Information Security Index (ISI) 4.2 for Information Security Evaluation (Case Study: Sleman Regency Communication and Informatics Office)

Herry Sofyan*, Wilis Kaswidjanti, and Luqiyyatus Shoubatil Ilmiyah

Department of Informatics, Universitas Pembangunan Nasional "Veteran Yogyakarta", Yogyakarta, 55281, Indonesia
herry.s@upnyk.ac.id

Abstract. This research aims to provide an overview of the current conditions related to the readiness (completeness and maturity) of information security and ensure information security is in accordance with applicable standards and can find out what should be improved in information security from various fields that will be made reports to agency leaders. Evaluation of Information Security using the Information Security Index (KAMI) 4.2 with criteria in SNI ISO / IEC 27001: 2013 in six areas namely governance, risk management, framework, asset management, technology and information security, and supplements. The evaluation results of the Sleman Regency Communication and Information Technology Office received a Good status with a final score of 622 and a maturity level of IV. The final results of the evaluation explain that the Sleman Regency Communication and Information Technology Office has a "Managed and Measurable" status and can already carry out Information Security Index (KAMI) certification, especially ISO / IEC 27001: 2013 certification. All aspects have a high score, only a few aspects that only need a little improvement, namely in the Governance Area and the Supplementary Area by using the completeness of the ISO / IEC 27001: 2013 and ISO / IEC 27002: 2013 standards in practice. This research focuses on evaluating the readiness (Completeness and Maturity) of information security by implementing the KAMI index version 4.2, but implemented in different case studies and providing recommendations for improvement based on the ISO / IEC 27001: 2013 information security policy standard and the ISO / IEC 27002 information security practice standard.

Keywords: Evaluation, Information Security, Information Security Index (KAMI) 4.2, ISO/IEC 27001:2013, ISO/IEC 27002:2013.

1 Background

Information security evaluation is needed for organizations amid the growing information security threats today, so it is important for organizations to be able to evaluate the level of security needed and find existing vulnerabilities [2]. Information itself is referred to as a valuable asset that has more value and can be used as a competitive

A. Putro Suryotomo and H. Cahya Rustamaji (eds.), *Proceedings of the 2023 1st International Conference on Advanced Informatics and Intelligent Information Systems (ICAI3S 2023)*,
Advances in Intelligent Systems Research 181,
https://doi.org/10.2991/978-94-6463-366-5_18

advantage for an organization [11]. The level of security needed to protect the main information technology assets of the company/organization will be well defined if the necessary resources related to this can be thoroughly analyzed in an information security readiness evaluation [3]. The Communication and Informatics Service of Sleman Regency has implemented a program, namely Smart City, which aims to improve services through IT-based technology, which at this time the Sleman Regency Communication and Informatics Service will and always re-integrate all public services, one of which is organizing e-government, which provides information and services for citizens ranging from business affairs to government affairs, so as to help run the government system more efficiently. In addition, there is a government program called the Electronic-Based Government System (SPBE). SPBE itself is integrated with all Regional Government Organizations (OPD). So that it makes it easier to find the data needed. The risk of data loss or leakage of valuable information is very likely to occur. Therefore, high information security is needed.

Regarding the importance of information security on the risk of data loss or information leakage, the Ministry of Communication and Informatics issued the Regulation of the Minister of Communication and Informatics of the Republic of Indonesia Number 4 of 2016 (Minister of Communication and Informatics, 2016), concerning Information Security Management Systems (SMKI) stating that every electronic system operator must secure information with ISO / IEC 27001 standard, it is also stated that electronic systems that have been operating must have an Information Security Management System Certificate within a period of no later than two years [7]. Referring to the Regulation of the Minister of Communication and Information Technology of the Republic of Indonesia Number 4 of 2016 concerning Information Security Management Systems in Chapter III article 7 (Minister of Communication and Information Technology, 2016), that there is a standardized tool set, namely the Information Security Index (KAMI) [6]. Information security index (KAMI) is an evaluation tool to analyze and evaluate the level of readiness (completeness and maturity) of information security implementation in an agency with criteria in SNI ISO/IEC 27001: 2013 in six areas, namely governance, risk management, framework, asset management, technology and information security, and supplements. When conducting initial interviews with the Sub-Coordinator of the Data Center Management of the Sleman Regency Communication and Informatics Office, Mr. Edi Haryanto, S.Kom, has not yet certified using the Information Security Index (KAMI) which refers to ISO / IEC 27001: 2013. Therefore, the purpose of this research is to provide information about the condition of readiness (completeness and maturity) of the information security framework to ensure information security is in accordance with applicable standards and can find out what should be improved in information security from various fields based on the control of international security standards ISO / IEC 27001: 2013 [4]. Thus, the method chosen in this research is the Information Security Index (KAMI) built by the Ministry of Communication and Information Technology of the Republic of Indonesia. Based on these research problems, this research focuses on evaluating the readiness (Completeness and Maturity) of information security by implementing the KAMI index at the Sleman Regency Communication and Information Technology Office, therefore, the title of this research is "Evaluation of Information security Using the Information Security Index

(KAMI) 4.2 (Case study: Sleman Regency Communication and Information Technology Office)".

2 Literature Review

There are several references used in supporting this research related to information security. One of them is research conducted by Pratiwi, H. A. and Wulandari, L., 2021. The method used uses the KAMI index version 4.0. This research does not provide recommendations based on ISO / IEC 27002: 2013 controls. The results of the electronic system evaluation obtained a score of 35 and were included in the Strategic Category. The evaluation results of the five areas of information security obtained a total score of 395 at the Basic Framework stage with Maturity levels I to II and have not been able to carry out SNI 27001 certification [8]. Evaluation is the process of determining the value of a thing or object based on certain references to determine certain objectives [10]. This assessment can be neutral, positive or negative or a combination of both. When something is evaluated, it will usually be followed by decision making on the object being evaluated. Information security is an effort to secure information assets against threats that may arise. So that information security can indirectly ensure business continuity, reduce risks that occur, optimize return on investment [9]. KAMI (Information Security) Index 4.2 is an evaluation tool to analyze the level of readiness of information security in government agencies. This evaluation tool is not intended to analyze the feasibility or effectiveness of existing forms of security, but rather as a tool to provide an overview of the state of readiness (completeness and maturity) of the information security framework to agency leaders. In addition to assisting evaluation, the KAMI Index also helps analyze similarities with aspects in the SNI ISO/IEC 27001: 2013 standard guidelines. [1].

ISO/IEC 27001: 2013 is a specific method related to information security standardization that has been recognized by the whole world. ISO/IEC 27001: 2013 consists of characteristics in the form of security controls that must be implemented by an institution to develop an Information Security Management System (ISMS) (Ministry of Communication and Information Technology, 2017). The SMKI has the task of maintaining confidentiality, information availability, and integrity by implementing risk management in terms of the process and ensuring that the risk is adequately managed to the authorized party.

The areas contained in the Information Security Index (KAMI Index) are entirely based on aspects contained in the ISO/IEC 27001:2013 standard by summarizing 14 control areas related to information security specifically in Annex A of ISO/IEC 27001:2013 which is depicted in Table 1.

Table 1. Relevance of ISO/IEC 27001:2013 and KAMI Index version 4.2.

ISO/IES 27001: 2013	Governance	Risk Management	Framework	Assets Management	Technology	Supplement
Information Security Policies	✓	✓	✓			✓
Organisation of Information Security	✓	✓	✓			
Human Resource Security	✓		✓	✓		✓
Asset Management				✓		✓
Access Control				✓		✓
Cryptography				✓		✓
Physical & Environmental Security				✓		
Operation Security			✓	✓	✓	✓
Communications Security	✓		✓	✓	✓	✓
System Acquisition, Development &			✓	✓	✓	
Supplier Relationships				✓		
Information Security Incident	✓	✓	✓	✓	✓	✓
Information Security Aspects of Business Continuity Management	✓	✓	✓		✓	✓
Compliance	✓	✓	✓	✓	✓	✓

The controls contained in the ISO / IEC 27001: 2013 standard are summarized and absorbed by the KAMI Information Security Index, therefore every point contained in the KAMI index = Information Security Index is certainly related to the controls of ISO / IEC 27001: 2013, and the provision of recommendations in this study is based on the relationship between the KAMI Index = Information Security Index and the ISO / IEC 27001: 2013 standard, which consists of controls A.5 - A.18, which amount to 114 controls in 14 security aspect areas and also recommendations for this study are complemented by controls that are more inclined to the practice or implementation of information security management, namely ISO / IEC 27002: 2013 [5].

3 Method and Design

The methodology is the stages or flow that will be used to conduct research at the Sleman Regency Communication and Information Service. This methodology makes the research done more structured and directed. The flow of the research method that

will be carried out in research on information security evaluation at the Sleman Regency Communication and Informatics Office. Details of the research stages, as presented in figure 1.

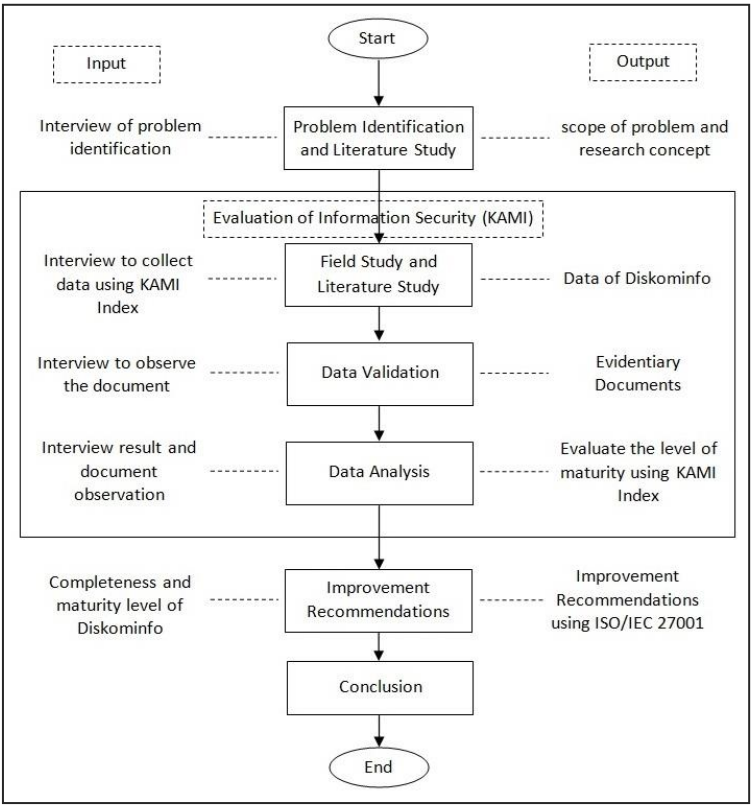

Figure 1. Research Methodology.

The explanation of the flow of research methods in figure 1:

Stage 1: Problem Identification and Literature Study. At this stage, a literature study is carried out first by searching and reading books, research journals, and related papers, so as to obtain a method that is suitable for conducting evaluations, namely the Information Security Index (US) method which refers to the ISO / IEC 27001: 2013 information security management standard. After obtaining the research method, the first interview was conducted to find out the state of the object and the security of the information system in the object of research, where the interview was conducted to the section responsible for managing information security at the Sleman Regency Communication and Information Technology Office.

Stage 2: Collecting data. After obtaining a suitable assessment model, filling out the KAMI Information Security Index 4.2 questionnaire by interviewing the section that holds the responsibility for information security in the Sleman Regency Communication and Information Technology Office government agency.

Stage 3: Data validation. After obtaining data information, the second interview was conducted based on the instrument for filling out the KAMI Information Security Index 4.2 questionnaire conducted by the relevant officials and also this second interview aims to ask whether or not there is evidence documentation of the results of the answers to the KAMI Information Security Index 4.2. Then make data observations and documentation to serve as evidence of filling in each of the points contained in the questionnaire through confirmation and validation of documentation data.
Stage 4: Data analysis. At this stage, an assessment based on the KAMI Index is carried out by calculating the questionnaire results points using the calculations contained and determined in the Information Security Index (KAMI Index) to obtain results for evaluating the condition of security and completeness of information and comparing information security points contained in ISO / IEC 27001: 2013.
Stage 5: Recommendations for improvement. recommendations for improvement based on information security management controls contained in ISO / IEC 27001: 2013 and based on the practice or implementation of ISO / IEC 27002: 2013.
Stage 6: is to draw conclusions from the results of the evaluation that has been carried out and the researcher will provide suggestions for further research with similar discussions and the Sleman Regency Communication and Information Technology Service.

3.1 Data Collection

In this chapter, data collection will be carried out by filling out the KAMI Index questionnaire, where the character of the respondent will be determined in advance according to the duties and responsibilities at the agency. Then after the questionnaire is filled in, data validation will be carried out by checking the proof document to get the accuracy of the results of filling out the questionnaire. The final stage in data collection, namely calculating the readiness level value (completeness and maturity) to provide recommendations for improvement based on ISO / IEC 27001: 2013 and ISO / IEC 27002: 2013. Before collecting data related to the KAMI index assessment in order to understand the characteristics, conditions, and level of electronic systems used by the Sleman Regency Communication and Information Service, it is necessary to fill out an electronic system category questionnaire. In the electronic system category where respondents chose 3 answers A with a score of 15, 4 answers B with a score of 8, and 3 answers C with a score of 3, with the total score obtained in the electronic system category being 26 as in Table 2, which means that the condition of the role of the electronic system is included in the "High" category.
The next information security category includes six areas, namely governance, risk management, framework, asset management, information security technology, and supplements can be seen in the attached table image. The results of the KAMI Index Questionnaire Answers can be seen in Table 3.

Table 2. Results of the electronic system category questionnaire

Electronic System Category		
Number of Questions		10
Respondents Answers		
Answer	Amount	Score
A	3	5
B	4	2
C	3	1
Total		26

Table 3. Results of KAMI index questionnaire answers information security area.

	Information Security Area					
	Governance	Risk Management	Framework	Assets Management	Technology	Total
Number of Questions	22	16	29	38	26	131
Control Category	Score					
1	23	30	35	71	41	
2	44	24	60	60	60	
3	39	18	63	36	18	
Respondents	106	72	158	167	119	622

In the information security governance area gets a total score of 106, the information security risk management area gets a total score of 72, the information security framework area gets a total score of 158, the information asset management area gets a total score of 167, the information security technology area gets a total score of 119, so the total number of questionnaire results to the five information security areas is 622. There are additional areas where this area has the aim of evaluating the readiness of securing third party involvement, securing cloud infrastructure services and protecting personal data used according to the context or scope of the Sleman Regency Communication and Informatics Service. The following are the results of the KAMI Index Questionnaire Answers for the supplementary area can be seen in Table 4.

Table 4. Supplement area KAMI index questionnaire answer results.

Sub Area	Number of Questions	Status: Not Done Yet (Score = 0)	Status: In Planning (Score = 1)	Status: Partial Implementation (Score=2)	Status: Complete Implementation (Score =3)	Total	Final Score: Total score/number of question (Max = 3.00)
Security of involvement of third-party service	27	2	0	5	20	70	2.59
Security of cloud	10	2	0	2	6	22	2.20
Security of personal data	16	0	0	0	16	48	3.00

The supplement area is divided into 3 areas, where each area has its own score. In the first area, namely Securing Third Party Involvement, it gets a total score of 70 or 2.59 with the calculation formula (70/27). In the second area, namely Cloud Infrastructure Service Security, it gets a total score of 22 or 2.2 with the calculation formula (22/10). In the third area, namely Personal Data Protection, gets a total score of 48 or 3 with the calculation formula (48/16). From the overall score of the 3 sub-areas in the supplement area, the final result is obtained in each sub-area, which presents the readiness and completeness in the supplement area. In the third-party liability security sub area, the score is 70 or 2.59 with the percentage obtained is 86%, in the cloud infrastructure service security sub area, the score is 22 or 2.2 with the percentage obtained is 73%, in the personal data protection sub area, the score is 48 or 3.00 with the presentation obtained is 100%.

4 Results and Discussion

Based on the results of the questionnaire that has been processed and validating the data, then there are 2 results of data analysis from the calculation of questionnaire data contained in the Dashboard sheet consisting of the level of readiness (completeness and maturity) of information security implementation described through radar diagram and

bar charts as well as reports on the evaluation results of calculations from questionnaires in each area. The following are the results of the evaluation of the completeness and maturity level assessment of all categories and security areas at the Sleman Regency Communication and Informatics Office as shown in Fig. 2.

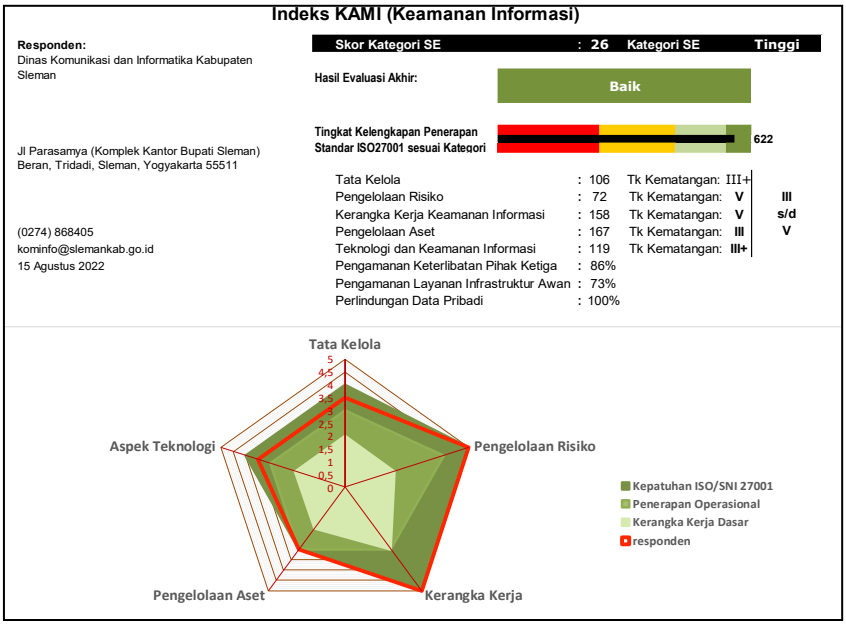

Figure 2. Pentagon radar diagram of evaluation results of readiness level assessment (completeness and maturity) of information security implementation.

4.1 Information Security Completeness Level

From the results of the final evaluation of the KAMI Index assessment at the Sleman Regency Communication and Information Service, it gets a good status. Where the score of the completeness level of the application of the ISO 27001 standard is 622 bar charts which are in the "Dark Green" color and the evaluation of the assessment in the Electronic Systems (SE) category gets a score of 26, the score is in the High category. The level of completeness of information security implementation illustrates that the 5 areas of information security have passed the basic framework standards.

There are 3 areas, namely the governance area, the technology aspect area, the asset management area, which have passed the operational implementation standard and are close to the ISO/IEC 27001/2013 compliance standard, there are 2 areas, namely the risk management area, the framework area, which have passed the ISO/IEC 27001/2013 compliance standard. Of the five areas of information security observed, the Sleman Regency Communication and Information Technology Office has exceeded the standards of the Implementation Process applied and also in the Risk Management

Area, and the Framework Area which is better than other areas (achievement of standards set in ISO 27001 / SNI).

4.2 Information Security Maturity Level

The results of the evaluation of the maturity level assessment of all categories and security areas at the Sleman Regency Communication and Information Technology Office for the maturity level from the lowest to the highest are I-V. The minimum limit that must be achieved by the Sleman Regency Communication and Informatics Service to be able to carry out ISO / IEC 27001: 2013 certification is at level III +, while currently the Sleman Regency Communication and Informatics Service has obtained an average maturity condition level at level IV which shows the position of the maturity level at the Sleman Regency Communication and Informatics Service at level IV with the condition status "Managed and Measurable" as in table 5 and means that the Sleman Regency Communication and Informatics Service can already carry out Information Security Index (KAMI) certification, especially ISO / IEC 27001: 2013 certification.

Based on the results of the discussion that has been discussed, all aspects have a high score, only a few aspects that only need a little improvement advice, namely in the Governance Area and the Supplementary Area by using the completeness of the ISO / IEC 27001: 2013 and ISO / IEC 27002: 2013 standards in practice. In the Information Security Governance Area, it is known that it has not defined information security countermeasures and policies. So that in the Information Security Governance Area the need to make policies from the elements described above in the Information Security Incident Management Document. In the supplement area, it is known that the agency has not defined, established and implemented thoroughly related policies and procedures related to third party non-compliance, has not implemented related policies and procedures for managing incidents by third parties, and has not implemented related to periodic service evaluation activities, service replacement processes, security review and evaluation activities that have been carried out. So that in the Supplement Area the Agency must pay more attention to the policy of securing information assets and notes of understanding with third parties, therefore the agency must Create a Standard Document on Governance of Data and Information Security Systems. Contract Documents with Third Parties. To see the improvement obtained from the improvement recommendations that have been given, it is necessary to conduct self-assessment again using the Information Security Index and reference recommendations referring to ISO / IEC 27001: 2013 for information security policies and ISO / IEC 27002: 2013 for the practice or implementation of information policies, so that it can be used as a comparison and evaluation of improvements for the future.

Table 5. Maturity level of communication and information agency of Sleman Regency.

Level	Condition
I	Origin condition
II	Implementation of basic framework
III	Defined and consistent
IV	Managed and measurable
V	Optimal

5 Discussions and Conclusions

From the results of information security evaluation research using the Information Security Index version 4.2 at the Sleman Regency Communication and Information Technology Office, it can be concluded that:1. From the results of the final evaluation of the KAMI Index assessment at the Sleman Regency Communication and Information Technology Office, it gets a good status. Where getting a score of the completeness level of the application of the ISO 27001 standard of 622 bar charts which are in the "Dark Green" color and the evaluation of the assessment in the Electronic Systems (SE) category gets a score of 26, the score is in the High category.

The results of the evaluation of the level of completeness and application of information security in the 5 security areas of the Sleman Regency Communication and Information Technology Office, that the 5 information security areas have passed the basic framework standards. There are 3 areas, namely the governance area, the technology aspect area, the asset management area, which have passed the operational implementation standard and are close to the ISO/IEC 27001/2013 compliance standard, there are 2 areas, namely the risk management area, the framework area, which have passed the ISO/IEC 27001/2013 compliance standard.

At the maturity level of all areas of the Information Governance-Area of Technology and Information Security area, the Sleman Regency Communication and Informatics Office gets Maturity Levels III to V, so that currently the Sleman Regency Communication and Informatics Office has obtained an average maturity condition level at level IV which shows the position of the maturity level at the Sleman Regency Communication and Informatics Office at level IV with the condition status "Managed and Measurable". With a final score of 622 and a maturity level of IV at this time the Sleman Regency Communication and Information Technology Office can already carry out Information Security Index (US) certification, especially ISO / IEC 27001: 2013 certification. Suggestions that can be taken from the results of this study are the Sleman Regency Communication and Informatics Office is very good at information security awareness, it's just a matter of implementing the regulations that have been determined, it must maintain the level of maturity that has been achieved from the results of the evaluation of KAMI index. Suggestions for the Sleman Regency Communication and Information Technology Office to conduct self-assessment or self-evaluation using the Information Security Index (KAMI) routinely at least 2 times a year, in order to measure

the level of success in improvement and get an overview of the achievements of the first and subsequent evaluations.

For further research, it is recommended to use a framework other than the Information Security Index, such as Cobit to get the results of differences in recommendations from different frameworks.

References

1. BSSN, “Daftar Standar Nasional Indonesia Terkait Keamanan Siber dan Sandi”, 2021.
2. Gourisetti, S. N. G., Mylrea, M., and Patangia, H. ”Cybersecurity Vulnerability Mitigation Framework Through Empirical Paradigm: Enhanced Prioritized Gap Analysis”. Future Generation Computer Systems, vol. 105, pp. 410–431. https://doi.org/10.1016/j.future. 2019. 12.018, 2020.
3. Hasan, S., Ali, M., Kurnia, S., and Thurasamy, R., “Evaluating The Cyber Security Readiness of Organizations and Its Influence on Performance”, Journal of Information Security and Applications, Vol. 58, 102726. https://doi.org/10.1016/j.jisa.2020.102726, 2021.
4. ISO/IEC 27001:2013, “Information technology - Security techniques - Information security management systems – Requirements”.
5. ISO/IEC 27002:2013, “Information technology - Security techniques - Code of practice for information security controls”.
6. KOMINFO - Direktorat Keamanan Informasi, ”Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI)”, 1–74, September 2017.
7. Menteri Komunikasi dan Informatika, “Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi”, 2016.
8. Pratiwi, H. A. and Wulandari, L., “Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor”, JIEMAR, Vol. 2, No. 5, pp. 146–163, https://doi.org/10.7777/ jiemar.v2i5.196, 2021.
9. Sarno, R. and Iffano “Sistem Manajemen Keamanan Informasi”, Percetakan ITS Press, Surabaya, 2009.
10. Umar, Husein, “Evaluasi kinerja perusahaan”, Gramedia Pustaka Utama, 2005, 979-686-698-6.
11. Yunella, M., Herlambang, A.D. and Putra, W. H. N., “Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI”, J-PTIIK Vol 3, No 10, pp. 9552–9559, 2019.