INFORMATION SECURITY OPTIMIZATION USING INFORMATION SECURITY INDEX MANAGEMENT (US) CASE STUDY: IBISA PURWOREJO

Eko Jhony Pranata[1], Muhammad Taufiq Nuruzzaman [2]

[12] Universitas Islam Negeri Sunan Kalijaga Yogyakarta
Email: [1]ekojhonypranata@gmail.com, [2]m.taufiq@uin-suka.ac.id

Abstract

Attacks that occur on networks are very common nowadays, with more and more ways to access data and of course more and more technologies are being used to increase threats to network security. Optimization of Information Security by using the Information Security Index (KAMI) on the Purworejo IBISA network obtained an index result of 235, so it can be said that it is not optimal and there are still many improvements. Therefore, that is the basis for the need to implement Open Source SIEM using Manageengine OpManager into the Information Security Index (KAMI). This research was conducted as a form of optimization to support the information security process so that it works in accordance with the standards in the KAMI Index. The research method carried out includes a literature study, then conducting a Pre-Assessment of the KAMI index, after that implementing the ManageEngine OpManager infrastructure, then monitoring the Information Security Index using technology on the ManageEngine OpManager, and conducting a Post-Assessment of the KAMI Index, then this final stage is Analyze the monitoring results and compare the results of monitoring the network conditions before and after the implementation of ManageEngine OpManager. The score from the comparison for research results related to the KAMI index Shows that the assessment score after the implementation of ManageEngine OpManager has increased by 57, better than before without the implementation of ManageEngine OpManager which originally got a value of 235 to 292. The advantage in the KAMI index is that it helps add value to aspects of governance, asset management, and Information Technology and Security,

***Keywords**: KAMI Index, Information Security, ManageEngine OpManage*

1. INTRODUCTION

The number of service users and the influence of the internet, the more information obtained from the internet. Worldwide, around 650 terabytes of data and 205 million emails are sent over the internet every minute. Planning, design and implementation of network topologies, in this case wireless computer networks, are not that reliable. The expansion of computer networks will have a major impact on the quality of internet connection services and existing data exchange conditions. The quality of internet services and data exchange connections after network expansion is of course very important to change the performance of the computer network itself.

Correspondingwith the Regulation of the Minister of Communication and Informatics Number 4 of 2016 concerning Information Security Management System Standards, every government agency is required to comply with the ISMS and have a CIA (Confidentiality, Availability and Integrity) score for information assets. their institution. According to research conducted by Iccs india team, which explains that cybercrime losses are estimated at 6 trillion and 60 million records are compromised because the cloud is not configured according to cybersecurity. Security breaches occur in small businesses, accounting for a total of 43% of attacks. 56% of data breaches took more than a month to find a solution. That is then corroborated by data on the most common ransomware attacks encountered in 2019, but WannaCry continues to claim victims worldwide,

2. LITERATURE REVIEW

WannaCrywere caught on more than 23.5 percent of devices eventually targeted by ransomware, and spam and phishing emails remained the most common sources of infection last year, said Precise Security. No less than 67% of ransomware infections are sent via email, and a lack of cybersecurity training and weak password and access management are the next reasons why computers end up encrypted after an attack. Only 16% of ransomware attacks are supported by malicious websites and online advertisements. "The number of ransomware attacks targeting government agencies, organizations in the health, energy and education sectors is steadily increasing.

TemporarySome simple ransomware can lock down a system in a way that is easy for a knowledgeable person to reverse, more sophisticated malware exploits a technique called crypto-virus ransomware.(Dewantara and Sugiantoro, 2021)

Institute of TechnologyBusinessAnd the Health of the Indonesian Sons of the Nation (IBISA) is one of the tertiary institutions or campuses located in

Purworejo, Central Java. IBISA has a Data and Information Base Center (PUSDATIN) The IBISA campus also has information system services, namely: Registration of new IBISA students through an online system, Academic information system services for students, lecturers and academics, Alumni data and Study Tracer, Online examination service system, eLearning is integrated with the academic system, integrated mail system and integrated employee management system.

Withthe need for government agencies to be able to implement information security management standards according to the ISMS and the need to trace to the public is an absolute option so that protection officers can clearly see what is going on with their networks. The question is whether the use of Ossim can detect all attacks on the network and effectively secure the network from existing attacks. Especially in terms of monitoring servers and networks, of course, administrators cannot work 24 hours in front of their computers so that they always know if there are disturbances on servers and networks.(Angga Juansyah, Bagus Pratama, 2018), therefore a supporting facility is needed by the administrator trading system to be able to monitor servers and networks even though they are not directly in front of the computer, so a tracking system is needed that can monitor their servers and the network for 24 hours and get notifications directly to the admin.

Beforeinformation security standards are applied, evaluation of information security devices in the IBISA Indonesia network is needed to get an overview of the state of readiness and maturity of information security management. Based on this, this study will measure the maturity level of information security management on the IBISA Indonesia network using the version prepared by Indonesian communications in 2019, namely our Index. Our index is made with ISO 27001:2018 Reference contained in information security ISO 27001 is a form of international standards framework that contains standards in the area of information security, scope of use of technology and asset management that helps organizations ensure that information security is operating effectively.

3. RESEARCH METHODS

The steps to be carried out in this study are related to the evaluation of Information Security (KAMI) using the ManageEngine OpManager on the IBISA Purworejo network, which can be seen in the following figure.

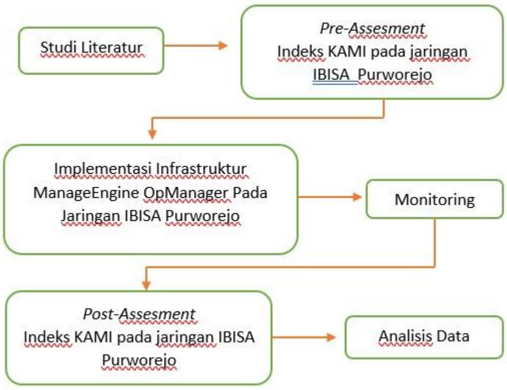

Studi Literatur
Pre-Assesment
Indeks KAMI pada jaringan IBISA Purworejo
Implementasi Infrastruktur ManageEngine OpManager Pada Jaringan IBISA Purworejo
Monitoring
Post-Assesment
Indeks KAMI pada jaringan IBISA Purworejo
Analisis Data

Figure 1 Research Flow

3.A. Study of literature

The first stage in this research is Literature Study to find references and theoretical foundations that can later be used as a reference or basis for this research. Literature study is carried out by reviewing papers or journals related to the theme of this research, reading and reviewing various related literature sources as an initial justification to see if there is a difference if ManageEngine OpManager and without implementing ManageEngine OpManager.

3.B. WE Index Pre-Assessment on the Purworejo IBISA Network

Before conducting a simulation of the implementation of the attack, you can see the results of the Network forensic presentation of the results of the simulation, which was then followed by filling out the KAMI Index Pre-Assessment questionnaire to the respondents, in this case the Head of the Information Technology Division and Database (PUSDATIN) IBISA Purworejo . The results of the questionnaire are then calculated according to the format in the application from the Information Security Directorate of the Indonesian Ministry of Communication and Informatics.

3.C. Implementation of the OpManager Infrastructure on the IBISA Purworejo Network

At this stage, the implementation of the ManageEngine OpManager infrastructure is carried out on a server and agent that will be placed on the IBISA Purworejo network with the scope of the network to be monitored and limited to computer networks located at IBISA Purworejo.

3.D. Monitoring

At this stage it is carried out to monitor the network and detect intrusion attempts, carry out filtering processes, and detect installations on bandwidth that are detected to be abnormal on the network as a result of attacks or threats to network security both internally and externally.

3.E. Post-Assessment of KAMI Index on the Purworejo IBISA Network

After presenting the results of monitoring, measurements regarding the KAMI Index will be carried out again for respondents, in this case, to the Information System Analysis Expert Staff at the PUSDATIN office in the IBISA Purworejo network environment by providing a Post-Assessment Information Security Index (KAMI) to measure again the value of the Information Security Index (KAMI) after monitoring with ManageEngine OpMananager . Then the results of the questionnaire will be recalculated according to the application format owned by the Information Security Directorate of the Indonesian Ministry of Communication and Informatics. Then the results of these calculations will be compared with the results of the Pre-Assessment that was carried out before whether there are differences or not,

3.F. Data analysis

The final stage of this study is to analyze the results of monitoring to be able to find out comparisons to the network both before and after the implementation and installation of ManageEngine OpMananager on the IBISA Purworejo network. Then the results of the analysis will get conclusions to become input material in conducting network security management in the future.

4. RESULTS AND DISCUSSION

4.A. OpManager architecture

The architecture of the ManageEngine OpManager is as follows:

a. *Central Servers*
*Central Servers*acts as a unified console that synchronizes data with multiple Probe servers. Central Server is designed to provide network visibility across locations, consolidate, and report on the health of multiple remote networks.

b. *Probe Servers*
*Probe Servers*acts as a polling machine. It monitors routers, switches, firewalls, servers, and other network devices for errors and performance. This generates availability, health, and performance reports. The Probe Server periodically synchronizes data with the Central Server.

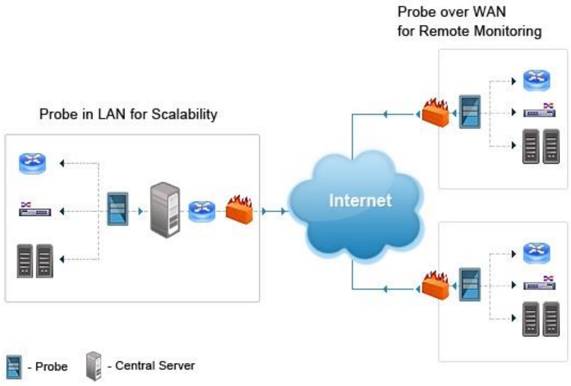
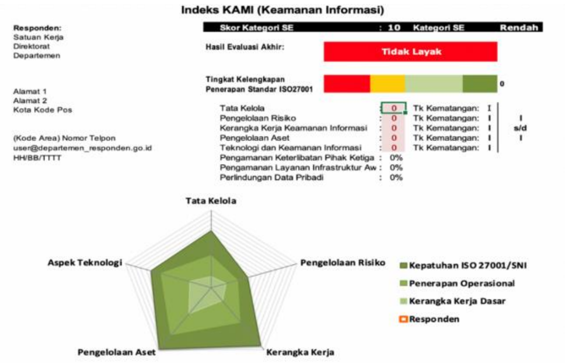


Figure 2 OpManager Architecture

4.B. Evaluation of the WE Index

Evaluation of the KAMI Index is recommended to be carried out by staff who are authorized and responsible for all information security management in agencies.



Indeks KAMI (Keamanan Informasi)

Responden:
Satuan Kerja
Direktorat
Departemen

Alamat 1
Alamat 2
Kota Kode Pos

(Kode Area) Nomor Telpon
user@departemen_responden.go.id
HH/BB/TTTT

Skor Kategori SE : 10 Kategori SE Rendah

Hasil Evaluasi Akhir: Tidak Layak

Tingkat Kelengkapan Penerapan Standar ISO27001 0

Tata Kelola	: 0	Tk Kematangan:	I	
Pengelolaan Risiko	: 0	Tk Kematangan:	I	I
Kerangka Kerja Keamanan Informasi	: 0	Tk Kematangan:	I	s/d
Pengelolaan Aset	: 0	Tk Kematangan:	I	I
Teknologi dan Keamanan Informasi	: 0	Tk Kematangan:	I	
Pengamanan Keterlibatan Pihak Ketiga	: 0%			
Pengamanan Layanan Infrastruktur Aw	: 0%			
Perlindungan Data Pribadi	: 0%			

Figure 3 Graph WE Index

Based on the picture above, the KAMI Index chart regarding evaluations carried out using the Information Security Index (KAMI), which includes 5 aspects including:

1. Information security governance

This section evaluates the form of information security governance and the organization/function, as well as the preparedness of the responsibilities and responsibilities of the Manager responsible for information security. The control required is to define the roles, responsibilities, authorities of information security management from the person in charge of the work unit to the operator. This includes ongoing work planning, budget allocation, plan evaluation, and strategies to improve information security governance performance

2. Information Security Risk Management

In this section, the readiness of implementing information security risk management is evaluated as a basis for implementing an information security strategy. The control implemented is the existence of a risk management framework and is clearly defined in terms of risk acceptance thresholds, risk management plans and mitigation measures. Review their effectiveness regularly

3. Information Security Framework

This section assesses the completeness and readiness of the information security management framework (policies and procedures) and implementation strategy. The controls required are a number of operating policies and procedures, including implementation strategies, measuring control effectiveness, and corrective actions.

4. Information Asset Management

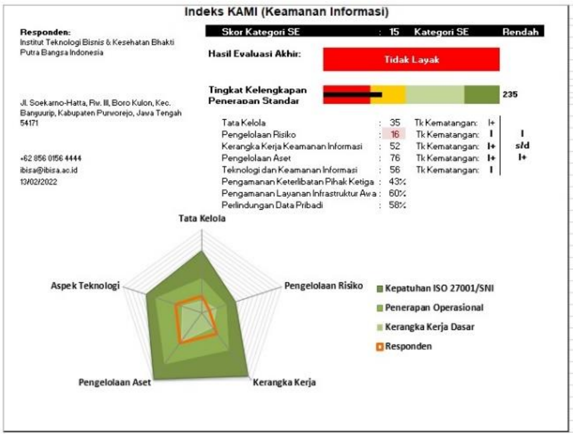
This section assesses the security and integrity of information assets, including the entire lifecycle of those assets. The necessary controls are a form of security regarding the existence of information assets and the entire technology process and the life cycle of the assets being managed.

5. Information Technology and Security

This section evaluates the integrity, consistency, and effectiveness of using technology to protect information assets. The controls used are strategies related to the level of risk and do not explicitly mention a particular technology or brand. Among the five aspects of information security based on the Information Security Index (KAMI), the role of IT in protecting information can be measured and used as input. IT service manager.

4.C. OUR Index Results

This stage discusses the results of the overall assessment of the 5 areas of information security on the IBISA Purworejo network. The following is a dashboard of the results of the assessment of the 5 information security areas of the IBISA Purworejo network.



Indeks KAMI (Keamanan Informasi)

Responden:
Institut Teknologi Bisnis & Kesehatan Bhakti
Putra Bangsa Indonesia

Jl. Soekarno-Hatta, Rw. III, Boro Kulon, Kec.
Banyuurip, Kabupaten Purworejo, Jawa Tengah
54171

+62 856 0156 4444
ibisa@ibisa.ac.id
13/02/2022

Skor Kategori SE : 15 Kategori SE Rendah

Hasil Evaluasi Akhir: Tidak Layak

Tingkat Kelengkapan Penerapan Standar 235

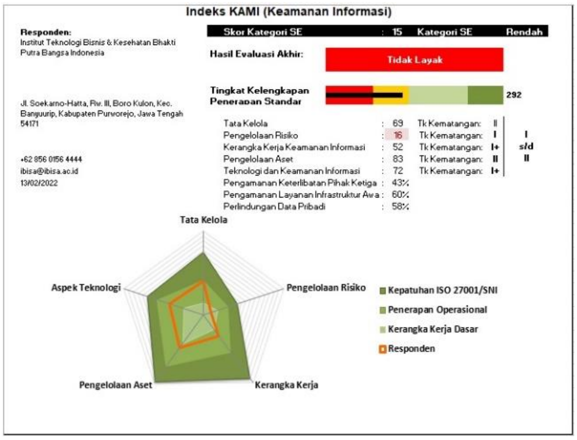
Tata Kelola	:	35	Tk Kematangan:	I+	
Pengelolaan Risiko	:	16	Tk Kematangan:	I	I
Kerangka Kerja Keamanan Informasi	:	52	Tk Kematangan:	I+	s/d
Pengelolaan Aset	:	76	Tk Kematangan:	I+	I+
Teknologi dan Keamanan Informasi	:	56	Tk Kematangan:	I	
Pengamanan Keterlibatan Pihak Ketiga	:	43%			
Pengamanan Layanan Infrastruktur Awa	:	60%			
Perlindungan Data Pribadi	:	58%			

Figure 4 Dashboard of the KAMI Index Pre-Assessment

In the picture above 3 shows that the category of electronic systems on the IBISA Purworejo campus network is in the Low category, with a score of 15. An electronic system where the performance or continuity of the IBISA Purworejo network flow has not been fully realized. At the same time, the integrity level of ISO 27001 implementation is at the level of "Inadequate", with a score level of 235, indicating that the institution's high dependence on electronic systems is not supported by adequate information security from the institution. This final result also shows that the IBISA Purworejo network still needs a lot of improvement. This can be seen from the level of maturity, with an average of I and I+ it can be said that the readiness of information security certification is still not feasible for information security certification.

After analysis and simulation, the results of the forensic analysis on the IBISA Purworejo network were presented and a re-questionnaire was carried out as a form of comparison, what happened after the ManageEngine OpManager was implemented in the IBISA Purworejo network infrastructure. The study conducted a Post-assessment of the IBISA Purworejo network with the Information Security Index (KAMI) questionnaire to be able to measure the value of the Information Security Index (KAMI) owned by the agency.

With the important role of IT being so high, and from the results of the attack analysis and its correlation with the ManageEngine OpMananager that was carried out. As shown in Figure 4.6 the value of monitoring the IBISA Purworejo network is 292, this shows that the level of information maturity has changed or increased previously when the Pre-assessment was at level I to I+ now is at level I to II when the Post-assessment carried out, as for the increase in value in the aspects of Governance, Asset Management and Technology and Information Security so that the total value increase from 235 to 292.



Indeks KAMI (Keamanan Informasi)

Responden:
Institut Teknologi Bisnis & Kesehatan Bhakti
Putra Bangsa Indonesia

Jl. Soekarno-Hatta, Rw. III, Boro Kulon, Kec.
Banyuurip, Kabupaten Purworejo, Jawa Tengah
54171

+62 856 0156 4444
ibisa@ibisa.ac.id
13/02/2022

Skor Kategori SE : 15 Kategori SE Rendah

Hasil Evaluasi Akhir: Tidak Layak

Tingkat Kelengkapan Penerapan Standar 292

Tata Kelola	:	69	Tk Kematangan:	II	
Pengelolaan Risiko	:	16	Tk Kematangan:	I	I
Kerangka Kerja Keamanan Informasi	:	52	Tk Kematangan:	I+	s/d
Pengelolaan Aset	:	83	Tk Kematangan:	II	II
Teknologi dan Keamanan Informasi	:	72	Tk Kematangan:	I+	
Pengamanan Keterlibatan Pihak Ketiga	:	43%			
Pengamanan Layanan Infrastruktur Awa	:	60%			
Perlindungan Data Pribadi	:	58%			

Figure 5 Dashboard of the KAMI Index Post-Assessment

Details on each aspect that has been measured in the index can be seen in Figure 5. It can be seen that there has been no change in the Risk Management aspect, the information security framework, there has been a change in the Governance aspect, Information and Technology asset management and Information Security which shows there is a successive increase of 34, 10 and 16 pawns.

4.D. Information Security Governance

Table 1 Maturity value of Information Security Governance Area (i)

Information	Score
Number of questions Stage 1	8
Number of questions Stage 2	8
Number of questions Stage 3	6
Min Score Limit for Deployment Stage 3 Scores	48
Total Score of Implementation Stages 1 & 2	35
Status Assessment Implementation Stage 3	Invalid
Maturity Level Score II	27
Maturity Level Minimum Score II	*12*
Maturity Level Achievement Score II	*36*
Status	I+
Maturity Level Score III	8
Maturity Level Validity III	No
Maturity Level Minimum Score III	8
Maturity Level Achievement Score III	14
Status	No
Maturity Level Score IV	0
Maturity Level Validity IV	No
Maturity Level Minimum Score IV	24
Maturity Level Achievement Score IV	54
Status	No

Table 2 Maturity Value of Information Security Governance Area (ii)

Deployment Status	Maturity Level				Total
	II	III	IV	V	
Is not done	1	0	6	0	7
In Planning	4	2	0	0	6
Under Application/Partially Applied	8	1	0	0	9
Completely Applied	0	0	0	0	0
Total	13	3	6	0	22

The completeness score that has been obtained from the maturity of information security governance is 35. Based on table 1 it can be seen that the number of questions in stages 1, 2 and 3 respectively are 8, 8 and 6 with a score limit for implementing 3 which is 48 and with the total of stages 1 & 2 is 35, so the assessment status for implementation stage 3 is "Invalid". For maturity score II, it is worth 27 with a minimum score of 12 and an achievement score of 36, so that the status "I +" is obtained. then for the score of maturity level III it is worth 8 with a validity of "No" along with a minimum score of 8 and an achievement score of 14, so that the status is "No".

Based on Table 2, there were 7 questions at maturity level II and IV which were not answered or in this case "Not done". Then there are 6 questions each at maturity level II and III which the reviewers responded to "In Planning". Furthermore, the status of implementation "In implementation/Partially Applied" contained in the 9 questions that have been responded to are at maturity levels II and III, namely 8 and 1 respectively. Based on the results obtained, it is known that in the current information security governance area this understanding of information security is still not as expected in agencies, there are many points that are not or have not been carried out.

2.1 Information Security Risk Management

Table 3 Maturity scores in the Information Security Risk Management area (i)

Information	Score
Number of questions Stage 1	10
Number of questions Stage 2	4
Number of questions Stage 3	2
Min Score Limit for Deployment Stage 3 Scores	36
Total Score of Implementation Stages 1 & 2	16
Status Assessment Implementation Stage 3	Invalid
Maturity Level Score II	8
Maturity Level Minimum Score II	14
Maturity Level Achievement Score II	*20*
Status	No
Maturity Level Score III	4
Maturity Level Validity III	No
Maturity Level Minimum Score III	4
Maturity Level Achievement Score III	8
Status	No
Maturity Level Score IV	4
Maturity Level Validity IV	No
Maturity Level Minimum Score IV	8
Maturity Level Achievement Score IV	12
Status	No
Maturity Level Score V	0
Maturity Level Validity V	No
Maturity Level Minimum Score V	12
Maturity Level Achievement Score V	18

Table 4 Maturity scores in the Information Security Risk Management area (ii)

Deployment Status	Maturity Level				Total
	II	III	IV	V	
Is not done	2	0	0	1	3
In Planning	8	2	2	1	13
Under Application/Partially Applied	0	0	0	0	0
Completely Applied	0	0	0	0	0

Total	10	2	2	2	16

The score that has been obtained on information security risk management is 16, based on table 3 it can be seen that the number of questions in stages 1, 2 and 3 respectively are 10, 4 and 2 with a minimum score limit for the score of implementation stage 3 which is 36 and with a total the score for stages 1 & 2 is 16, so the assessment status for the implementation stage 3 is "Invalid". for the maturity level II score there is a value of 8 with a minimum score of 14 along with an achievement score of 20 so that a "No" status is obtained. then for the score of maturity level III there is a value of 4 with a validity of "No" and the minimum score is worth 4 and the achievement score is worth 8 so that the status is "No". Furthermore, the maturity level score IV is worth 4 with a "No" validity with a minimum score of 8 and an achievement score of 12 with a "No" status. Furthermore, the maturity level score V is 0 with a "No" validity with a minimum score of 12 and an achievement score of 18 so that it gets "No" status.

According to table 4 there were 3 questions at levels II and V which were not answered or "Not Done" with 2 questions at level II and 1 question at level V. then at the "In Planning" stage there were 13 questions each of which had been responded to at level II, III, IV, and V respectively are 8 questions for level II, 2 questions at level III, 2 questions at level IV and 1 question at level V. For the level of maturity in the implementation status "In Implementation/Partially Applied " and at the maturity level of implementation status “Completely Implemented” there were no questions responded to.Based on the results that have been obtained, it can be seen that the current conditions in the Information Security Risk Management area, namely that most of the Information Security Risk Management is still at the planning stage, although there are some that have not been implemented.

4.E. Information Security Management Framework

Table 5 Maturity score of the Information Security Framework area (i)

Information	Score
Number of questions Stage 1	12
Number of questions Stage 2	10
Number of questions Stage 3	7
Min Score Limit for Deployment Stage 3 Scores	64
Total Score of Implementation Stages 1 & 2	52
Status Assessment Implementation Stage 3	Invalid
Maturity Level Score II	20
Maturity Level Minimum Score II	15
Maturity Level Achievement Score II	*24*
Status	I+
Maturity Level Score III	32
Maturity Level Validity III	No
Maturity Level Minimum Score III	45
Maturity Level Achievement Score III	62
Status	No
Maturity Level Score IV	0
Maturity Level Validity IV	No
Maturity Level Minimum Score IV	15
Maturity Level Achievement Score IV	27
Status	No
Maturity Level Score V	0
Maturity Level Validity V	No
Maturity Level Minimum Score V	12
Maturity Level Achievement Score V	18
Status	No

Table 6 Maturity scores in the Information Security Framework area (ii)

Deployment Status	**Maturity Level**				**Total**
	II	**III**	**IV**	**V**	
Is not done	0	2	0	0	2
In Planning	8	5	2	1	16
Under Application/Partially Applied	2	4	1	1	8
Completely Applied	1	2	0	0	3
Total	11	13	3	2	29

The completeness score obtained on the information security framework is 52. It can be seen from Table 5 that Items 12, 10 and 7 are for stages 1, 2 and 3 respectively for stages 1, 2 and 3. The minimum score limit for implementation score 3 is 64 points out of a total of 64 Implementation stage 1 and 2 is 52, so the assessment status at implementation stage 3 is "Invalid". Then the Maturity Score II has a value of 20 with a minimum score of 15 and an achievement score of 24, so Get "I+" status. The next Maturity Level Score is III with a value of 32, with a validity of "No", and a Minimum Score of 45, and an achievement score of 62, so that a "No" status is obtained. Next Maturity Rating IV is worth 0, with "No" Validity, and with a minimum score of 15 and an achievement score of 27 with "No" status . Then for maturity level V there is a score of 0 with a "No" Validity, a minimum score of 12 with an achievement score of 18 so that a "No" status is obtained.

Based on table 6 there are 2 questions at maturity level III which were not responded to or "Not Done". At the implementation status stage "In Planning" there are 16 questions, each of which is 8 questions at maturity level II, 5 questions at maturity level III, 2 questions at maturity level IV and 1 question at maturity level V. Application/Partially Applied” there are 8 questions with 2 questions at maturity level II, 4 questions at maturity level III and 1 question each for maturity levels IV and V. In the implementation status “Completely Implemented” there is 1 question at maturity level II and 2 questions at maturity level III.

4.F. Management of Information Security Assets

Table 7 Maturity Score in the Information Asset Management area (i)

Information	Score
Number of questions Stage 1	24
Number of questions Stage 2	10
Number of questions Stage 3	4
Min Score Limit for Deployment Stage 3 Scores	88
Total Score of Implementation Stages 1 & 2	72
Status Assessment Implementation Stage 3	Invalid
Maturity Level Score II	60
Maturity Level Minimum Score II	25
Maturity Level Achievement Score II	*62*
Status	I+
Maturity Level Score III	16
Maturity Level Validity III	No
Maturity Level Minimum Score III	35
Maturity Level Achievement Score III	50
Status	No

Table 8 Maturity scores in the Information Asset Management area (ii)

Deployment Status	**Maturity Level**				**Total**
	II	**III**	**IV**	**V**	
Is not done	4	3	0	0	7
In Planning	7	1	0	0	8
Under Application/Partially Applied	7	2	0	0	9
Completely Applied	9	3	0	0	12
Total	27	9	0	0	36

The completeness score obtained in the management of information assets is 76. Based on table 7 the number of questions in stage 1 is 24, then questions in stage 2 are 10 and 4 questions in stage 3 with a minimum score limit for implementation stage 3 which is 88 and a total score that obtained in stages 1 & 2 is 72, so the status in implementation 3 is "Invalid". the level II maturity score is worth 60 with a minimum score of 25 and the achievement score is worth 62 so that it is in the "I +" maturity status. Furthermore, the score for maturity level III is worth 16 with a validity value of "No" and a minimum score of 35 and an achievement score of 50 so that a "No" status is obtained.

Based on table 8 there are 7 questions at maturity level II and III which were not responded to or "Not Done" respectively 4 questions at maturity level II and 3 questions at maturity level III. At the implementation status stage "In Planning" there are 8 questions, 7 questions each at maturity level II, 1 question at maturity level III. while at the implementation status stage "In Application/Partially Applied" there are 9 questions with 7 questions at maturity level II, 2 questions at maturity level III. in the implementation status of "Completely Applied" there are 9 questions at maturity level II and 3 questions at maturity level III.

4.G. Information Security Technology

Table 9 Scores of the Information Technology and Security framework area (i)

Information	**Score**
Number of questions Stage 1	14
Number of questions Stage 2	10
Number of questions Stage 3	2
Min Score Limit for Deployment Stage 3 Scores	68
Total Score of Implementation Stages 1 & 2	56
Status Assessment Implementation Stage 3	Invalid
Maturity Level Score II	16
Maturity Level Minimum Score II	18
Maturity Level Achievement Score II	*28*
Status	No
Maturity Level Score III	40
Maturity Level Validity III	No
Maturity Level Minimum Score III	40
Maturity Level Achievement Score III	62
Status	No
Maturity Level Score IV	0
Maturity Level Validity IV	No
Maturity Level Minimum Score IV	6
Maturity Level Achievement Score IV	9
Status	No

Table 10 Scores of the Information Technology and Security framework area (ii)

Deployment Status	**Maturity Level**				**Total**
	II	**III**	**IV**	**V**	
Is not done	5	1	0	0	6
In Planning	3	4	1	0	8
Under Application/Partially Applied	5	2	0	0	6
Completely Applied	1	4	0	0	6
Total	14	11	1	0	26

The completeness score obtained from technology and information security is 56. Based on table 9 it can be seen that the number of questions in stage 1 is 14, then questions in stage 2 are 10 and 2 questions in stage 3 with a minimum score limit for implementation stage 3, namely 68 and the total score obtained in stages 1 & 2 is 56, so the status in application 3 is "Invalid". the level II maturity score is worth 16 with a minimum score of 18 and the achievement score is worth 28 so there is a maturity status of "No". For maturity level III scores are worth 40 with a validity value of "No" and a minimum score of 40 and an achievement score of 62 so that a "No" status is obtained. Furthermore, the IV Maturity score is 0, with "No" Validity.

Based on table 10, there are 6 questions at maturity level II and III which were not responded to or "Not Done" respectively 5 questions at maturity level II and 1 question at maturity level III. At the implementation status stage "In Planning" there are 8 questions, 3 questions each at maturity level II, 4 questions at maturity level III and 1 question at maturity level IV. while at the implementation status stage "In Application/Partially Applied" there are 6 questions with 4 questions at maturity level II, 2 questions at maturity level III. in the implementation status of "Completely Applied" there are 6 questions, 2 questions at maturity level II and 4 questions at maturity level III.

The following is the eligibility level for the 5 aspects based on the level of value validity.

Table 11 feasibility level for the 5 aspects based on the value validity level.

	Governance	**Management Risk**	**Framework Work**	**Management**	**Technology**

				Asset	Aspect
Level II					
Status	I+	No	I+	I+	No
Level III					
validity	No	No	No	No	No
Status	No	No	No	No	No
Level IV					
validity	No	No	No	No	No
Status	No	No	No	No	No
V level					
validity	No	No	No	No	No
Status	No	No	No	No	No
Final Status	I+	I	I+	I+	I
	2	1	2	2	1

Based on Table 11, it can be seen that the maturity status of the five Information Security areas can be seen that the governance and framework aspects are at level II with an “I+” value, for risk management and technology aspects at level II with a “No” status. then in the asset management aspect the status at level II is worth "I+". At maturity level III, IV and V in all aspects starting from Governance, Risk Management, Framework, Asset Management and Technology Aspects have a "No" validity. In this case, it can be seen that of the five aspects, no one has reached the minimum threshold of maturity level, while the minimum threshold for certification readiness is at the level of "III+".

Table 12 IBISA network traffic

Test Date	Working hours			Not working hours		
	Min	Max	Avg	Min	Max	Avg
7/04/2022	86.0	801.0	278.82	76.0	1351.0	286.11
8/04/2022	90.0	3217.0	392.77	80.0	1181.0	250.62
9/04/2022	84.0	1242.0	288.93	80.0	1901.0	282.77
10/04/2022	87.0	1247.0	288.01	67.0	2412.0	275.3
11/04/2022	66.0	830.0	275.16	76.0	1222.0	219.3
12/04/2022	79.0	689.0	220.63	75.0	6139.0	335.44
13/04/2022	67.0	6055.0	734.07	87.0	3337.0	296.66

Network development of this detection system begins with modeling normal conditions and observed networks, then proceed as exceptions. The advantage of an anomaly-based detection system is that it does not require in-depth malware knowledge and can detect attacks in the form of new malware. Meanwhile, the drawbacks of an anomaly-based detection system are not being able to know what type of attack is attacking the network and the high rate of false positives.

ManageEngine OpManager has the ability to observe network traffic. In this research, the next step is to monitor and collect data on the Purworejo IBISA network system. Monitoring and data collection on the IBISA Purworejo network was carried out for one week starting from April 7 2022 to April 13 2022, observations were made during working hours from 07.00 WIB to 17.00 WIB and during non-working hours from 17.00 WIB to 07.00 WIB.

The purpose of data collection is to analyze security and network conditions, by monitoring traffic changes on the network. From the observational data it has been found that network traffic conditions during working hours are greater than non-working hours.

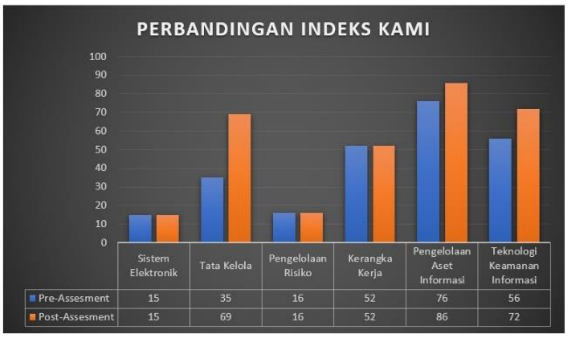


Figure 6Comparison of the WE Index Pre-Assessment and Post-Assessment IBISA Purworejo network

Based on Figure 6 it can be seen that the increase in the value of the Information Security Index (KAMI) is found in several aspects including: aspects of governance, management of information assets and information security technology which can be shown in the table below.

Table 13 Pre-Assessment of “Information Security Governance” Aspect

No	Information Security Governance Evaluation	Status	Points
1	Has the IBISA Purworejo Network implemented a socialization program and increased understanding of information security, including the importance of compliance for all parties involved?	In Application / Applied Part	2
2	Does the IBISA Purworejo Network implement competency and expertise improvement programs for officials and officers implementing information security management?	In Planning	2
3	Has the IBISA Purworejo Network integrated information security requirements/requirement	Is not done	0

	s into existing work processes?		
4	What are the conditions and problems of information security inIBISA Purworejobecome a consideration or part of the strategic decision-making process in your agency/company?	In planning	2
5	Has your IBISA Purworejo Network defined metrics, parameters and processesperformance measurement of information security management which includes the mechanism, measurement time, implementation, monitoring and reporting escalation?	Is not done	0
6	Has your IBISA Purworejo Network implemented an information security management performance appraisal program for the implementing individuals (officials & officers)?	Is not done	0
7	isIBISA Purworejohave implemented information security management targets and targets for various relevant areas, evaluated their achievements on a regular basis, implemented corrective measures to achieve existing targets, including reporting the status to the head of the agency/company?	Is not done	0

Table 14 Post-Assessment of "Information Security Governance" Aspect

No	Information Security Governance Evaluation	Status	Points
1	Has the IBISA Purworejo Network implemented a socialization program and increased understanding of information security, including the importance of compliance for all parties involved?	Applied Regularly Thorough	3
2	Does the IBISA Purworejo Network implement competency and expertise improvement programs for officials and officers implementing information security management?	Applied Regularly Thorough	6
3	Has the IBISA Purworejo Network integrated information security requirements/requirements into existing work processes?	Applied Regularly Thorough	6
4	What are the conditions and problems of information security inIBISA Purworejobecome a consideration or part of the strategic decision-making process in your agency/company?	In Deployment/Partially Applied	4
5	Has your IBISA Purworejo Network defined metrics, parameters and processesperformance measurement of information security management which includes the mechanism, measurement time, implementation, monitoring and reporting escalation?	In Deployment/Partially Applied	6
6	Has your IBISA Purworejo Network implemented an information security management performance appraisal program for the implementing individuals (officials & officers)?	Applied Regularly Thorough	9
7	isIBISA Purworejohave implemented information security management targets and targets for various relevant areas, evaluated their achievements on a regular basis, implemented corrective measures to achieve existing targets, including reporting the status to the head of the agency/company?	In Deployment/Partially Applied	6

Table 15 Pre-Assessment of "Information Asset Management" Aspect

No	Evaluation of Information Asset Management	Status	Points
1	Definition of individual information security responsibilities for all personnel at IBISA Purworejo	In Application / Applied Part	2
2	Procedures for destroying data/assets that are no longer needed	Is not done	0
3	Is there a process in place to check (inspect) and maintain: computer equipment, supporting facilities and job site security feasibility for placing important information assets?	In Planning	2
4	Is there a security mechanism in place for sending information assets (devices and documents) involving third parties?	In Application / Applied Part	4

Table 16 Post-Assessment of "Information Asset Management" Aspect

No	Evaluation of Information Asset Management	Status	Points
1	Definition of individual information security responsibilities for all personnel at IBISA Purworejo	Applied Regularly Thorough	3

2	Procedures for destroying data/assets that are no longer needed	In Planning	2
3	Is there a process in place to check (inspect) and maintain: computer equipment, supporting facilities and job site security feasibility for placing important information assets?	In Application / Applied Part	4
4	Is there a security mechanism in place for sending information assets (devices and documents) involving third parties?	Applied Regularly Thorough	6

Table 17 Pre-Assessment of "Information Technology and Security" Aspect

No	Information Technology and Security Evaluation	Status	Points
1	Is the operating system for each desktop and server device updated to the latest version?	In Application / Applied Part	2
2	Are networks, systems and applications used routinely scanned to identify possible vulnerabilities or configuration changes/intactness?	Is not done	0
3	isIBISA Purworejoroutinely analyze compliance with existing standard configuration implementations?	Is not done	0
4	Is the communication network segmented according to its interests (division of agencies/companies, application needs, special access points, etc.)?	Is not done	0
5	Is there a standard configuration for system security for all network assets, systems and applications, which is updated according to developments (industry standards that apply) and needs?	Is not done	0
6	Does the IBISA Purworejo Network implement a development and test environment that has been secured in accordance with existing technology platform standards and is used for the entire life cycle of the system being built?	Is not done	0
7	Does the IBISA Purworejo Network involve an independent party to review the reliability of information security on a regular basis?	In Planning	2
8	Are there reports of failed/successful virus/malware attacks followed up and resolved?	In Planning	2
9	Do all networks, systems and applications use an accurate time synchronization mechanism, according to existing standards?	In Planning	2

Table 18 Post-Assessment of "Information Technology and Security" Aspect

No	Information Technology and Security Evaluation	Status	Points
1	Is the operating system for each desktop and server device updated to the latest version?	In Application / Applied Part	3
2	Are networks, systems and applications used routinely scanned to identify possible vulnerabilities or configuration changes/intactness?	In Application / Applied Part	2
3	isIBISA Purworejoroutinely analyze compliance with existing standard configuration implementations?	In Planning	1

4	Is the communication network segmented according to its interests (division of agencies/companies, application needs, special access points, etc.)?	In Planning	1
5	Is there a standard configuration for system security for all network assets, systems and applications, which is updated according to developments (industry standards that apply) and needs?	In Planning	1
6	Does the IBISA Purworejo Network implement a development and test environment that has been secured in accordance with existing technology platform standards and is used for the entire life cycle of the system being built?	Is not done	6
7	Does the IBISA Purworejo Network involve an independent party to review the reliability of information security on a regular basis?	In Planning	6
8	Are there reports of failed/successful virus/malware attacks followed up and resolved?	In Planning	4
9	Do all networks, systems and applications use an accurate time synchronization mechanism, according to existing standards?	In Application / Applied Part	4

The results of the comparison above show that ManageEngine OpManangager can help increase the value or points for aspects of Technology in the Information Security Index (KAMI) but have no effect on other aspects. It can be seen that the value of our IBISA Purworejo network Index is 292 from the previous 235 points, this shows that the level of information security maturity that was previously when the Pre-assessment was at level I to I+ is now at level I to II when Post-assessment is done. However, the Governance aspect shows a change in value from 35 to 69, Information Asset Management shows a change in value from 76 to 86 and the Information Security Technology Aspect shows a change in value from 56 to 72.

5. CONCLUSIONS AND RECOMMENDATIONS

The level of maturity and integrity of the IBISA Purworejo network's information security is still low. the reason for the low integrity and maturity level of this information security is that the IBISA Purworejo Network has not fully implemented the information security requirements or is still in the planning stage. the use of ManageEngine OpMananager technology is proven to be able to increase the value of the Information Security Index (KAMI) on the IBISA Purworejo network in various aspects. Increasing values in various aspects cannot be separated from the role of using ManageEngine OpMananager technology in analyzing weaknesses and changes in the configuration of information assets on the IBISA Purworejo network. ManageEngine OpMananager can also carry out monitoring and process analysis of IBISA Purworejo's assets and network systematically. This means that information security on the IBISA Purworejo network is not feasible and needs a lot of improvement. Meanwhile, the maturity level for each area of information security is at level I to II. Then as a standard policy of ISO/IEC 27001:2018, the expected expiration date for the minimum threshold for certification readiness is at Level or maturity level III+.

Recommendations or suggestions for further research are to build awareness among PUSDATIN IBISA Purworejo staff regarding information security. Staff first realized the importance of protecting information security from all aspects related to information security in supporting network performance. The KAMI index is used at least once a year as a tool for reviewing information security readiness and evaluating the success of improvements that have been implemented by achieving a certain level of completeness or maturity.

BIBLIOGRAPHY

ADI REYNALDO, SENGKEY RIZAL, P. (2020) ‘Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI’, *Jurnal Teknik ...*, pp. 189–198. Available at: https://ejournal.unsrat.ac.id/index.php/informatika/article/view/31597.

ANGGA JUANSYAH, BAGUS PRATAMA, I. D. (2018) ‘Analisis dan implementasi open source security information managament (ossim) pada keamanan jaringan komputer pt. satria antaran prima palembang’. Available at: http://library.palcomtech.com/pdf/5621.pdf.

ARFANUDIN, C. *ET AL*. (2019) 'Analisis Serangan Router Dengan Security Information and Event Management (Siem) Dan Implikasinya Pada Indeks Analysis of Router Attack With Security Information and Event Management and Implications (Siem) in Information Security', 2(1), pp. 1–7.

DARWIS, D. AND SOLEHAH, N. Y. (2021) 'PENERAPAN FRAMEWORK COBIT 5 UNTUK AUDIT TATA KELOLA KEAMANAN INFORMASI PADA KANTOR WILAYAH KEMENTERIAN', 1(2), pp. 38–45.

DEWANTARA, R. AND SUGIANTORO, B. (2021) 'Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta)', *Jurnal Teknologi Informasi dan Ilmu Komputer*, 8(6), p. 1137. doi: 10.25126/jtiik.2021863123.

HERMAWAN, W. (2019) 'Perancangan Manajemen Risiko Keamanan Informasi pada Penyelenggara Sertifikasi Elektronik (PSrE)', *Jurnal Telekomunikasi dan Komputer*, 9(2), p. 129. doi: 10.22441/incomtech.v9i2.6474.

KAMAL, M. R. AND SETIAWAN, M. A. (2021) 'Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII', *Automata*, (4).

KORNELIA, A. AND IRAWAN, D. (2021) 'Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1', *Jurnal Pengembangan Sistem Informasi dan Informatika*, 2(2), pp. 78–86. doi: 10.47747/jpsii.v2i2.548.

KRISTANTO, T. *ET AL*. (2019) 'Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ', *JISA(Jurnal Informatika dan Sains)*, 2(2), pp. 30–33. doi: 10.31326/jisa.v2i2.497.

LENAWATI, M., WINARNO, W. W. AND AMBOROWATI, A. (2017) 'Tata Kelola Keamanan Informasi pada PDAM Menggunakan ISO/IEC 27001:2013 dan COBIT 5', *Sentra Penelitian Engineering dan Edukasi*, 9(1), pp. 44–49. Available at: http://speed.web.id/jurnal/index.php/speed/article/view/220.

NOFRY ARMAN, WIDHY HAYUHARDHIKA NUGRAHA PUTRA, A. R. (2019) '3. Tampilan Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI).pdf'.

PAMUNGKAS, W. C. AND SAPUTRA, F. T. (2020) 'Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013', *Jurnal Sistem Komputer dan Informatika (JSON)*, 1(2), p. 101. doi: 10.30865/json.v1i2.1924.

WIJATMOKO, T. E. (2020) 'Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy', *Cyber Security dan Forensik Digital*, 3(1), pp. 1–6. doi: 10.14421/csecurity.2020.3.1.1951.

WIJAYA, Y. D. (2021) 'Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) Iso/Iec 27001:2013', *Jurnal Sistem Informasi dan Informatika (Simika)*, 4(2), pp. 115–130. doi: 10.47080/simika.v4i2.1178.

YAUMA DZIKRI IMANY, WIDHY HAYUHARDIKA NUGRAHA PUTRA, ADMAJA D. H. (2019) 'Tampilan Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia).pdf'.

YUNELLA, DWI HERLAMBANG, NUGRAHA PUTRA, M. (2019) 'Tampilan Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI.pdf'.