. Charity Organization ABC is a national-level zakat institution responsible for managing zakat funds, waqf, infaq, qurban and philanthropic funds [9]. The establishment of Charity Organization ABC is intended as a zakat management institution with modern management that delivers zakat as part of solving social problems (problem solvers) that continue to develop in society [10]. In fulfilling this program, Charity Organization ABC 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 ABC, so there are still minimal policies related to information security in the crowdfunding system.

The Minister of Communication and Information (KOMINFO) 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 [11]. 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

EISSN: 2961-872X ● PISSN: 2961-8924 ● DOI: 10.56741/esl.v1i01.61

using ISO 27001:2013 [12], COBIT, a combination of COBIT 4.1 [13], ITIL V.3 [14], ISO 27001 [15] 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 [16]. 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 4.1. 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 [17]. At the same time, in the KAMI Index 4.1, there are not too many changes, only revisions and editorial additions by the National Cyber and Crypto Agency (BSSN).

II. RELATED WORKS

A. *Information Security Information*

According to ISO 27001:2005, information security 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 in it, applies risk management processes, and assures interested parties that risks are correctly managed [18].

Information security is applied in organizations to overcome obstacles and problems that arise both technically and non- technically [19]. Information securityhas three aspects: confidentiality, integrity, and availability. Confidentiality is an aspect that ensures that information and data owned by the company can be accessed only by authorized parties. Integrity, an element to maintain accuracy, guarantees that the data held is not modified without the permission of the authorities and the integrity of the information. Integrity as an aspect to maintain accuracy, ensure that the data owned is not modified without the authorities' permission and the integrity of the data [20].

B. *Information Security Management System (ISMS)*

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 a security breach [21]. 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 and an identification analysis are each process and management are 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 [22]. The following explains the Plan-Do- Check-Act process:

Plan, n 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 planned plan.

Check, this process will monitor and measure the extent to which the achievement has met the planned goals.

Act, this process will improve activities that have not been following the plan, learn from previous mistakes, and enhance activities to achieve better results.

C. *Information Technology Risk Management 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 fail the goals of the agency or organization [23]. Risk management is the process of striking a balance between efficiency and realizing opportunities to gain profits and reduce losses and vulnerabilities [24].

An organization or agency has 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, protect data from various dangerous threats such as data theft, viruses, and other attacks.

D. *ISO/IEC 27001 as an ISMS Standard*

ISO/IEC 27001 is an international standard document recommended 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 in such a way that it can apply to small and large-scale organizations or agencies that are used to specify the need to create, implement, implement, monitor, analyze, improve management regularly and maintain and document a Management System Information Security (SMKI) [25].

E. *Information Security Index version 4.1 as an ISMS tool*

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, 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. The KAMI index is 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 and an information security framework in the environment for organizational leaders or agencies.

Organizations or agencies can use the KAMI index on a national and small scale. The evaluation of the KAMI Index is recommended to be carried out by staff or officials who have the responsibility and authority to manage information security within the organization or agency. In the KAMI Index, the items to be evaluated focus on five areas, namely Electronic Systems, Governance, Risk Management, Asset Management, Technology and Information Security [26].

Before the quantitative assessment process, the initial stage is to carry out a classification process for the Electronic System used by the agency or organization to classify the Electronic System used into a certain "level" or "size." The results obtained mean the dependence of an organization or agency on the role of Electronic Systems. Each category has questions based on readiness to implement and secure information security following the ISO/IEC 27001:2013 standard. Table 1 is the score for each level.

TABLE I.
MATURITY SCORE

	Maturity Score		
Security Status	Level 1	Level 2	Level 3
Not done	0	0	0
In planning	1	2	3
In progress	2	4	6
Fully applied	3	6	9

III. RESEARCH METHOD

This research assesses the level of information security in an organization using KAMI Index 4.1 method. Figure 1 describes the research flow.

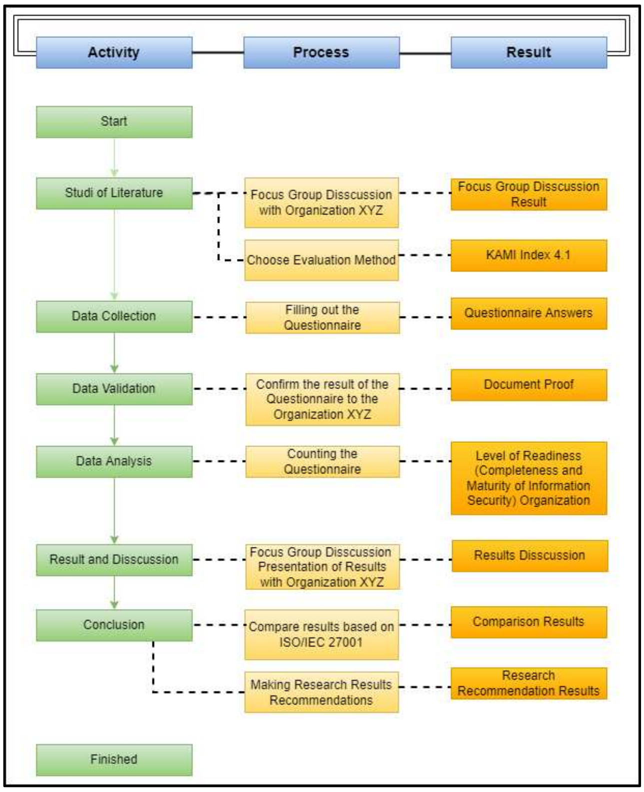
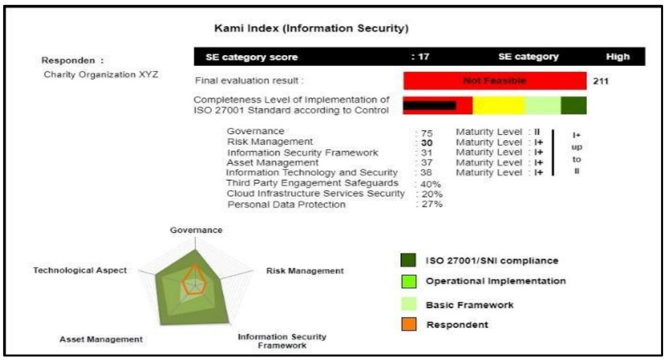

Activity
Process
Result
Start
Studi of Literature
Focus Group Disscussion with Organization XYZ
Focus Group Disscussion Result
Choose Evaluation Method
KAMI Index 4.1
Data Collection
Filling out the Questionnaire
Questionnaire Answers
Data Validation
Confirm the result of the Questionnaire to the Organization XYZ
Document Proof
Data Analysis
Counting the Questionnaire
Level of Readiness (Completeness and Maturity of Information Security) Organization
Result and Disscussion
Focus Group Disscussion Presentation of Results with Organization XYZ
Results Disscussion
Conclusion
Compare results based on ISO/IEC 27001
Comparison Results
Making Research Results Recommendations
Research Recommendation Results
Finished

Fig. 1. Research Stages of KAMI Index.

IV. RESULT AND DISCUSSION

Research the maturity level of information security on the Charity Organization ABC crowdfunding system using the KAMI Index evaluation tool 4.1. The KAMI index has 194 questions divided into seven sections. A series of studies have been carried out, and the evaluation results are shown in Figure 2. In the radar diagram, the orange line pattern is the condition of the SMKI in Charity Organization ABC based on the results of filling out the questionnaire by the informants.


Kami Index (Information Security)

Responden :
Charity Organization XYZ

SE category score : 17 SE category High

Final evaluation result : Not Feasible 211

Completeness Level of Implementation of ISO 27001 Standard according to Control

Governance	: 75	Maturity Level : II	I+ up to II
Risk Management	: 30	Maturity Level : I+	
Information Security Framework	: 31	Maturity Level : I+	
Asset Management	: 37	Maturity Level : I+	
Information Technology and Security	: 38	Maturity Level : I+	
Third Party Engagement Safeguards	: 40%		
Cloud Infrastructure Services Security	: 20%		
Personal Data Protection	: 27%		

Fig. 2. Evaluation Results Dashboard.

The Electronic System category is the first category in the KAMI Index that evaluates the electronic system level used. In the category of electronic systems, there are three categories of results, namely low, high and strategic. The electronic system category has ten questions with a maximum score of 50. The results obtained in the Electronic System category based on the WE Index assessment obtained a score of 28, so that will can include it in the high category according to the maturity level table of the KAMI Index where the High category ranges from a score of 16 to 34, as an assessment guide can be seen in Table 2.

TABLE II.
ELECTRONIC SYSTEM CATEGORY SCORE

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

It needs to be improved. Based on table 3, 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, conduct regular assessments of the risk management framework to ensure/improve its effectiveness. Table 3. evaluation results for all categories.

TABLE III.
TABLE TYPE STYLES

Security Status	Maturity level						Total
	1	SC	2	SC	3	SC	
Governance Category							
Not done	0	2	0	4	0	0	0
In planning	1	7	2	0	3	0	7
In progress	2	1	4	0	6	0	2
Fully applied	3	0	6	0	9	0	0
Total score							9
Framework Category							
Not done	0	0	0	0	0	2	0
In planning	1	2	2	3	3	3	8
In progress	2	5	4	4	6	1	26
Fully applied	3	0	6	1	9	0	6
Total score							40
Asset Management Category							
Not done	0	3	0	4	0	2	0
In planning	1	4	2	0	3	2	4
In progress	2	2	4	2	6	1	12
Fully applied	3	1	6	4	9	2	27
Total score							43

Security Status	Maturity level 1	SC	2	SC	3	SC	Total
Information Technology and Security Category							
Not done	0	13	0	7	0	3	0
In planning	1	3	2	1	3	1	5
In progress	2	8	4	2	6	0	24
Fully Applied	3	0	6	0	9	0	0
Total score							29
Supplement Category							
Not done	0	5	0	4	0	2	0
In planning	1	1	2	1	3	0	3
In progress	2	7	4	3	6	0	26
Fully Applied	3	1	6	2	9	0	15
Total score							44

The Governance category is to evaluate the level of governance in the system used. The Information Security Governance assessment in the crowdfunding system at Charity Organization ABC 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 maturity level I+, which means they are in the initial condition level. Based on table 2, 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.

The Risk Management category is to evaluate the level of risk in the system used. Information Security Risk Assessment in the crowdfunding system at Charity Organization ABC obtained a total Information Security Risk evaluation score of 9 out of 16 questions with maturity level I. Information Security Risk Management in the crowdfunding system is valid at maturity level I, which means it is initial. This system already understands the need for information security management. The framework category is to evaluate the framework on the system used. Assessment of the Information Management Framework in the crowd funding system at Charity Organization ABC received a total evaluation score of 43 out of 29 questions with maturity level I status. The Information Management Framework area is at maturity level I, which means it is in the initial condition. Based on table 4, the information security framework on the crowdfunding system needs to determine a secure system development policy it is necessary to control information system audits and verify review and evaluate the continuity of information security.

The Asset Management category is to evaluate asset management on the system used. The Management of Information Assets assessment in the crowd funding system at Charity Organization ABC obtained a total evaluation value of 29 out of 38 questions with maturity level status I. In the area of Information Asset Management, it is valid at maturity level I, which means it is in the initial condition. Based on table 5, Information Security Asset Management in the crowdfunding system needs to protect all assets (offices, rooms, and facilities) from external environmental threats, ensure the procedures for intellectual property rights and access security used.

The Information Security Technology category is to evaluate the technology in the system used. The assessment of Information Security and Technology Management in the crowdfunding system at Charity Organization ABC obtained a total value of the Information Technology and Security evaluation of 44 out of 26 questions with a maturity level status of I+. In the area of Technology and Information Security, it is valid at maturity level I, which means it is in the initial condition. Based on table 6, information security technology in the crowdfunding system needs to control malware and networks.

The Supplement Category is the last category on the KAMI Index. The results of the evaluation at the supplement stage obtained 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 US Index assessment, which indicates the level of readiness and maturity of information security. Based on the KAMI index, the assessment of this supplement category aims to detect the emergence of new information security risks with the involvement of these three aspects.

V. Conclusion

The assessment results of the level of use of Electronic Systems are 32 out of a total of 50. This shows that the crowdfunding system has entered the high category in electronic systems, which means that electronic systems are an inseparable part of the work process running on Charity organizations. The order of maturity levels from the lowest to the highest is I – V. The minimum limit to carry out ISO 27001 certification is III+. For now, the maturity level of the Crowdfunding System at Charity Organization Pusat is only limited to I to I+, and the security level of the information system is at the Initial Condition level.The recommended National Cyber and Crypto Agency (BSSN) research is carried out twice a year. The focus of the following analysis should be able to assess organizational information security using other frameworks to produce data to support corporate information security.

Acknowledgment

Thank you to Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Ahmad Dahlan who have provided funding for this research activity through Skema Penelitian Unggulan Program Studi (PUPS) in 2021 based on contract number PUPS-278/SP3/LPPM-UAD/VI/2021.

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] A. Kornelia and D. Irawan, D. "Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1," *Jurnal Pengembangan Sistem Informasi dan Informatika*, vol. 2, no. 2, pp.78-86, 2021.

[5] F. H. Purwanto and M. Huda, "Measurement of XYZ College InformationSecurity 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 AssessmentUsing 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 (US) at the Regional Office of the Ministry ofLaw 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] R. Riswaya, A. Sasongko, and A. Maulana, "Evaluation of InformationTechnology Security Governance Using Our Index for Preparation of Standard SNI Iso/Iec 27001 (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, "Publication Analysis And Financial Statements Based On Psak No. 45 (Case Study Of Lazismu Menteng Jakarta Pusat)," *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] S. I. D. Octaviani, Suprapto, and A. D. Herlambang, "Evaluation of the Readiness of the Information Security Framework at the Batu City Communications and Information Office Using KAMI Index," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 3, pp. 2741–2745, 2019.

[12] 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.

[13] D. Ariyadi, H. Kusbandono, and I. P. Astuti, "Recommendations for IT Infrastructure Improvement in Vocational High Schools Based on Maturity Level Evaluation with 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.

[14] R. D. Pribadi, Y. Herry, A. I. Hadiana, and W. Witanti, "Measurement of 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.

[15] A. Fathurohman and R. W. Witjaksono, "Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City)," *Bull. Comput. Sci. Electr. Eng.*, vol. 1, no. 1, pp. 1–11, 2020, doi: 10.25008/bcsee.v1i1.2.

[16] 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.

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

[18] Y. C. Yuze, Y. Priyadi, and . C., "Analysis of Information Security Management Systems Using ISO/IEC 27001: 2013 And Recommendation 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.

[19] 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.

[20] N. A. Widodo and and A. F. R. , R. Rizal Isnanto, "Information Security Management System Planning And Implementation Based ON ISO/IEC 27001:2005 STANDARDS (Case Study in a National Private Bank)," vol.4,a no. 1, pp. 60–66, 2016.

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

[22] W. Apriandari and A. Sasongko, "Information Security Management System Analysis 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.

[23] A. Asriyanik and Prajoko, "Information Security Management in Academic Information Systems Using ISO 27005:2011 on Academic Information Systems (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)," *J. Tek. Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 315–325, 2018.

[24] N. Matondang, I. N. Isnainiyah, and A. Muliawatic, "Analysis of Information System Data Security Risk Management (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.

[25] 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.

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