Use of the Information Security Index (KAMI) 4.2 as an Evaluation Method at the Paser Regency Communication, Informatics, Statistics and Coding Service

Nikita Samantha*, Dwi Arief Prambudi, I Putu Deny Arthawan Sugih Prabowo
Information Systems Study Program, Department of Mathematics and Information Technology, Institut Teknologi Kalimantan

Email: *10191065@student.itk.ac.id, dwiariefprambudi@lecturer.itk.ac.id, putudeny.asp@lecturer.itk.ac.id

DOI: https://doi.org/10.31284/j.jtm.2024.v5i1.4619
Received 13 June 2023; Received in revised 24 July 2023; Accepted 14 August 2023; Available online 15 January 2024

Abstract

Paser Department of Communication, Informatics, Statistics, and Cryptography (Diskominfostaper) is a regional institution tasked to provide information on regional development and public service provider. Based on Kominfo regulation No. 4 *of* 2016*, Diskominfostaper Paser district as a local government apparatus, requires implementation and supervision related to information security in order to safeguard all managed information. However, the information security that exists today is still very weak because on several occasions there have been attempts to hack the system owned and the involvement of third parties without a formal contract. In addition, there has never been an evaluation of information security either independently or from an external party. In this study, an evaluation of information security was carried out at Diskominfostaper Paser Regency using the Index* KAMI 4.2 *with the* ISO/IEC 27001:2013 *standard to determine the level of information security readiness. The results of the evaluation were obtained with an overall final score of 220 and a final score in the Electronic System* (SE) *category of* 30 *which was included in the "High" category, thus indicating that information security is currently in the "Inadequate" Preparedness Level status with a Maturity Level of level* I *to level* II*. As a result, of* 95 *recommendations for improvement were produced in the six areas of the Index* KAMI 4.2 *assessment in order to improve compliance with the Completeness Level status in fulfilling the* ISO/IEC 27001:2013 *Basic Framework.*

Keywords: *Information Communication, Statistics and Encryption Service of Paser Regency, Evaluation, Information Security Index (*KAMI*)* 4.2*,* ISO/IEC 27001:2013*, Information Security*

1. Introduction

Information Technology (IT) is developing very rapidly nowadays, causing all organizations to have to adapt and implement advances in information technology at any time. Based on a survey by the Central Statistics Agency (BPS), technological development in Indonesia in 2021 was 62.10%, a much higher increase compared to 2020 which was only 53.73% [1]. Information technology can be said to be a technology used to manage data in many ways to create valuable information that can be used as a decision-making process [2]. Information can be defined as raw data that is converted into a form that is more valuable for the recipient. The more important and valuable the information, the more information security is needed to avoid the emergence of risks from these information assets [3]. Therefore, information security is an asset that must be maintained to avoid misuse of that information [4]. There is a vulnerability to information security in organizations, so an Information Security Governance is needed, including regional officials as public service providers.

The Department of Communications, Informatics, Statistics and Encoding or what can be abbreviated as Diskominfostaper Paser Regency is a regional institution that carries out its main tasks

and functions (tupoksi) and always strives to realize public services and quality performance in order to implement good governance using the use of Information Technology in accordance with Presidential direction No. 3 of 2003 concerning public services based on e-government in order to achieve Paser Regency becoming a Smart City [5]. As a public service provider in the field of communications and informatics, the Paser Regency Diskominfostaper provides information related to regional development and public services through print and electronic media, which is the most important part, so it requires implementation and attention regarding information security in order to safeguard all managed information.

Based on the results of interviews with the Paser Regency Diskominfostaper, it is known that the information security they have is still very weak because on several occasions there have been hacking attempts on their systems. This can occur due to a lack of workers who are experts in the field of Information Technology, so that the handling itself involves a third party (external) without an official contract to maintain the security of the information system. Apart from this, the Paser Regency Diskominfostaper has also never carried out an information security evaluation either internally or independently (self assessment) or with external parties through the National Cyber & Crypto Agency (BSSN). So based on the problems above, an information security evaluation was carried out at the Paser Regency Diskominfostaper to assess the current information security condition whether it complies with applicable standards or not.

Information security evaluation is an activity in assessing the level of maturity and readiness related to information security in an organization. The information security evaluation method will be used in accordance with international standards, namely the Information Security Index (KAMI) method established by the National Cyber & Crypto Agency (BSSN). Based on regulations by BSSN Number 8 of 2021, the Information Security Index (KAMI) is applied to assess the level of readiness or maturity of information security which has been designed in accordance with the ISO/IEC 27001:2013 standard so that it is able to provide an overview of the current conditions in the organization. The National Cyber & Crypto Agency (BSSN) has issued an improved version of the previous Information Security Index (KAMI) 4.2 which includes 7 (seven) evaluation areas based on the SNI ISO/27001:2013 standard, namely Electronic Systems Category, Information Security Governance area, Management area Information Security Risk, Information Security Framework area, Information Asset Management area, Technology Aspects area, as well as Supplements [6]-[7].

This research resulted in an overall final score for information security evaluation at the Paser Regency Diskominfostaper of 220 and a final score in the Electronic Systems (SE) category of 30 which is included in the "High" category, thus indicating that information security is currently at a Readiness Level of "No Feasible" with a Maturity Level at level I to level II. A total of 95 recommendations for improvement were produced in the six areas of the Index KAMI 4.2 assessment to increase compliance with the Completeness Level status in meeting the Basic Framework of ISO/IEC 27001:2013.

2. Methodology

The stages carried out in this research consisted of 8 (eight) stages, starting from the literature study stage to the conclusion and suggestion stage. A detailed explanation of each stage in carrying out research can be seen in Figure 1 below.

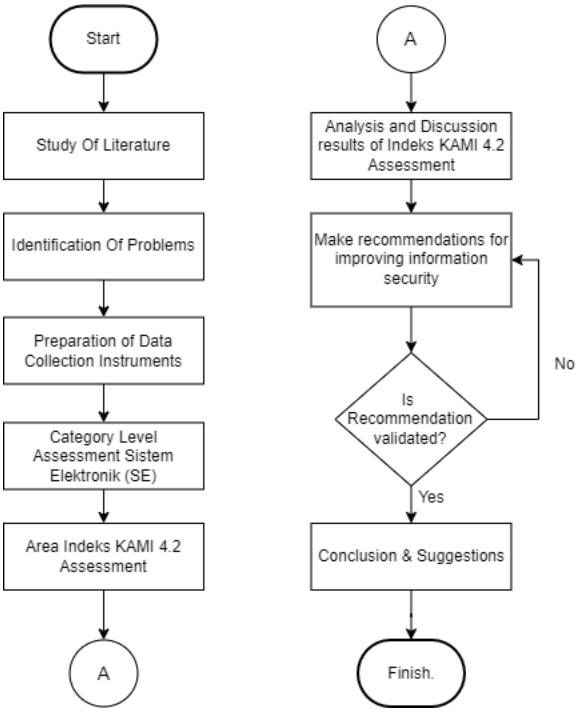

Figure 1. Research Flow Diagram

2.1 Study Of Literature

The literature study stage is carried out to search for theories and research studies to provide researchers with knowledge in identifying problems in research objects sourced from books, journals, articles or guidebooks related to theories related to research. In this research, literature studies related to the Paser Regency Diskominfostaper, Information Security, the Index KAMI 4.2 assessment method, Information Security Management Systems (SMKI) and ISO/IEC 27001:2013 were used.

2.2 Identification Of Problems

The problem identification stage was carried out to determine the existing conditions and dig deeper into the problems, especially those related to information security at the Paser Regency Diskominfostaper. Problem identification was carried out using the interview method conducted with respondents from the Paser Regency Diskominfostaper. The results obtained from this stage are that the existing conditions related to information security at the Paser Regency Diskominfostaper are still very weak, so it is necessary to carry out an evaluation using the Index KAMI 4.2 in accordance with the ISO/IEC 27001:2013 standard to determine and assess the level of maturity and readiness of the Diskominfostaper information security Paser Regency.

2.3 Preparation Of Data Collection Instruments

The stages of preparing data collection instruments were carried out to help and make it easier for researchers to collect data at the Paser Regency Diskominfostaper. This stage was carried out by compiling the seven areas of the Index KAMI 4.2 assessment with respondents in each field belonging to the Paser Regency Diskominfostaper. The results obtained from this stage are mapping the Index KAMI 4.2 area with respondents so that the data and information obtained to carry out assessments in the next stage are precise and accurate.

2.4 The Electronic System (SE) Category Level Assessment

The level assessment stages of the Electronic System (SE) Category were carried out to classify the characteristics of the electronic system used at the Paser Regency Diskominfostaper at low, high or strategic levels. The assessment was carried out using the interview method with

respondents, and the assessment results were processed using Microsoft Office Excel software provided by the Index KAMI 4.2. The results obtained from this stage are in the form of classification of characteristic levels including low, high or strategic through the total score from the Electronic System (SE) category assessment at the Paser Regency Diskominfostaper.

2.5 Index KAMI 4.2 Area Assessment

The assessment stage of the Index KAMI 4.2 area was carried out to determine the completeness and maturity value of current information security at the Paser Regency Diskominfostaper. The assessment was carried out using an interview method with respondents, and the results of the assessment covering the Information Security Governance area, Information Security Risk area, Information Security Framework area, Information Asset Management area, Information Technology and Security area and Supplements were processed using Microsoft Office Excel software which had been provided by Index KAMI 4.2. The results obtained from this stage are in the form of the level of security completeness and security maturity level from the total score of the Index KAMI 4.2 area assessment at the Paser Regency Diskominfostaper.

2.6 Analysis And Discussion Results Of Index KAMI 4.2 Assessment

The analysis and discussion stages of the assessment results are carried out to analyze and discuss the final results obtained from the Index KAMI 4.2 assessment results to assess the maturity and completeness of information security and make decisions in accordance with the evaluation results. Analysis was carried out using data presented by the Index KAMI 4.2 dashboard in Microsoft Office Excel software. The results obtained from this stage are in the form of information security conditions at the Paser Regency Diskominfostaper, whether they have fulfilled the ISMS according to the ISO/IEC 27001:2013 standard or not based on the maturity, completeness and readiness of the information security dashboard of the Index KAMI 4.2.

2.7 Make Recommendations For Improving Information Security

The stage of making recommendations for improvements is carried out to provide recommendations and suggestions for improvements to areas that have the implementation status of Not Implemented at the Paser Regency Diskominfostaper. In determining a recommendation, the relationship beten the Index KAMI 4.2 area and ISO/IEC 27001:2013 is matched so that clauses and controls are obtained that are appropriate to the area that will be recommended for improvement. Then the results of the improvement recommendations will be validated whether the recommendations provided are in accordance with ISO/IEC 27001:2013. The results obtained from this stage are in the form of recommendations and suggestions documents according to the ISO/IEC 27001:2013 standard in implementing ISMS from the results of evaluations that have been carried out using the Index KAMI 4.2.

2.8 Conclusion & Suggestions

At this stage, conclusions and suggestions are drawn based on the results of all the stages that have been carried out in this research. The conclusion at this stage contains the final results of the research that has been carried out, and as a solution experienced in solving existing problems. Suggestions at this stage contain suggestions and suggestions for further research.

3. Result and Discussion

This section contains an explanation of the results of information security evaluation research using the Index KAMI 4.2 at the Paser Regency Diskominfostaper starting from the stages of preparing data collection instruments to the results of the research.

3.1 Preparation Of Data Collection Instruments

The preparation of the data collection instrument was carried out in two stages, namely mapping fields and sources with the Index KAMI 4.2 area and preparing an assessment list for all the

Index KAMI 4.2 areas. The first stage carried out mapping of the four fields owned by the Paser Regency Diskominfostaper according to their duties and functions, then adjusted to each area of the KAMI Index 4.2. The mapping results can be seen in Table 1 below.

Table 1. Mapping Resource Persons with Index KAMI 4.2

Field of Resource Persons	Index KAMI 4.2
Communication and Information Technology Field	- Electronic System (SE) - Information Security Governance Area - Information Security Framework Area
Informatics Application Field	- Technology and Information Security Area - Supplements
Field of Statistics and Coding	- Information Security Risk Management Area - Information Asset Management Area

The next stage is to prepare an assessment list for all areas of the KAMI 4.2 Index. There are 194 (one hundred and ninety four) questions divided into 7 evaluation areas including the Electronic Systems Category with 10 questions, the Information Security Governance area with 22 questions, the Information Security Risk Management area with 16 questions, the Information Security Management Framework area with 29 questions questions, the Information Asset Management area with 38 questions, the Information Technology and Security area with 26 questions and Supplements with 53 questions.

3.2 The Electronic System (SE) Category Level Assessment

After preparing the data collection instruments, an assessment of the Electronic System (SE) Category level was carried out using the interview method with resource persons. The results of the assessment can be seen in Table 2 below.

Table 2. Electronic System (SE) Category Level Assessment Results

Section I : Electronic Systems Category			
This section evaluates the level or category of electronic systems used			
Number of Electronic System (SE) Questions		**:**	**10**
Results of Resource Persons' Answers			
Implementation Status	**Number of Questions**	**Score**	**Total Score**
[A]	4	5	20
[B]	4	2	8
[C]	2	1	2
Score for determining the Electronic Systems category :			**30**

The score obtained for determining the Electronic System Category (SE) was 30 and was included in the "High" category, which means the importance of using electronic systems at the Paser Regency Diskominfostaper. With the increasing dependence of an organization on the role of SE, there will be an increase in the number of forms of information security implementation [8].

3.3 Index KAMI 4.2 Area Assessment

After an assessment is carried out regarding the use of Electronic Systems (SE), an assessment is then carried out on all areas of the Index KAMI 4.2 including the Information Security Governance Area, Information Security Risk Area, Information Security Framework Area, Information Asset Management Area, Information Technology and Security Area and Supplements. The assessment of the Index KAMI 4.2 area at the Paser Regency Diskominfostaper can be seen in the following subchapter.

3.3.1 Information Security Governance Area Assessment

An assessment of the Information Security Governance area was carried out to explain and evaluate the readiness regarding the functions, duties, responsibilities and authority of information

security managers starting from leaders, work units to operational implementers at the Paser Regency Diskominfostaper which was carried out using the interview method with resource persons, as for the results of the assessment can be seen in Table 3 below.

Table 3. Information Security Governance Area Assessment Results

Section II : Information Security Governance		
This section evaluates the readiness of the form of information security governance along with the agency/company/function, duties and responsibilities of information security managers.		
Results of Resource Persons' Answers		
Implementation Status	**Number of Area Questions**	**Area Evaluation Value Score**
Not Implemented	8	0
In Planning	3	3
Under Implementation/Partially Implemented	3	8
Comprehensively Implemented	8	33
Number of Questions / Area Evaluation Values :	**22**	**44**
Security Completeness Level Results		
Security Category Level (KP)	**Number of Area Questions**	**Implementation Score 1 and 2**
Security Category (KP) 1	8	16
Security Category (KP) 2	8	28
Security Category (KP) 3	6	0
Number of Questions / Application Score:	**22**	**44**
Security Maturity Level Results		
Maturity Category Level	**Number of Area Questions**	**Score**	**Maturity Status Level**
II	13	36	II
III	3	8	I
IV	6	0	I
Total Score / Status Level :	**22**	**44**	**II**

Table 3 can be concluded that the Paser Regency Diskominfostaper Information Security Governance area currently has a total evaluation score of 44 points and a security maturity level where the higher the security completeness value, the higher the security maturity. In this area, the results obtained are at security maturity level II, which means implementing the basic framework.

3.3.2 Information Security Risk Areas Assessment

An assessment of the Information Security Risk area was carried out to explain and evaluate the readiness to implement information security risk management as a basis for implementing strategies and implementing controls that ensure that all risks at the Paser Regency Diskominfostaper were carried out using the interview method with resource persons. The results of the assessment can be seen in Table 4 following.

Table 4. Information Security Risk Area Assessment Results

Section III : Information Security Risks		
This section evaluates the readiness to implement information security risk management as a basis for implementing information security strategies.		
Results of Resource Persons' Answers		
Implementation Status	**Number of Area Questions**	**Area Evaluation Value Score**
Not Implemented	12	0
In Planning	0	0
Under Implementation/Partially Implemented	0	0
Comprehensively Implemented	4	9
Number of Questions / Area Evaluation Values :	**16**	**9**
Security Completeness Level Results		

Security Category Level (KP)	Number of Area Questions	Implementation Score 1 and 2
Security Category (KP) 1	10	9
Security Category (KP) 2	4	0
Security Category (KP) 3	2	0
Number of Questions / Application Score:	**16**	**9**

Security Maturity Level Results

Maturity Category Level	Number of Area Questions	Score	Maturity Status Level
II	10	9	I
III	2	0	I
IV	2	0	I
V	2	0	I
Total Score / Status Level :	**16**	**9**	**I**

Table 4 can be concluded that the Paser Regency Diskominfostaper Information Security Risk area currently has a total evaluation value of 9 points and a security maturity level where the higher the security completeness value, the higher the security maturity. In this area, the results obtained are at security maturity level I, which means in initial conditions.

3.3.3 Information Security Framework Area Assessment

An assessment of the Information Security Framework area was carried out to explain and evaluate the policies, operational procedures and competencies of Human Resources (HR) at the Paser Regency Diskominfostaper which was carried out using the interview method with resource persons. The results of the assessment can be seen in Table 5 below.

Table 5. Information Security Framework Area Assessment Results

Section IV : Information Security Framework		
This section evaluates the completeness and readiness of the information security management framework (policies & procedures) and its implementation strategy.		
Results of Resource Persons' Answers		
Implementation Status	**Number of Area Questions**	**Area Evaluation Value Score**
Not Implemented	15	0
In Planning	0	0
Under Implementation/Partially Implemented	4	8
Comprehensively Implemented	10	33
Number of Questions / Area Evaluation Values :	**29**	**41**
Security Completeness Level Results		
Security Category Level (KP)	**Number of Area Questions**	**Implementation Score 1 and 2**
Security Category (KP) 1	12	19
Security Category (KP) 2	10	22
Security Category (KP) 3	7	0
Number of Questions / Application Score:	**29**	**41**
Security Maturity Level Results		
Maturity Category Level	**Number of Area Questions**	**Score**	**Maturity Status Level**
II	11	11	I
III	13	30	I
IV	3	0	I
V	2	0	I
Total Score / Status Level :	**29**	**41**	**I**

Table 5 can be concluded that the Paser Regency Diskominfostaper Information Security Framework area currently has a total evaluation score of 41 points and a security maturity level where

the higher the security completeness value, the higher the security maturity. In this area, the results obtained are at security maturity level I, which means in initial conditions.

3.3.4 Information Asset Management Area assessment

The assessment of the Information Asset Management area was carried out to explain and evaluate the form of security related to the existence of information assets including all technical and administrative processes in the asset use cycle at the Paser Regency Diskominfostaper which was carried out using the interview method with resource persons. The results of the assessment can be seen in Table 6 following.

Table 6. Information Asset Management Area Assessment Results

Section V : Information Asset Management		
This section evaluates the completeness of the security of information assets, including the entire use cycle of these assets.		
Results of Resource Persons' Answers		
Implementation Status	**Number of Area Questions**	**Area Evaluation Value Score**
Not Implemented	25	0
In Planning	0	0
Under Implementation/Partially Implemented	2	4
Comprehensively Implemented	11	42
Number of Questions / Area Evaluation Values :	**38**	**46**
Security Completeness Level Results		
Security Category Level (KP)	**Number of Area Questions**	**Implementation Score 1 and 2**
Security Category (KP) 1	24	28
Security Category (KP) 2	10	18
Security Category (KP) 3	4	0
Number of Questions / Application Score:	**38**	**46**
Security Maturity Level Results		
Maturity Category Level	**Number of Area Questions**	**Score**	**Maturity Status Level**
II	29	34	I+
III	9	12	I
Total Score / Status Level :	**38**	**46**	**I+**

Table 6 can be concluded that the Paser Regency Diskominfostaper Information Asset Management area currently has a total evaluation score of 41 points and a security maturity level where the higher the security completeness value, the higher the security maturity. In this area, the results obtained are at the security maturity level I+, which means that it is in the initial condition.

3.3.5 Information Technology and Security Area Assessment

An assessment of the Information Technology and Security area was carried out to explain and evaluate the completeness, consistency and effectiveness of the use of technology in securing information assets at the Paser Regency Diskominfostaper which was carried out using the interview method with resource persons. The results of the assessment can be seen in Table 7 below.

Table 7. Information Technology and Security Area Assessment Results

Section VI : Technology and Information Security		
This section evaluates the completeness, consistency and effectiveness of the use of technology in securing information assets.		
Results of Resource Persons' Answers		
Implementation Status	**Number of Area Questions**	**Area Evaluation Value Score**
Not Implemented	7	0
In Planning	1	3

Under Implementation/Partially Implemented	3	8
Comprehensively Implemented	15	69
Number of Questions / Area Evaluation Values :	**26**	**80**

Security Completeness Level Results

Security Category Level (KP)	Number of Area Questions	Implementation Score 1 and 2
Security Category (KP) 1	14	28
Security Category (KP) 2	10	40
Security Category (KP) 3	2	0
Number of Questions / Application Score:	**26**	**68**

Security Maturity Level Results

Maturity Category Level	Number of Area Questions	Score	Maturity Status Level
II	14	28	II
III	11	49	I
IV	1	3	I
Total Score / Status Level :	**26**	**80**	**II**

Table 7 can be concluded that the Paser Regency Diskominfostaper Information Technology and Security area currently has a total evaluation score of 80 points and a security maturity level where the higher the security completeness value, the higher the security maturity. In this area, the results obtained are at security maturity level II, which means implementing the basic framework.

3.3.6 Supplement Assessment

The assessment of the Supplement was carried out to explain and evaluate the policy of involving third parties or external parties in the supply chain starting from the management and handling of a service to risk management, the use of cloud infrastructure-based services and forms of security and protection of personal data at the Regency Diskominfostaper The assessment was carried out using the interview method with resource persons. The results of the assessment can be seen in Table 8 below.

Table 8. Supplement Assessment Results

Section VII : Supplement			
This section evaluates the completeness, consistency and effectiveness of the use of technology in securing information assets.			
Number of Questions Supplement : 53			
Results of Resource Persons' Answers			
Implementation Status	**Third Party Engagement Security Value Score**	**Cloud Infrastructure Services Security Value Score**	**Personal Data Protection Value Score**
Not Implemented	0	0	0
In Planning	1	0	0
Under Implementation/Partially Implemented	8	2	8
Comprehensively Implemented	36	0	9
Area Evaluation Value :	**45**	**2**	**17**

Security Completeness Level Results

Security Category Level (KP)	Number of Area Questions	Implementation Score 1
Security Category (KP) 1	53	56
Number of Questions / Application Score:	**53**	**56**

Table 8 can be concluded that the Paser Regency Diskominfostaper Supplement currently has a total evaluation value of the Supplement for the Security of Third Party Involvement section of 45 points and decimalized to 1.67 or 56%, the Supplement for the Security of Cloud Infrastructure Services section of 2 points and decimalized to 0.20 or 7% and the Personal Data Protection section supplement is 17 points and decimalized to 1.06 or 35%. The results obtained are still less than the expected standard, so it can provide opportunities for risks related to data controlled by the Paser Regency Diskominfostaper.

3.4 Analysis And Discussion Results Of Index KAMI 4.2 Assessment

The analysis and discussion stages of the assessment results are carried out to analyze and discuss the final results obtained from the Index KAMI 4.2 assessment results to assess the maturity and completeness of information security and make decisions in accordance with the evaluation results. The analysis was carried out using the Index KAMI 4.2 dashboard which displays the final evaluation results of the seven areas including the maturity level of each area, final evaluation of information security readiness status, level of completeness in implementing ISO/IEC 27001:2013 and the KAMI 4.2 Index Radar Chart can be seen in Figure 2 below. .

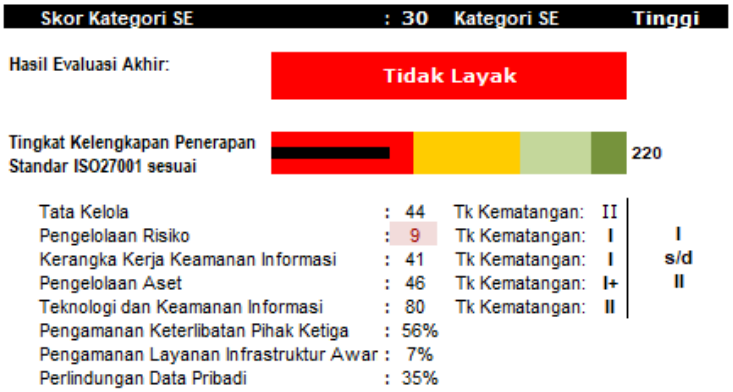

Figure 2. Dashboard Index KAMI 4.2 Diskominfostaper Paser

The results of the evaluation of the level of information security readiness that was carried out at the Paser Regency Diskominfostaper obtained an Electronic Systems (SE) Category score of 30 and was included in the "High" category, which means that the importance of using electronic systems is a main part of the work process or a part that cannot be separated from the ongoing work process. Level of Completeness of Implementation of ISO/IEC Standard 27001:2013 Diskominfostaper Paser Regency received a score of 220 which is marked by a black horizontal line which stops at the "Red" bar which means the status of the level of information security readiness or the final evaluation result is "Not Appropriate" in meets ISO/IEC 27001:2013 Standard. Meanwhile, to get a "Good" readiness status, the minimum is to get a final score above 583. The information security maturity level results at the Paser Regency Diskominfostaper are at levels I to II.

Details of the maturity level of the six areas of the Index KAMI 4.2 assessment at the Paser Regency Communication, Information, Statistics and Encryption Service (Diskominfostaper) include the Information Security Governance area with a final score of 44, the Information Security Risk area with a final score of 9, the Information Security Framework area with a final score of 41, the Information Asset Management area with a final score of 46, the Information Technology and Security area with a final score of 80, and the Supplement area which is divided into three parts, namely Securing Third Party Involvement with a percentage of 56%, Securing Cloud Infrastructure Services with the percentage is 7% and the last is Personal Data Protection with a percentage of 35%. There is also a Radar Chart which shows the Level of Completeness of the six areas of the Index KAMI 4.2 assessment at the Paser Regency Diskominfostaper which has been evaluated, which can be seen in Figure 3 below.

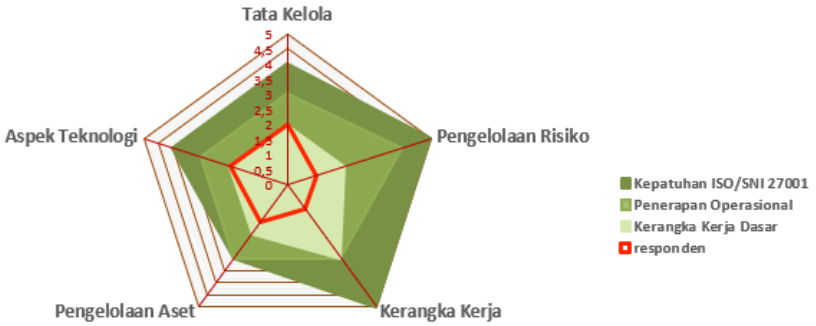

Figure 3. Radar Chart Index KAMI 4.2 Diskominfostaper Paser

The radar chart shows that overall the implementation of the Information Security Management System (SMKI) has not been met, including compliance with ISO/IEC 27001:2013, operational implementation of the basic framework and respondents. The area that has the best Information Security implementation results is the Technology and Information Security area which is supported by evaluation results that are closest to fulfilling ISMS compliance. Meanwhile, other areas still need improvement to meet the Basic Framework level.

3.5 Make Recommendations For Improving Information Security

The stage of making recommendations for improvements is carried out to provide recommendations and suggestions for improvements to areas that have the implementation status of Not Implemented at the Paser Regency Diskominfostaper.

3.5.1 Recommendations For Improving Information Security Governance Area

Recommendations for improvements to the Information Security Governance area at the Paser Regency Diskominfostaper include 8 questions that have the implementation status of "Not Implemented" based on ISO/IEC 27001:2013. One example of recommendations for improvements can be seen in Table 9 below.

Table 9. Recommendations For Improving Information Security Governance Area

No.	Question	Application Status	Skor Value
2.10	Has your agency/company integrated information security needs/requirements into existing work processes?	Not Implemented	0

Recommendations For Improving ISO/IEC 27001:2013
Control A.7.2.1 *Management responsibilities*

Agencies must ensure that their information security policies and controls are relevant and adequate to strengthen the terms and conditions in the work process. Previously, the agency had to know the information security requirements and then divide and adjust the integrated work processes with information security requirements. The aim was to find out whether information security requirements needed to be in the work process or not and this had to be accompanied by reasons.

3.5.2

Recommendations For Improving Information Security Risk Area

Recommendations for improvements to the Information Security Risk area at the Paser Regency Diskominfostaper include 12 questions that have the implementation status of "Not Implemented" based on ISO/IEC 27001:2013. One example of recommendations for improvements can be seen in Table 10 below.

Table 10. Recommendations For Improving Information Security Risk Area

No.	Question	Application Status	Skor Value
3.8	Has the impact of losses related to the loss/disruption of the function of main assets been determined in accordance with the existing definition?	Not Implemented	0

Recommendations For Improving ISO/IEC 27001:2013
Control A.16.1.6 *Learning from information security incidents*

Agencies can evaluate and analyze information security incidents to reduce the possibility of incidents or the impact of future incidents. Evaluation of information security incidents can show increased control needs and determine the calculations of the information security policy review process in minimizing damage that occurs in the future. Documents required by agencies include Risk Register documents.

3.5.3

Recommendations For Improving Information Security Framework Area

Recommendations for improvements to the Information Security Framework area at the Paser Regency Diskominfostaper include 15 questions that have the implementation status of "Not Implemented" based on ISO/IEC 27001:2013. One example of recommendations for improvements can be seen in Table 11 below.

Table 11. Recommendations For Improving Information Security Framework Area

No.	Question	Application Status	Skor Value
4.9	Are formal procedures in place to manage exceptions to information security practices, including processes for following up on the consequences of these conditions?	Not Implemented	0

3.5.4

Recommendations For Improving ISO/IEC 27001:2013
Control A.18.2.3 *Technical compliance review*

Agencies are required to implement official procedures to monitor compliance with technical policies consistently, specifically and follow up on exceptions to information security applications. Every technical compliance review is only carried out by competent or authorized people and the process is always under the supervision of parties who have authority in information security management at the agency.

Recommendations For Improving Information Asset Management Area

Recommendations for improvements to the Information Asset Management area at the Paser Regency Diskominfostaper include 25 questions that have the implementation status of "Not Implemented" based on ISO/IEC 27001:2013. One example of recommendations for improvements can be seen in Table 12 below.

Table 12. Recommendations For Improving Information Asset Management Area

No.	Question	Application Status	Skor Value
5.12	Regulations on the use of personal data that require written permission to be given by the owner of the personal data	Not Implemented	0

3.5.5

Recommendations For Improving ISO/IEC 27001:2013
Control A.18.1.4 *Privacy & Protection of Personally Identifiable Information*

Agencies must develop policies regarding personal data privacy. This policy must be communicated to everyone involved in managing personal information. Responsibility for handling personal data and ensuring awareness of privacy principles must be handled in accordance with relevant laws and regulations.

Recommendations For Improving Technology and Information Security Area

Recommendations for improvements to the Technology and Information Security area at the Paser Regency Diskominfostaper include 7 questions that have the implementation status of "Not Implemented" based on ISO/IEC 27001:2013. One example of recommendations for improvements can be seen in Table 13 below.

Table 13. Recommendations for Improvements Technology and Information Security Area

No.	Question	Application Status	Skor Value
6.10	Are all logs analyzed periodically to ensure accuracy, validity and completeness of their contents (for audit trail and forensic purposes)?	Not Implemented	0

Recommendations For Improving ISO/IEC 27001:2013
Control A.12.4.1 *Event logging*
Control A.18.1.2 *Protection of Records*

Event logs that record user activity, exceptions, failures and information security events in the agency must be analyzed, created, stored and reviewed periodically. So that the results of logs or recorded records in the system must be protected from loss, damage, falsification, unauthorized access and unauthorized release, in accordance with statutory, contractual and business regulatory requirements so that they can become forensic evidence and track record evidence when audits are carried out.	**3.5.6**

Recommendations For Improving Suplemen

Recommendations for improvements to the Supplement at the Paser Regency Diskominfostaper include 28 questions which have the implementation status of "Not Implemented" based on ISO/IEC 27001:2013. One example of recommendations for improvements can be seen in Table 14 below.

Table 14. Recommendations For Improving Suplemen

No.	Question	Application Status	Skor Value
7.1.3.3	Are there regular reports available on the achievement of service level targets (SLAs) and security aspects required in commercial agreements (contracts)?	Not Implemented	0

4.

Recommendations For Improving ISO/IEC 27001:2013
Control A.10.1.2 *Key Management*
Control A.13.1.2 *Security of Network Services*

Agencies and external parties are advised to create documents related to the success of service levels or Service Level Agreements (SLA) contained in the contracts of both parties. The contents of the service level agreement Service Level Agreement (SLA) or contracts with external parties for cryptographic services need to cover issues of responsibility, service reliability and response time for service provision.

Conclusions

The conclusion that can be obtained from research related to information security evaluation using the KAMI 4.2 Index at the Paser Regency Diskominfostaper is an assessment in the Electronic Systems (SE) Category of 30 which is included in the “High” category. This means that the importance of using sistem elektronik is a main part of the work process or a part that cannot be separated from the ongoing work process. The assessment results from the Information Security Governance Area, Information Security Risk Area, Information Security Framework Area, Information Asset Management Area, Information Technology and Security Area and Supplements were 220, so that the final information security evaluation results at the Paser Regency Diskominfostaper were at status The Readiness Level is “Not feasible” in meeting ISO/IEC 27001:2013 standards or controls with the Maturity Level being at level I to level II. Recommendations and suggestions for improvement were submitted in each area, including 8 recommendations in the field of Information Security Governance, 12 recommendations in the field of Information Security Risk, recommendations in the field of Information Security Framework, 25 recommendations in the field of Information Asset Management, recommendations in the field of Technology. and Information Security as well as 28 recommendations in the field of supplements, resulting in a total of 95 recommendations and suggestions for improvement in all areas. With recommendations and suggestions for improvement, it is hoped that it will be able to increase compliance with the Completeness Level status in meeting the Basic Framework of ISO/IEC 27001:2013.

References

[1] Badan Pusat Statistik, “Statistik Telekomunikasi Indonesia 2021," 2021.
[2] Prabawati, V. A., Rachmadi, A., and Perdanakusuma, A. R., "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan Kerangka Kerja OCTAVE-S Pada Unit Pengelola Sistem Informasi Dan Kehumasan (PSIK)," Fakultas Ilmu Komputer Universitas Brawijaya, 3(3), 2829–2836, 2019.
[3] T. Kristanto et al, “Analisis Manajemen Keamanan Informasi Menggunakan Standart ISO 27001:2005 Pada Staff IT Support di Instansi XYZ," vol. 02, no. 02, 2019.

[4] Siswanti, S, "Penilaian Kematangan Proses Keamanan Sistem Informasi Pendaftaran Pasien Menggunakan Framework Cobit 4.1.," SATIN-Sains dan Teknologi Informasi, 7(1), 123–133, 2021.
[5] Rencana Strategi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Paser, "Rencana Strategi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Paser," Kabupaten Paser, Dinas Komunikasi Informatika, Statistik dan Persandian, 2016-2021.
[6] Badan Siber dan Sandi Negara Republik Indonesia, Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2021. 2021, pp. 10–27.
[7] Badan Siber dan Sandi Negara Republik Indonesia, "Indeks KAMI Versi 4.2," diambil kembali dari "Indeks KAMI": https://bssn.go.id/indeks-kami/, 2019.
[8] Prasetyowati, D. D., Gamayanto, I., Wibowo, S., & Suharnawi, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang", Journal of Information System Vol.4, No. 1, 65-75, 2019.

How to cite this article:
Samantha N, Prambudi D A, Prabowo I P D A S. Use of the Information Security Index (KAMI) 4.2 as an Evaluation Method at the Paser Regency Communication, Informatics, Statistics and Coding Service. *Jurnal Teknologi dan Manajemen.* 2024 Januari; 5(1):1-14. DOI: 10.31284/j.jtm.2024.v5i1.4619