Assessment of Information Security on Regional Financial Management Information System using KAMI Index 4.2

Rizky Dea Annisa Hidayah
Department of Information System Universitas Ahmad Dahlan Yogyakarta of Indonesia

Imam Riadi
Department of Information SystemUniversitas Ahmad Dahlan Yogyakarta of Indonesia

ABSTRACT
The security aspect concerns confidentiality, integrity, and availability. Problems with the implementation of security in SIMDA Finance have never held an information security assessment, there is no official policy regarding access rights to use SIMDA so data changes often occur. BPKAD requires an information security assessment to get an overview of the application of information security. The assessment is carried out using a questionnaire from the Information Security (KAMI) Index which refers to the ISO/IEC 27001:2013 standard, where respondents fill out questionnaires in 7 assessment areas. The results of the assessment show that the final score in the Electronic System area is in the High category with a score of 27, which means that SIMDA Finance is a part that is tied to the ongoing work process. The maturity level with a total score obtained from the results of the 5 areas of the KAMI Index is 218 which is at the Infeasible level. Meanwhile, for the maturity level, it gets groups I to II so it does not meet the feasibility of ISO 27001:2013 standardization. The results of the recommendations are in accordance with the results of the analysis, so SIMDA Finance needs to document all ongoing processes. Agencies need to pay attention to the implementation of information security internally and externally.

Keywords
Assessment, Information Security, KAMI Index 4.2

1. INTRODUCTION
Information technology is very important for organizations that can support organizational and individual performance. The local government is one of the government agencies that have utilized technology. The Regional Financial and Asset Management Agency (BPKAD) needs to compile financial reports for regional financial management, to make these financial reports, a reliable system is needed, namely a system that can process data (input) and generate information (output) that can be used by management for decision making [1]. According to Government Regulation Number 56 of 2005 concerning Regional Financial Information Systems (SIKD), followed by the Central Government Finance Agency (BPKP) compiling a Computer Application Program, namely the Regional Financial Management Information System (SIMDA). SIMDA Finance has been used at the BPKAD of Brebes Regency since 2007 to carry out several functions and tasks in regional financial management [2].

Technology and information systems have a role in advancing agencies, but they can also cause losses because they are vulnerable to threats. BPKAD also needs to implement information security to prevent threats to information assets. Based on the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 4 of 2016 concerning Information Security Management Systems, it states that every implementation of electronic systems requires security of information in the public interest, public services, the smooth running of state administrators or state defense and security [3]. This also needs to be implemented and considered in the Brebes Regency Regional Government, especially the BPKAD agency [4]. For example, in 2020, the National Cyber Security Operations Center (Pusopskamsinas) of the National Cyber and Crypto Agency (BSSN) found 88,414,296 cyber-attacks that occurred from January 1 to April 12, 2020 [5].

Information security protects information from various threatsto ensure smooth business processes, as well as reduce business risks [6]. The security aspect concernsconfidentiality, integrity, and availability [7]. Information security and awareness of the dangers of information leakage are important in the use of technology. However, technological developments do not always follow maximum security, so security threats will always be a problem in the application of information systems [8]. It is very important to maintain balance and ensure information security [9].

Problems with the implementation of security in SIMDA Finance have never held an information security assessment, there is no official policy regarding access rights to use SIMDA so data changes often occur. Therefore, BPKAD requires an information security assessment to get an overview of the implementation of information security. In this study, the assessment was carried out using a questionnaire tool based on the latest version of the Information Security Index (KAMI) which refers to the ISO/IEC 27001:2013 standard. The US index 4.2 has 7 scoring areas. The resulting data will provide an overview of readiness from aspects of completeness to maturity of information security so that it can be used to make improvements [10]. ISO 27001:2013 is one of the common information security standards used as the basis for information security operations [11]. The ISO/IEC 27001:2013 framework will regulate the Information Security Management System (ISMS), to design and recommend [12]. The method was designed by the Ministry of Communication and Information Technology to measure and analyze the readiness and maturity of information security [13]. The usefulness of information security assessment is useful for building an information security management framework and carrying out comprehensive improvements [14].

The importance of this research is that organizations can implement information security by using the established standards and have no difficulty understanding the extent to

which these standards have been implemented. As well as tobuild awareness of information security, which includes user awareness to enforce the rules, be aware of the dangers of information security, understand responsibilities, and act according to the rules [15].

2. STUDY LITERATURE

Study literature was conducted to get a solid basis for research. A literature study is a written summary of books, journals, and other documents. Activities carried out at this stage are reading, studying, and understanding related to research.

2.1 Regional Management InformationSystem (SIMDA) Financial

Information System is a combination of people, hardware, software, computer network, and data communications, and databases that are collected, used, to disseminate information [16]. IT Governance has responsibilities that consist of leaders, organizational structures, and processes that run in the organization. IT Governance integrates and ensures that IT in an organization supports business objectives. IT Governance enables organizations to take advantage [17].

The Regional Financial Management Information System (SIMDA) is a local government asset data processing system, with the output of the Financial SIMDA application consisting of, budgeting, administration, accounting, and reporting. The purpose of the SIMDA application is to utilize information systems to improve financial accountability and local government performance, including adequate transaction and information control [18].

2.2 Information Security

Technology has become a means to help human survival in various sectors. Information technology is closely related to the development of computer technology and is integrated with telecommunications technology. With this formulation, the term information technology means the collection of data or facts that are processed and then converted or stored in the form of computer-based illustrated, video, or text-based information, but technology also has its own security aspect [19].

Information security is not just about securing information, but how to prevent access, use, modification, and destruction of information to irresponsible parties [20]. In designing an information security system there are three important aspects that need to be considered, namely, confidentiality, integrity, and availability (CIA) as illustrated by the CIA Triad in Figure 1.

Figure 1. CIA Triad

a. Confidentiality must maintain the confidentiality of information by limiting the access rights of others.
b. Integrity must maintain the authenticity of the data/ information stored and guard against threats that can cause changes to the original information.
c. Availability information must be available andcan be accessed quickly by users when needed[21].

2.3 Information Security Management Systems (ISMS)

The Information Security Management System (ISMS) contains policies related to information management and IT risk. The main purpose of implementing ISMS is to eliminate or minimize the impact of threats on information security in an organization. The principle applied to ISMS is that an organization can Plan, Do, Check and Act or commonly called the PDCA Cycle [22].

2.4 ISO/IEC 27001

Series is a standard that focuses on Information Security Management Systems (ISMS). The need to establish a policy for information security based on the ISO/IEC 27001 standard certification must be defined and communicated to all employees and internal parties of an organization. This policy is to encourage the implementation of security controls tomake all parties in the organization aware of the responsibility for the protected organizational assets [23].

2.5 KAMI Index

KAMI Index is an assessment tool designed by the Ministry of Communications and Information Technology, which isused to analyze the level of readiness of information security in an organization. The assessment is carried out in various areas that are the target of implementing information security in the organization by adjusting the SNI ISO/IEC 27001:2013 standards.

KAMI Index does not analyze the existing feasibility, but as an illustration of the condition of the level of information security readiness. The results of the assessment of the data used will provide a view of readiness, from the aspect of completeness and maturity of the information security performance applied to the organization, so that it can be used to develop corrective steps and prioritization.

Respondents were also asked to explain the role of ICT in organizations in carrying out business processes. The aim of this process is to classify organizations into Low, Medium, High, and Critical sizes [24].

Table 1. Scoring Mapping

Security Status	Security Category		
	1	2	3
Are not done	0	0	0
In Planning	1	2	3
In application/ Partially applied	2	4	6
Completely Applied	3	6	9

Based on Table 1 Questions related to the basic information security framework are marked with the label “1”. Questions related to the implementation of information security operations are marked with the label “2”, and ISO/SNI 27001 compliance is labeled “3”.

Table 2. SE Correlation and Assessment Criteria

ELECTRONIC SYSTEM CATEGORY				
Low		**Final Score**		**Readiness Status**
10	15	0	174	Not Eligible
		175	312	Fulfillment of the Basic Framework
		313	535	Fairly Good
		536	645	Good
High		**Final Score**		**Readiness Status**
16	34	0	0	Not Eligible
		273	273	Fulfillment of the Basic Framework
		456	456	Fairly Good
		584	584	Good
Strategic		**Final Score**		**Readiness Status**
35	50	0	333	Not Eligible
		334	535	Fulfillment of the Basic Framework
		536	609	Fairly Good
		610	645	Good

Level of security application. This maturity level will later be used as a tool to report mapping and ranking of information security readiness in an organization. The maturity level is defined as:

- Level I – Initial Condition
- Level II – Implementation of the BasicFramework
- Level III – Defined and Consistent
- Level IV – Managed and Measurable
- Level V – Optimal

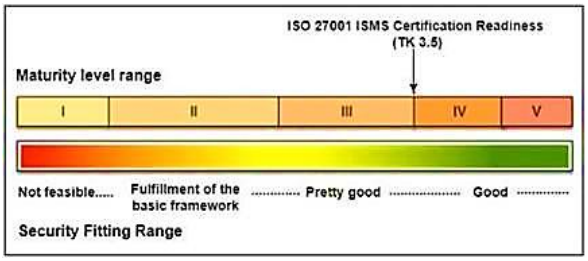

Figure 2. Relationship between Maturity Levels andReadiness

This level is added with intermediate levels, namely I+, II+, III+, and IV+. The minimum threshold for information security is Level III+ [25].

3. METHODOLOGY

This research will raise the subject of information security assessment in a system in organizations, especially BPKAD in the Brebes Regency Regional Government, by focusing on assessing the governance applied.

The method used in this study using KAMI Index version 4.2 covers seven areas of aveluation. The results of this study can help make recommendations to improve information security within the agency.

This section discusses the stages of research that will be carried out. This stage of research makes the research carried out focused. The flow of stages in completing this research such as literature study, data retrieval, analysis of results, making recommendations as shown in Figure 3

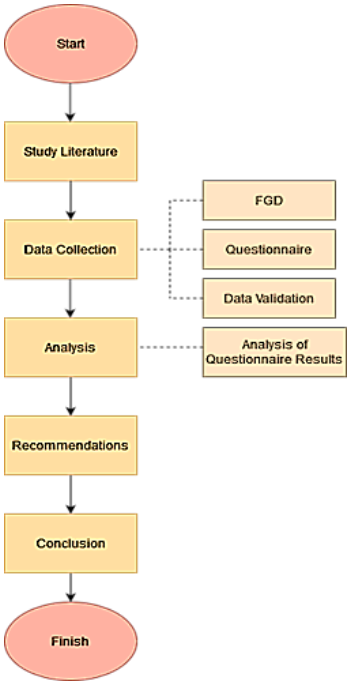

Figure 3. Research Stages

3.1 Data Collection

3.1.1 Focus Group Discoussion (FGD)

FGD is a group discussion activity that focuses on discussing certain problems in an informal setting. Data or information from respondents is an opinion and decision of the group.

3.1.2 Filling Out the Questionnaire

KAMI Index 4.2 questionnaire, where the respondent fills out the questionnaire. Data collection (*Sampling)* uses a purposive sampling where the sampling is a data source with certain considerations. In accordance with the Guide to the Implementation of Information Security Governance (2011) the selection of respondents is adjusted who has responsibilities in accordance with the questions in the questionnaire.

3.1.3 Data Validation

Data validation to prove the accuracy of the data with the actual situation. The technique used to validate the data is *a checklist.* Where checklist is done by face to face with the respondent in the process of filling *checklist*, the evidence from *checklist* that is requested is all the questions from the respondents who are answered**.**

3.2 Data Analysis

Data is processed through the KAMI Index questionnaire, resulting in a score for each assessment area. Furthermore, it will be analyzed according to the results of KAMI Indexscore. The data analysis method refers to the use of the KAMIIndex in the Information Security Governance Guidebook compiled by the Information Security Directorate Team. The analysis was carried out according to the results of the assessment on KAMI Index before and after validation.

3.3 Recommendations

The results of the analysis will produce recommendations with consideration of ISO 27001. At the recommendation stage, the recommendations are made based on the answers to each of KAMI Index questions. Recommendations are made as a reference for agencies to implement information security that can comply with the ISO 27001 standard. Recommendations

can be implemented in stages so that they can be developed and used by agencies.

3.4 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.

3.5 Conclusion

The conclusion stage is the last stage in the research. The conclusions obtained contain the results of the assessment on the KAMI Index, as well as the current state of security implementation. In addition, the conclusions also provide suggestions for improvement that are expected to be used as a reference in the future to achieve agency goals.

4. RESULT AND DISCUSSION

In this sub-chapter, analysis will be carried out based on data processing from calculations in KAMI Index questionnaire. In the analysis, there are two value results before validation and after validation, but only the results after validation are listed.

4.1 Information Security GovernanceAnalysis

The results of the application in this area, on the score before validation the majority of the application status is in the application /partial application, while the score after validation of the majority of the application state becomes in the planning.

Table 3. Completeness Score Governance

Security Status	Security Category						Total
	1	SK	2	SK	3	SK	
Are not done	0	0	0	1	0	1	0
In Planning	1	7	2	5	3	5	17
In the application/ Partially applied	2	1	4	2	6	0	10
Completely Applied	3	0	6	0	9	0	0
Total							27

Based on Table 3 the final score obtained is 27 where the final

Table 4. Governance Maturity Score

Control Category	Min	Score Achievement	SK	Valid	Status
II	12	36	19		I+
III	8	14	8	No	-
IV	24	54	0	No	-

While for Table 4 Maturity level II score also has a score of 19 which exceeds the minimum score for maturity level I+, which is 12, but does not exceed the minimum score for achieving maturity level II. Therefore it gets an I+ level.

4.2 Analysis of Information Security RiskManagement

The results of the application in this area, on the score before validation the majority of the application status is in the application /partial application, while the score after validation of the majority of the application state becomes in the planning.

Table 5. Risk Management Completeness Score

Security Status	Security Category						Total
	1	SK	2	SK	3	SK	
Are not done	0	1	0	1	0	0	0
In Planning	1	6	2	3	3	2	12
In the application/ Partially applied	2	3	4	0	6	0	6
Completely Applied	3	0	6	0	9	0	0
Total							27

Based on Table 5 the final score obtained is 18 where this final score is obtained after the data validation process. There is a difference of 5 points from the score before validation.For the label "3" a score of 0 is stated because the label "3" will give results if all questions related to the labels "1" and "2" are filled with "Partially Applied".

Table 6. Risk Management Maturity Score

Control Category	Min	Score Achievement	SK	Valid	Status
II	14	20	12	No	-
III	4	8	2	No	-
IV	8	12	4	No	-

While for Table 6 Maturity level II score has a score of 12 which does not exceed the minimum score for maturity level II, which is 14. Therefore, it gets group I with a "NO" validity.

4.3 Information Security Framework Analysis

score is obtained after the data validation process. Any questions that do not have evidence are downgraded to "In Planning" unless they have received the status of "InPlanning" or "Not Executed" then they do not need to be downgraded. There is a difference of 19 points from the score before validation.

The results of the application in this area, on the score before validation and after validation the majority of the application state is in partial deployment/applied.

Table 7. Completeness Score Framework

Security Status	Security Category						Total
	1	SK	2	SK	3	SK	
Are not done	0	0	0	0	0	0	0
In Planning	1	6	2	4	3	3	14
In the application/ Partially applied	2	6	4	6	6	4	36
Completely Applied	3	0	6	0	9	0	0
Total							50

Based on Table 7 the final score obtained is 50 where thisfinal score is obtained after the data validation process. There is a difference of 8 points from the score before validation.

Table 8. Maturity Score Framework

Control Category	Min	Score Achievement	SK	Valid	Status
II	15	24	16		I+
III	45	62	34	No	-
IV	15	27	0	No	-
V	12	18	0	No	-

While for Table 8 Maturity level II score has a score of 16 which exceeds the minimum score of maturity level II, which is 15, but does not exceed the achievement score, which is 24.

Therefore, it gets group I+.

4.4 Analysis of Information AssetManagement

The results of the application in this area, on the score before validation and after validation the majority of the application state is in partial deployment/applied.

Table 9. Asset Management Completeness Score Information

Security Status	Security Category						Total
	1	SK	2	SK	3	SK	
Are not done	0	0	0	0	0	0	0
In Planning	1	7	2	2	3	1	11
In the application/ Partially applied	2	11	4	6	6	3	46
Completely Applied	3	6	6	2	9	0	30
Total							87

Based on Table 9 the final score obtained is 87 where this final score is obtained after the data validation process. There is a difference of 40 points from the score before validation.

Table 10. Maturity Score of Information Asset Management

Control Category	Min	Score Achievement	SK	Valid	Status
II	25	62	67		II
III	35	50	20	No	-

4.5 Analysis of Information Technologyand Security

The results of the application in this area, on the score before validation the majority of the application state is in the application / partially applied, while the score after validation of the majority of the application state becomes in the planning.

Table 11. Technology and Information Security Completeness Score

Security Status	Security Category						Total
	1	SK	2	SK	3	SK	
Are not done	0	1	0	2	0	1	0
In Planning	1	9	2	8	3	1	28
In the application/ Partially applied	2	4	4	0	6	0	8
Completely Applied	3	0	6	0	9	0	0
Total							36

Based on Table 11 the final score obtained is 36 where this final score is obtained after the data validation process. There is difference of 15 points from the score before validation.

Table 12. Technology and Information SecurityMaturity Score

Control Category	Min	Score Achievement	SK	Valid	Status
II	18	28	17	No	-
III	40	62	19	No	-
IV	6	9	0	No	-

As for Table 12 Maturity level II score has a score of 17 which does not exceed the minimum score of maturity level II, which is 18, and does not exceed the achievement score, which is 28. Therefore, it gets group I with "NO" validity

4.6 Supplement

In the supplement category, the assessment is in the form of a percentage (%) at each point.

Table 13. Rating Category Supplement

Points	Name	Score
7.1	Security of ThirdParty Engagement Service Providers	1.81
7.2	Security of Cloud Infrastructure Services (*Cloud Services*)	2.60
7.3	Personal Data Protection	2.25

In the supplement category the assessment is in the form of a percentage (%). In Table 13 the results of the assessment are based purely on the results of the respondents. For points 7.1 Third Party Security Service Providers get 60% results obtained from a score of: 3 (1.81:3), there is a difference of

While for Table 10 The maturity level II score has a score of 67 which exceeds the minimum score for the maturity level II, which is 25, and exceeds the achievement score, which is 62. Therefore, it gets class II.

5% from before validation. As for the point 7.2 Cloud Infrastructure Services (*Cloud Services*) getting 87% no difference from before validation, and the last point 7.3 Personal Data Protection getting 75% there is a 17%difference from before validation.

4.7 Dashboard Results

Based on the results of the questionnaire scores obtained, it produces a dashboard view of the KAMI Index which describes the level of completeness and maturity in each assessment area.

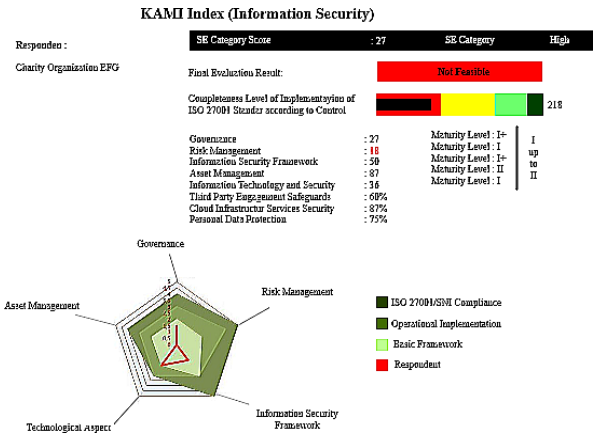

Figure 4. Dashboard of asessment

Figure 4 shows that the level or category of the electronic system used at the BPKAD of Brebes Regency is in the High category with a score obtained is 27, there is no difference in scores in the SE category before validation. The level of completeness of the implementation of the ISO 27001 standard in accordance with the SE category is at the **"Not Appropriate"** with a total score of 218 generated in each information security area, having a difference of 84 points from before validation. Meanwhile, the maturity level obtained in each area is classified as I to II.

5. CONCLUSION

Results the final score in the Electronic System area is in the High category with a score of 27, which means SIMDA

Finance is a part that is tied to the ongoing work process. Maturity level with a total score obtained from the results of the 5 areas of KAMI Index is 218 which is at the "Not Eligible" level. Meanwhile, for the maturity level, it gets groups I to II so it does not meet the feasibility of ISO 27001:2013 standardization. Based on the recommendations required by the agency, SIMDA Finance needs to document all ongoing processes. Agencies need to pay attention to the implementation of information security internally and externally.

6. REFERENCES

[1] PKP. (2014). SIMDA BMD Application Operation Manual version 2.0.7. November 2015, 1–61.

[2] Sugiyantari, D., Titisari, P., & Sumani, S. (2018). The Effectiveness of the Implementation of the Cloud Finance Regional Management Information System (Simda) in the Jember Regency Government. Bisma, 12(1), 106. https://doi.org/10.19184/bisma.v12i1.7607

[3] Yunella, M., Herlambang, AD, & Putra, WHN (2020). Evaluation of Information Security Governance at the Malang City Communication and Informatics Service Using the KAMI Index. Journal of Information Technology and Computer Science Development, 3(10), 9552–9559. http://j-ptiik.ub.ac.id/index.php/jptiik/article/view/6521

[4] Firzah, BA (2017). Evaluation of Information Security Management Using the Information Security Index (KAMI) Based on Iso / Iec 27001: 2013 at the Directorate of Technology and Information System Development (Dptsi) Its Surabaya Evaluating Information Security Management Using Ind. 6(1).

[5] BSSN. (2019). Information Security Index (KAMI). National Cyber and Crypto Agency (BSSN), November.

[6] Pratiwi Hadiati Agus, WL (2020). Evaluation of theLevel of Information Security Readiness Using the Information Security Index (KAMI Index) Version 4.0 at the Bogor City Communications and Information Office. Journal of Technology Development …, 2(5), 146–163

[7] Information, TDK (2013). Guidelines for the Implementation of Information Security Governance for Public Service Providers. In Journal of Chemical Information and Modeling (Vol. 53, Issue 9).

[8] Saputra. (2020). Iso 17799 Policies In Organizations As Information Security System Management. Angewandte Chemie International Edition, 6(11), 951–952., 3(2), 5–24.

[9] Kirillova, EA, Yakhutlov, UM, Wenqi, X., Huiting, G., & Suyu, W. (2020). Information security in the management of personnelin a modern organization. Proceedings of the 2020 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2020, 107–109. https://doi.org/10.1109/ITQMIS51053.2020.93228 84

[10] Sensuse, DI, Syarif, M., Suprapto, H., Wirawan, R., Satria, D., & Normandia, Y. (2017). Informationsecurity evaluation using KAMI index for security improvement in BMKG. 2017 5th International Conference on Cyber and IT Service Management, CITSM 2017. https://doi.org/101.1109/CITSM.2017.8089293.

[11] Monev, V. (2020). Organizational Information Security Maturity Assessment Based on ISO 27001 and ISO27002. 2020 34th International Conference on Information Technologies, InfoTech 2020 - Proceedings, September, 17–18. https://doi.org/10.1109/InfoTech49733.2020.92110 66

[12] Yasin, M., Akhmad Arman, A., Edward, IJM, & Shalannanda, W. (2020). Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ). Proceedings of the 14th International Conference on Telecommunication Systems, Services, and Applications, TSSA 2020, 2013(95), 3–7. https://doi.org/10.1109/TSSA51342.2020.9310875

[13] Adi Reynaldo, Sengkey Rizal, P. (2020). Information Security Analysis of Southeast Minahasa District Government Using the US Index. Journal of Engineering, 15(3), 189–198.

[14] Yasin, M., Akhmad Arman, A., Edward, IJM, & Shalannanda, W. (2020). Designing information security governance recommendations and roadmap using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ). Proceedings of the 14th International Conference on TelecommunicationSystems, Services, and Applications, TSSA 2020, 2013(95), 3–7. https://doi.org/10.1109/TSSA51342.2020.9310875

[15] Adi Reynaldo, Sengkey Rizal, P. (2020). Information Security Analysis of Southeast Minahasa District Government Using the US Index. Journal of Engineering, 15(3), 189–198.

[14] Sun, Z., Zhang, J., Yang, H., & Li, J. (2020). Research on the Effectiveness Analysis of Information Security Controls. Proceedings of 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2020, Itnec, 894– 897. https://doi.org/10.1109/ITNEC48623.2020.908480 9

[15] Nurbojatmiko, Fajar Firmansyah, A., Aini, Q., Saehudin, A., & Amsariah, S. (2020). Information Security Awareness of Students on Academic Information System Using the Kruger Approach. 2020 8th International Conference on Cyber and IT Service Management, CITSM 2020.https://doi.org/101.1109/CITSM50537.2020.92687 95

[16] Bhaskoro, SF, & Riadi, I. (2022). Analysis of Risk Assessment on Attendance Information Systems using COBIT 5 Framework. International Journal of Computer Applications, 184(7), 16–24. https://doi.org/10.5120/ijca2022922030

[17] Noveryal, N., & Riadi, I. (2022). Analysis a Maturity of Case Search Information Systems using Cobit 5 Framework. International Journal of Computer Applications, 184(12), 29–35. https://doi.org/10.5120/ijca2022922101

[18] Development and Finance Supervisory Agency. SIMDA Computer Application Program. Accessed on Friday 24 September 2021. http://bpkp.go.id/konten/433/SIMDA.bpkp

[19] Hardianti, S., & Riadi, I. (2022). Service Risk Assessment Learning Management System using ISO 31000:2018/31010. International Journal of Computer Applications, 184(4), 1–11.

https://doi.org/10.5120/ijca2022921993

[20] Volchkov, A. (2019). Information security governance: framework and toolset for CISOs and decision makers. CRC Press

[21] Rahardjo, B. (2017). Information & Network Security. INDONESIAN PEOPLE. http://budi.rahardjo.id/files/keamanan.pdf

[22] Susanto, H. (2018). Information Security Is INFORMATION Security. In Zen and the Art of Information Security. APPLE ACADEMIC PRESS. https://doi.org/10.1016/b978 159749168- 6/50012-7

[23] Chopra, A., & Chaudhary, M. (2020). Implementing an Information Security Management System. In Implementing an Information Security Management System. APRESS. https://doi.org/10.1007/978-1-4842-5413-4

[24] Purnama, C. (2016). Management Information Systems (C. Anam (ed.)). Global People.

[25] KOMINFO. (2011). Guidelines for the Implementation of Information Security Governance for Public Service Providers. In the Directorate of Information Security, Ministry of Communications and Information Technology (Issue April).

[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 US 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.