ISSN: 0974-5823 Vol. 7 No. 2 February, 2022

International Journal of Mechanical Engineering

Evaluation of the Readiness Level of Information System Security at the BAKAMLA Using the KAMI Index based on ISO 27001:2013

Peik Sugiarto

Fakultas Teknik Elektro, Univeristas Indonesia

Yohan Suryanto

Fakultas Teknik Elektro, Univeristas Indonesia

Abstract - Data, particularly security and safety data possessed by an agency, becomes very critical information that requires specific protection to ensure its security. To ensure data confidentiality, integrity, and availability, it is required to assess the security of information controlled by Bakamla. The KAMI index is a tool developed by BSSN to help agencies assess the maturity of their information system security. The KAMI Index is used to analyze the maturity level of information system security at Bakamla. Based on the assessment of the KAMI Index that has been carried out on the Information System at Bakamla, the result is Not Eligible. Therefore, actions based on certain standards are needed, one of which is ISO 27001:2013.

INTRODUCTION

Globalization era, in which everyone can easily get information anywhere and anytime, has made information very important for some people or agencies. Information is a very valuable asset for companies to be protected. Thus, many companies are willing to invest their money to secure the information they have. Furthermore, information requires information security in the data exchange process. Information security consists of some steps taken to secure the information from the sender, transfer process, and received by the recipient. It is important for government agencies to maintain information security in order to increase public trust in the information. Many things can cause the vulnerability of information security, one of which is our less concerned behavior dealing with information. This is because the biggest gap in information security is an awareness of the information confidentiality. Many cases of data breaches are due to the negligence of the information owner.

As listed in the Web Defacement Incident Recapitulation report book issued by the National Cyber and Encryption Agency (hereinafter called as BSSN), Indonesia has seen more than 88 million attacks from January to April 2020[1]. This is in line with the Ministry of Communication and Informatics (hereinafter called as Kominfo), stating that Indonesia is ranked third in the world's cyber-attack destination. One of the destinations attacked is a government agency. Recently, data leaks presenting more than 270 million members of the Health Care and Social Security Agency (BPJS) shocked the internet. The attacks aimed at government agencies raised since the government agencies are less aware of the impact of these attacks and lack of human resources who understand how to deal with cyber-attacks.

The Maritime Security Agency (hereinafter called Bakamla) of the Republic of Indonesia is an agency established to carry out security and safety patrols in Indonesian waters. To get their duties and functions done, Bakamla has a network that uses a Virtual Private Network (VPN) as well as other activities used by network users. The quality of data information security at Bakamla needs to be improved to ensure Confidentiality, Integrity, Availability.

The readiness level of information security at Bakamla must be measured so that the evaluation process becomes more effective and efficient. Therefore, this study examines the maturity level of information security at Bakamla and evaluate and provide recommendations to improve the quality of information security at Bakamla. .

REVIEW OF RELATED LITERATURE

This study discusses the readiness level of information system security designed by Bakamla in order to support its duties and functions as an agency that carries out security patrols. Furthermore, this study mainly discusses about Bakamla, Information, Information Security, and the KAMI Index.

2.1. Information

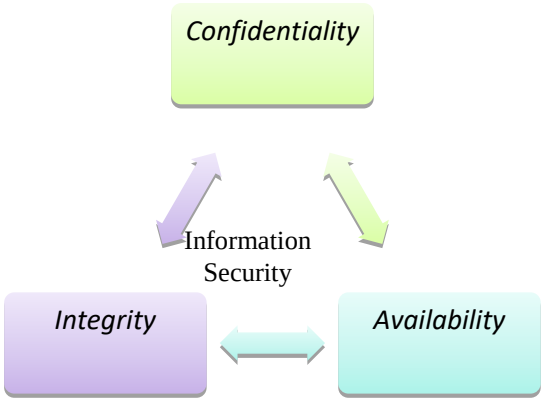
Information is the whole meaning that has been processed and arranged so that it can provide a certain understanding. In other words, information is a collection of data that has certain meanings and benefits and has gone through a filtering process. The information provided must have benefits for a person or some people. Therefore, information is very useful for someone in making choices or for leaders in making policies. The information obtained by the leaders greatly affects the policies that will be

taken. If the information obtained is wrong, it is very likely that the policies taken are wrong. The nature of information varies from ordinary to confidential. Ordinary information can be known by anyone who wants to know the information, while confidential information can only be known by specific recipients

Extra security is needed to maintain the confidentiality of the information, so that the information is only known to the rightful recipient. If the confidential information can be read or known by people other than the recipient, the information is no longer confidential and can be misused by unauthorized persons. Therefore, it is necessary to secure information to maintain the confidentiality, availability, and integrity of information.

2.2. Information Security

The increasing number of cybercrimes that attack victims to get the important information has made companies or agencies take extra security for the information they have. The purpose of securing the information is to maintain the aspects of confidentiality, integrity, and availability.



Confidentiality is an important aspect in maintaining information security. Confidentiality of data or information ensures that the data or information is accessed by the authorities. Integrity is an aspect to maintain the authenticity and integrity of data or information from unauthorized parties. This aspect ensures that the data is not modified by unauthorized persons. Meanwhile, availability aspect ensures that data can be accessed whenever needed by anyone who has access rights to the data.

2.3. KAMI Index

BSSN issued a guideline to evaluate and conduct an assessment of the readiness to implement information security which refers to SNI ISO/IEC 27001. Furthermore, BSSN state that the KAMI Index conducts an assessment to find out the readiness level of information security owned by a company or agency. However, it does not serve as a measuring tool to assess the effectiveness of information security. The KAMI Index assesses Governance, Frameworks, Asset Management, Third-party Technology Aspects, Cloud Service Security, and Personal Data Protection (PDP)[1].

2.4. ISO 27001

The International for Standardization (ISO) is a body engaged in standardization to develop and promote the quality, safety, and efficiency of a product. ISO is used in companies or agencies to conduct global competition. The companies that already have ISO certification indicate that the agency is better than those without ISO certification. ISO issues various standardizations, one of which is standardization in the field of information security, i.e., ISO 27001 on information security management systems. ISO 27001 is used to assist companies or agencies in the development and maintenance of an Information Security Management System (ISMS).

ISO 27001:2013 is one part of ISO 27001 which focuses on ISMS. ISO 27001:2013 is used to improve and maintain the ISMS in a company or agency. ISMS is a system used to manage and control security risks so that information security aspects of confidentiality, integrity and availability are maintained properly.

2.5. Previous Related Literature

KAMI Index as a tool to determine the level of security readiness in the agency or company has been discussed in previous research. Sensuse, et al. [2] used the KAMI Index to determine the level of information security readiness from the Meteorology, Climatology, and Geophysics Agency (BMKG). The result of this assessment shows that BMKG is at “need improvement” or level 2. Thus, they recommended several steps to be followed up to increase the readiness level of information security.

Nabila et al [4] evaluated information security at the Communication and Information Office of Malang Regency using the KAMI Index. They proposed 17 recommendations on governance, 16 recommendations on risk management, 27 recommendations on frameworks, 31 recommendations on asset management, 6 recommendations on technology and information security, and 9 recommendations on supplements. Those recommendations were proposed to the Communication and Information Office of Malang Regency to be equipped to implement information security.

RESEARCH METHOD

his study uses the KAMI Index in evaluating the level of information security readiness in Bakamla. The first step is to identify the problem, aiming to register all existing problems and analyze them to find a solution. The second step is literature study, aiming to increase the research and information about the research conducted. The next step is data collection using interviews with those who are in charge for information security at Bakamla. After that, the collected data are analyze to draw conclusions and become the basis for recommendations for increasing the level of information security readiness at Bakamla.

RESULT AND DISCUSSION

This section will discuss the results of the assessment of the readiness level of information security at Bakamla using the KAMI Index 4.0. The assessment results become the basis for analysis and recommendations to increase the readiness level of information security at Bakamla.

4.1. Category of Electronic System at Bakamla

The Electronic Systems at Bakamla are categorized based on an assessment using the KAMI Index 4.0. In this assessment, there are 10 questions related to the Electronic System at the agency and the result of this assessment is the LOW, HIGH, STRATEGY category.

Part I: Category of Electronic System		
This section evaluates the level or category of the electronic system used		
[Electronic System Category]Low; Tall; Strategic		**Status**
#	**Characteristics Agency/Company**	
1.8	The level of criticality of the existing processes in the Electronic System, relative to the threat of attempted attacks or breaches of information security [A] Processes that pose a risk of disrupting the lives of many people and have a direct impact on public services [B] Processes that risk disrupting the lives of many people and have an impact indirect [C] Processes that only impact the company's business	B
1.9	Impact of the failure of the Electronic System [A] Unavailability of public services on a national scale or endangering national security and defense [B] Unavailability of public services in 1 or more provinces [C] Unavailability of public services in 1 district/city or more	A
1.10	Potential loss or negative impact from incidents of breach of Electronic System information security (sabotage, terrorism) [A] Causing fatalities [B] Limited to financial losses [C] Causing temporary operational disruptions (no harm and result in financial losses)	B
	Electronic System Category determination score	**23**
	Addiction Level	**High**

Figure 4.1

The assessment results of the Electronic System category at Bakamla

Figure 4.1 shows the results of the assessment that has been carried out on the Bakamla Electronic System. The Bakamla Electronic System scored 17 and was categorized as High. This can be interpreted that the electronic systems at Bakamla are part of Bakamla's business processes. The assessment results are categorized as High for several reasons, including: the impact of a system failure will have an impact on a national scale; the investment value and maintenance costs are quite expensive; it has compliance with certain standards, etc.

Based on the category of Electronic Systems in Bakamla, a score of 536 is needed from the 7 categories contained in the KAMI Index assessment to get the good category.

4.2. Information Security Governance

The assessment in the field of information security governance aims to evaluate the readiness of agency governance and the responsibilities of information security managers

Part II: Information Security Governance				
This section evaluates the readiness of the form of information security governance along with the agencies/companies/functions, duties and responsibilities of information security managers.				
[Evaluation]Is not done; In Planning; Under Application or Partially Applied; Completely Applied				**Status**
#			**Information Security Function/Organization**	
2.1	II	1	Is the head of your agency/company in principle and officially responsible for the implementation of information security programs (eg those listed in the ITSP), including the determination of related policies?	In Planning
2.2	II	1	Does your agency/company have functions or sections that specifically have duties and responsibilities to manage information security and maintain compliance?	In Planning
2.3	II	1	Do the information security implementing officers/officers have the appropriate authority to implement and ensure compliance with the information security program?	In Planning
2.4	II	1	Is the person in charge of information security implementation given the appropriate allocation of resources to manage and ensure compliance with the information security program?	In Implementation / Partially Applied
2.5	II	1	Is the role of implementing information security that covers all requirements mapped out completely, including internal audit needs and authority segregation requirements?	In Planning
2.6	II	1	Has your agency/company defined the requirements/standards of competence and expertise for implementing information security management?	Is not done
2.7	II	1	Do all information security implementers in your agency/company have adequate competence and expertise in accordance with applicable requirements/standards?	In Planning
2.8	II	1	Has your agency/company implemented a socialization and awareness-raising program for information security, including its compliance interests for all related parties?	In Planning

Figure 4.2

The assessment results of the Information Security Governance at Bakamla

Figure 4.2 shows the Information Security Governance assessment at Bakamla uses 18 points of the KAMI index which include the implementation of stage 1 and stage 2. To implement stage 3, the minimum score is 48; therefore, Bakamla cannot yet implement stage 3.

4.3. Information Security Risk Management

The next assessment is Information Security Risk Management.

Part III: Information Security Risk Management					
This section evaluates the readiness to implement information security risk management as the basis for implementing an information security strate					
[Evaluation]Is not done; In Planning; Under Application or Partially Applied; Completely Applied					Status
#			Information Security Risk Assessment		
3.1	II	1	Does your agency/company have an information security risk management work program that is documented and officially used?		In Planning
3.2	II	1	Has your agency/company determined the person in charge of risk management and the escalation of reporting the status of information security risk management to the leadership level?		In Implementation / Partially Applied
3.3	II	1	Does your agency/company have a documented and officially used information security risk management framework?		In Planning
3.4	II	1	Does this risk management framework include definitions and relationships between the level of classification of information assets, the level of threat, the likelihood of the threat occurring and the impact of losses on your agency/company?		In Planning
3.5	II	1	Has your agency/company set a threshold level of acceptable risk?		In Planning
3.6	II	1	Has your agency/company defined ownership and management? *(custodian)* existing information assets, including key/critical assets and the key work processes that use these assets?		In Planning
3.7	II	1	Have the threats and weaknesses related to information assets, particularly for each key asset identified?		In Planning
3.8	II	1	Has the impact of losses related to the loss/disruption of the function of the main asset been determined according to the existing definition?		In Planning

Figure 4.3

The assessment results of information security risk management at Bakamla

Bakamla got a score of 10 from the scores of stages 1 and 2. To carry out an assessment in stage 3, a minimum score is 36. The results of this assessment are very small because almost all aspects of information security risk management in Bakamla are still in planning stage.

4.4. Information Security Management Framework

The next assessment is the Information Security Management Framework at Bakamla.

Part IV: Information Security Management Framework				
This section evaluates the completeness and readiness of the information security management framework (policies & procedures) and implementa				
[Evaluation]Is not done; In Planning; Under Application or Partially Applied; Completely Applied				Status
#			Formulation and Management of Information Security Policies & Procedures	
4.5	II	1	Do all existing information security policies and procedures reflect the need for mitigation from the results of the information security risk assessment, as well as certain objectives/objectives set by the head of the agency/company?	In Planning
4.6	II	1	Is there a process in place to identify conditions that jeopardize information security and designate them as information security incidents to be followed up according to the procedures in place?	In Planning
4.7	II	1	Are information security aspects that include incident reporting, maintaining confidentiality, intellectual property rights, rules for the use and security of ICT assets and services included in contracts with third parties?	In Planning
4.8	II	2	Are the consequences of violating the information security policy defined, communicated and enforced?	In Planning
4.9	II	2	Are there formal procedures in place to manage an exception to an information security application, including a process for following up on the consequences of this situation?	In Planning
4.10	III	2	Has your organization implemented operational policies and procedures to manage implementation? *security patches*, allocation responsibility for monitoring releases *security patches* new, confirming its installation and reporting it?	Is not done
4.11	III	2	Has your organization addressed the information security aspects of project management related to scope?	In Implementation / Partially Applied

Figure 4.4

The assessment results of the information security management framework at Bakamla.

From the minimum assessment in stage 3, namely 64, Bakamla got a score of 35 in the assessment of Information Security Management Framework. The low score is because the policies with great score that are still in planning stage.

4.5. Information Asset Management

The next assessment is information asset management

Part V: Information Asset Management				
This section evaluates the completeness of securing information assets, including the entire life cycle of those assets.				
[Evaluation]Is not done; In Planning; Under Application or Partially Applied; Completely Applied				Status
#			Information Asset Management	
5.3 1	II	1	Is the installed computing infrastructure protected against power supply interruptions or the impact of lightning?	In Implementation / Partially Applied
5.3 2	II	1	Are there regulations for securing computing devices belonging to your agency/company when used outside the official work location (office)?	In Planning
5.3 3	II	1	Is there a process in place for moving ICT assets (software, hardware, data/information etc) from a defined location (including updating their location in the inventory list)?	In Planning
5.3 4	II	2	Is the construction of the storage room for critical information processing equipment using designs and materials that can cope with the risk of fire and equipped with supporting facilities (fire/smoke detection, fire extinguishing, temperature and humidity control) that are	In Implementation / Partially Applied
5.3 5	II	2	Is there a process in place to check (inspection) and maintain: computer equipment, supporting facilities and the appropriateness of job site security to place critical information	In Planning
5.3 6	II	2	Is there a security mechanism in place for the delivery of information assets (devices and documents) involving third parties?	In Implementation / Partially Applied
5.3 7	II	2	Are there regulations in place to secure critical work sites (server rooms, archive rooms) from the risk of devices or materials that could harm the information assets (including information processing facilities) located on them? (eg prohibition of using mobile phones in the server room, using cameras etc.)	In Planning
5.3 8	III	3	Is there a process in place to secure the work location from the presence/presence of third parties working for the benefit of your agency/company?	Is not done

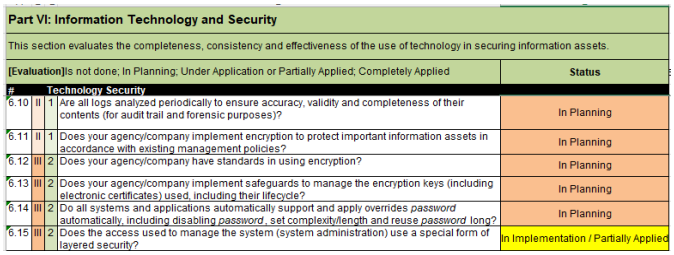
Figure 4.5

The assessment results of information asset management at Bakamla

The assessment results show the management of information assets at Bakamla stages 1 and 2 got a score of 57. This is still not enough to carry out the stage 3 requiring a minimum score of 88. The low score of asset management at Bakamla is because the lack of documentation or proper asset inventory.

4.6. Information Technology and Security

The next assessment is in the category of technology and information security.



Part VI: Information Technology and Security				
This section evaluates the completeness, consistency and effectiveness of the use of technology in securing information assets.				
[Evaluation]Is not done; In Planning; Under Application or Partially Applied; Completely Applied				Status
#			Technology Security	
6.10	II	1	Are all logs analyzed periodically to ensure accuracy, validity and completeness of their contents (for audit trail and forensic purposes)?	In Planning
6.11	II	1	Does your agency/company implement encryption to protect important information assets in accordance with existing management policies?	In Planning
6.12	III	2	Does your agency/company have standards in using encryption?	In Planning
6.13	III	2	Does your agency/company implement safeguards to manage the encryption keys (including electronic certificates) used, including their lifecycle?	In Planning
6.14	III	2	Do all systems and applications automatically support and apply overrides *password* automatically, including disabling *password*, set complexity/length and reuse *password* long?	In Planning
6.15	III	2	Does the access used to manage the system (system administration) use a special form of layered security?	In Implementation / Partially Applied

Figure 4.6

The assessment results of technology and information security at Bakamla

Figure 4.6 shows the Technology and Security at Bakamla got a score of 44 points which include the implementation of stage 1 and stage 2. This is still not enough to carry out the stage 3 requiring a minimum score of 68.

4.7. Assessment Result of the KAMI Index

This section explains the final assessment results of the readiness level of information security at Bakamla using the KAMI Index 4.0.

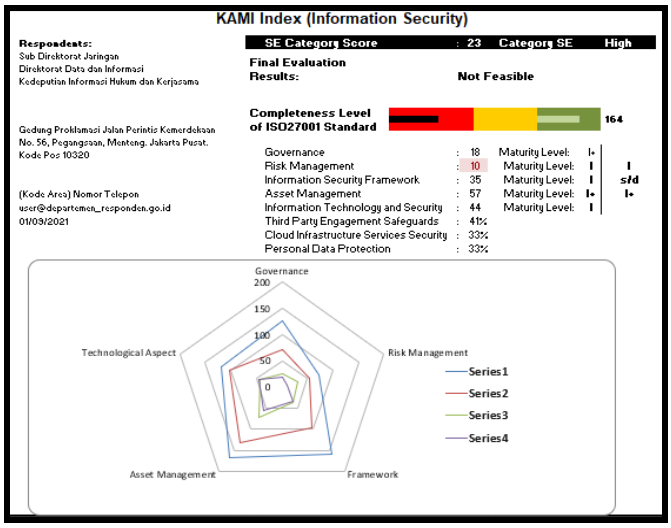


Figure 4.7

Final results of the KAMI Index assessment

Figure 4.7 shows the final results of the KAMI Index assessment carried out to determine the readiness level of information security at Bakamla. In this case, Bakamla got the final score of the KAMI Index assessment of 164, which is included in the Ineligible category. The Governance and Asset Management category is at Readiness Level I+, while the others are at Readiness Level I.

RECOMMENDATIONS BASED ON ISO 27001:2013

After getting the assessment results of the KAMI Index and knowing the score of each category in the KAMI Index, the next step is making recommendations for improvement based on ISO 27001:2013 to the not good categories. The following are recommendations given to agencies in order to increase the readiness level of Information System Security at Bakamla:

NO	Question	Status	Score
2.6	Has your agency/company defined the requirements/standards of competence and expertise for implementing information security management?	Not implemented	0
Suggested Improvements based on ISO 27001:2013			

Control A.7.2.2: Information security awareness, education, and training.

Bakamla must issues policies related to awareness about information system security to avoid existing threats. The division appointed as the party responsible for information system security must ensure that all employees comply with existing policies. In addition, from the employee's perspective, they must be given responsibilities for their position. The following methods can be done to build the responsibility of each employee:

- conducting training on security awareness
- punishing the employees who violate the policies
- mentioning the information system security in the employment contract.

2.11	Has your agency/company identified personal data used in the work process and implemented security in accordance with applicable laws and regulations?	Not implemented	0

Suggested Improvements based on ISO 27001:2013

Control A.6.1.1 : Information security roles and responsibilities.

In order to maintain the security of information systems in the agency, it is advisable to perform a functional separation and the duties of each employee must be explained.

Control A.18.1.4: Privacy and protection of personal identifiable information

Making a policy on the protection of personal data is very important because it covers personal information. In addition, Bakamla must socialize the importance of personal data and how to secure the data to all employees. There should be also a division or person who is responsible for securing information systems at Bakamla.

NO	Question	Status	Score
3.9	Has your agency/company implemented a structured information security risk analysis/study initiative on existing information assets (to be used later in identifying mitigation or countermeasures that are part of the information security management program)?	Not implemented	0

Suggested Improvements based on ISO 27001:2013

Control A.16.1.1: responsibility and procedure:

Bakamla must implement SOPs related to handling information system security to ensure a fast response to disturbances or attacks effectively. Bakamla must establish a mechanism for handling information security incidents and report to the supervisor who is responsible for it. The report must include information about the weaknesses of the system affected by the incident because the report will be used to conduct an assessment and decision making on the incident. Handling of incidents must be in accordance with existing procedures and gathering evidence.

The mechanism must include competent executors in dealing with problems related to information security disturbances. The team and management must agree on the objectives of managing information security incidents. In addition, the employees who are responsible for handling information security incidents understand the organization's priorities for dealing with information security incidents.

NO	Question	Status	Score
4.10	Has your organization implemented policies and operational procedures to manage implementation of security patches, allocate responsibility for monitoring new security patch releases, ensure installation and report them?	Not implemented	0

Suggested Improvements based on ISO 27001:2013

Control A.14.1.1: Analysis and specification of information security requirements**.**

Bakamla must establish rules and procedures regarding information system security on new systems and existing systems. This aims to simplify the process of updating security patches on a regular and structured basis and reporting to the supervisor on a regular basis.

CONCLUSION

Based on the assessment results of the readiness level of information system security at Bakamla using the KAMI Index, it can be concluded that:

1. Bakamla Electronic System got a score of 17, meaning in the High category. It can be interpreted that the electronic systems at Bakamla are part of Bakamla's business processes.
2. The readiness level of information system at Bakamla is still low because Bakamla has not implemented all the required steps and is still in planning stage. In addition, there are several questions that have not been carried out. It can be seen from the results of the KAMI Index dashboard, in which the security of Bakamla's information system got a score of 164, meaning in the Infeasible category. From the assessment results, information system security at Bakamla needs improvement in 5 categories.
3. Of the 5 categories of assessment, Bakamla got the Readiness Level I+ in the Governance and Asset Management category. Meanwhile, for the Risk Management, Management Framework, and Information Security Technology categories, Bakamla got the Readiness Level I.
4. The recommendations refer to ISO 27001:2013 based on the assessment results of the KAMI Index to the information system security at Bakamla.
5. It is suggested to take into action the recommendations based on ISO 27001:2013 and carry out ISO certification to increase the readiness level of information system security at Bakamla.

REFERENSI

[1] Komunikasi Publik, Biro Hukum dan Hubungan Masyarakat – BSSN. https://bssn.go.id/indeks-kami/

[2] D. I. Sensuse, M. Syarif, H. Suprapto, R. Wirawan, D. Satria and Y. Normandia, "Information security evaluation using KAMI index for security improvement in BMKG," 2017 5th International Conference on Cyber and IT Service Management (CITSM), 2017, pp. 1-4.

[3] Wijaya, Yahya Dwi. "EVALUASI KEMANANAN SISTEM INFORMASI PASDEAL BERDASARKAN INDEKS KEAMANAN INFORMASI (KAMI) ISO/IEC 27001: 2013." Jurnal Sistem Informasi Dan Informatika (Simika) 4.2 (2021): 115-130.

[4] Ramadhani, Nabilla Diva, Widhy Hayuhardhika Nugraha Putra, and Admaja Dwi Herlambang. "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi)." Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN 2548 (2020):

[5] Firzah A Basyarahil, Hanim Maria Astuti, dan Bekti Cahyo Hidayanto, *"Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya"* JURNAL TEKNIK ITS Vol. 6, No. 1, (2017) ISSN: 2337-3539 (2301-9271 Print*).*

[6] M. Rizal and Y. G. Sucahyo*, "A Study on the reparedness of Information Security Framework Area based on the Assessment of Information Security Index in Ministry of XYZ,"* in ICACSIS 2013, 2013, no. March, pp. 978–979.

[7] Sensuse, DI, Syarif, M, Suprapto, H, Wirawan, R, Satria, D & Normandia, Y*, "Information security evaluation using KAMI index for security improvement in BMKG".* in 2017 5th International Conference on Cyber and IT Service Management, CITSM 2017.

[8] Manullang, Astri & Candiwan, Candiwan & Harsono, Listyo. *"Asesmen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Institusi XYZ".* Journal of Information Engineering and Educational Technology. 1. 73. 10.26740/jieet.v1n2.p73-82.

[9] Pratama, E., Suprapto, S., & Perdanakusuma, A. "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur)". Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, 2(11), 5911-5920.

\