



# Cyber security analysis of academic services based on domain delivery services and support using Indonesian e-government ratings (PEGI)

Imam Riadi<sup>\*1</sup>, Iwan Tri Riyadi Yanto<sup>2</sup>, Eko Handoyo<sup>3</sup>

Department of Information System Universitas Ahmad Dahlan Yogyakarta, Indonesia<sup>1,2</sup>

Department of Computer Engineering Universitas Muhammadiyah Lamongan, Indonesia<sup>3</sup>

## Article Info

### Keywords:

COBIT 5, Maturity, PEGI, Safety

### Article history:

Received 28 May 2020

Accepted 25 August 2020

Published 30 November 2020

### Cite:

Riadi, I., Riyadi Yanto, I., & Handoyo, E. (2020). Cyber Security Analysis of Academic Services based on Domain Delivery Services and Support using Indonesian E-Government Ratings (PEGI). *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 5(4). doi:<https://doi.org/10.22219/kinetik.v5i4.1083>

\*Corresponding author.

Imam Riadi

E-mail address:

imam.riadi@is.uad.ac.id

## Abstract

Safe academic services are the most important part of universities. The security of academic services is very important to maintain information optimally and safely. Along with the development of technology, academic information services are often misused by some irresponsible parties that can cause threats. To prevent these things from happening, it is necessary to know the extent of governance of higher education academic information system security by evaluating. So the research was conducted to determine the maturity of the security of Higher Education academic information service security by using the COBIT 5 framework in the DSS05 domain. The DSS05 domain in COBIT 5 is a good framework for use in implementing and evaluating the security of academic information services. Meanwhile, to determine the achievement of the evaluation of the security level of academic information systems, the Indonesian e-government ranking (PEGI) method is required. The combination of the COBIT 5 framework in the DSS05 domain using the PEGI method in academic information security service is able to provide a level of achievement in the form of Customer Value. The results of the COBIT 5 framework analysis of the DSS05 domain using the PEGI method get a score of 3.50 so that the quality of academic information service security evaluation achievement is at a very good level. At this level, universities are increasingly open to technological development. Higher education has applied the concept of quantification in every process, and has always been monitored and controlled for its performance in the security of academic information systems.

## 1. Introduction

Institutions place information technology as things that can support the achievement of the company's strategic plan to achieve the goals of the institution's vision, mission and goals. Information technology will get effective results if it uses good governance in its use and is able to be assessed and evaluated [1]. The information system is a system that contains an SPD network (data processing system), which is equipped with communication channels that are used in data organization systems [2]. There are various concepts of information systems, suitability is one of the keys to successful implementation and acceptance of information systems [3][4]. Along with the development of technology, it is often misused by some irresponsible parties that can cause threats [5]. Academic information system services must provide security, privacy and integrity of data processed, so that the performance of academic information systems is also an important part that must be considered so that academic information systems can be utilized optimally and safely [6]. The application of information security systems aims to overcome all problems and obstacles both technically and non-technically that can affect system performance, such as availability, confidentiality, and integrity so that the level of information security can be assessed [7][8]. As in Figure 1.



Figure 1. Aspects of Information Security

The existence of security problems triggers, procedures to control access rights in an information system [9]. A good information system security must apply the Deming cycle of quality standard. The security of academic information

Cite: Riadi, I., Riyadi Yanto, I., & Handoyo, E. (2020). Cyber Security Analysis of Academic Services based on Domain Delivery Services and Support using Indonesian E-Government Ratings (PEGI). *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 5(4). doi:<https://doi.org/10.22219/kinetik.v5i4.1083>

systems can be audited with various standards such as COBIT, COSO, ITIL, CMM, BS779, ISO 9000. COBIT (Control Objectives for Information and related Technology) is a standard guide to information technology management practices and a collection of documentation of best practices for IT governance that can help auditors, management, and users to bridge the gap between business risk, control needs, and technical issues [10][11]. All organizations can adjust COBIT 5 to their various goals, and are able to evaluate the organization in achieving its intended goals [12]. Domain DSS (Deliver, Service and Support) relates to system delivery and service support needed by the system, which includes service, security and continuity management, service support for users, and data management and operational facilities so that it is more focused on domain scopes that provide services that well [13]. DSS domain has sub-domain DSS05 which in this sub-domain is a more intensive procedure for information security. The method that can be used in evaluating achievement evaluations is PEGI. Indonesian e-government ranking (PEGI) is a model created by the Directorate of e-Government, Directorate General of Applications and Telematics, Ministry of Communication and Information (Kementerian KOMINFO) which can be used as a solution to analyze e-Government [14]. Page has five dimensions of assessment, namely each policy, institutional, infrastructure, application and planning. Each dimension has the same weight in the assessment because all are important, interrelated and mutually supportive [15]. The PEGI method in academic information system security is able to provide a level of achievement in the form of maturity value. So as to be able to provide a decision on the extent to which the academic information system security process has been carried out by universities.

This study aims to conduct an evaluation related to the security of academic information service security that has been implemented at the University. This study aims to obtain the value of information system security from an institution, so that recommendations and innovations can be made for information system security in the institution. So that institution can provide security and comfort for the delivery of the information system services.

**2. Research Method**

**2.1 DSS05 Framework COBIT 5**

The DSS05 sub-domain is part of the DSS (Deliver, Service and Support) domain. Like Figure 2.

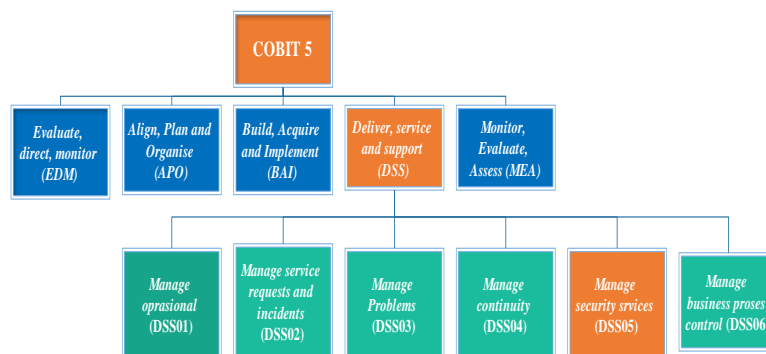


Figure 2. DSS05 Schema

The DSS05 sub-domain is managed security services where the sub-domain is grouped into 7 processes. Like Figure 3.

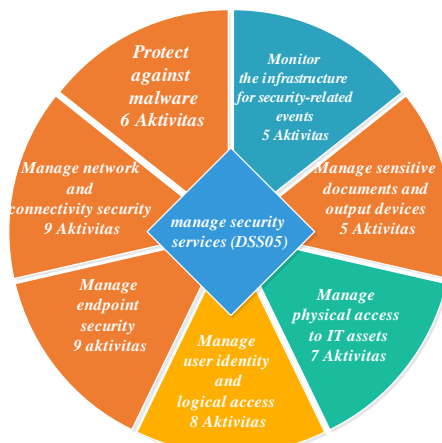


Figure 3. Metode DSS05

The seven processes carry out some 49 statements or activities as follows [16]:

1. Protect against malware (DSS05.01) where this process implements and maintains existing preventive, detective and corrective measures (especially security patches and virus control) throughout the company to protect information systems and technology from malware (e.g. Viruses, worms, spyware, spam).
2. Manage network and connectivity security (DSS05.02) where this process is used in security measures and related management procedures to protect information from all connectivity methods.
3. Manage endpoint security (DSS05.03) where this process provides certainty for endpoints (for example: Laptops, desktops, servers, and mobile devices and cellular networks or other software) guaranteed a level equal to or greater than the agreed security requirements.
4. Manage user identity and logical access (DSS05.04) This process gives certainty to all users having the right to access information according to business needs. They and coordinate with business divisions that manage access rights.
5. Manage physical access to IT assets (DSS05.05) this process determines and applies procedures to give, limit and revoke access to physical buildings. Buildings and areas according to business needs, including emergencies. Access to buildings, buildings and areas must be justified, authorized, recorded and monitored.
6. Manage sensitive documents and output devices (DSS05.06) where this process establishes physical security. In terms of documents relating to institutions. So all document output is standardized in security.
7. Monitor the infrastructure for security-related events (DSS05.07) where this process uses intrusion detection tools, to monitor infrastructure for unauthorized access rights and ensure every event is integrated with event monitoring and event management.

## 2.2 Indonesian E-Government Ratings (PeGI)

PeGI is a model created by the Directorate of e-Government, Directorate General of Applications and Telematics, Ministry of Communication and Information (Kementerian KOMINFO) yang dapat digunakan sebagai solusi untuk menganalisis e-Government. Pegi has five dimensions of assessment, namely each policy, institutional, infrastructure, application and planning. Each dimension has the same weight in the assessment because all are important, interrelated and mutually supportive [17].

The e-Government Directorate implemented the PeGi for the first time in 2007. All provinces in Indonesia were invited, as many as 11 provinces participated, namely Aceh, Lampung, South Sumatra, Banten, West Java, Central Java, Special Region of Yogyakarta, East Java, West Kalimantan, Sulawesi Southeast, and East Nusa Tenggara. PeGi is expected to be able to increase the development and use of ICTs in government institutions throughout Indonesia. In its implementation, KOMINFO cooperates with various groups from the ICT community, universities and related government agencies.

In general, the assessment of Indonesian e-Government governance is shown in Figure 4 and explained [18]:

- a. Value 1.0-1.49 (very less): Indicator does not exist at all or very less in terms of quantity and quality.
- b. Value 1.5-2.49 (less): Indicator already exists, but still needs to be added in terms of quantity and improved in quality.
- c. Value 2,5-3,49 (good): Indicators of number and quality are quite good and can be seen to have a positive impact on the use of e-government, but improvements are needed to maintain the continuity of implementation in the future.
- d. Value 3.5-4.0 (very good): Indicator both in terms of quantity and very good quality. The impact of implementing e-government is very real. Readiness to continue to be developed in the future is clearly visible.

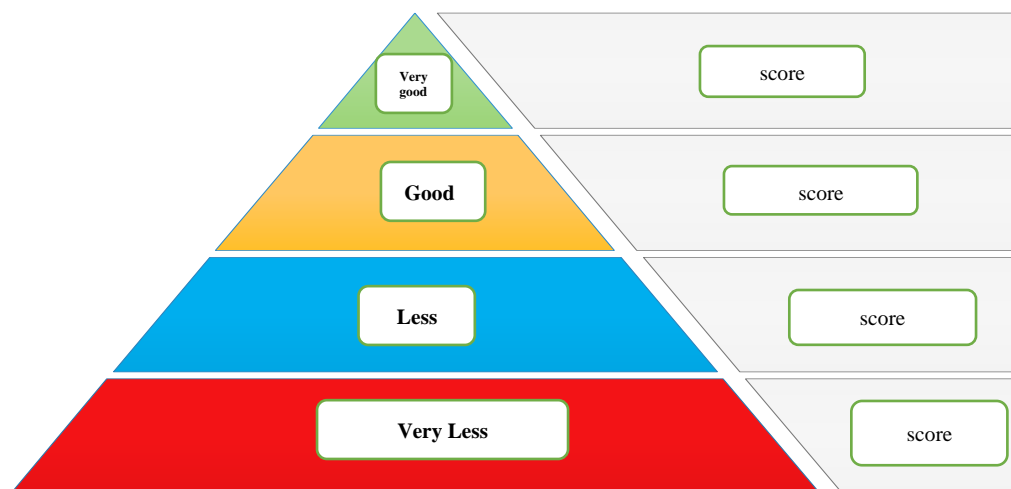


Figure 4. PeGi Rating

### 3. Results and Discussion

This section will be presented in the process of methods guaranteed in a structured manner. analysis of the implementation and performance measurement of the maturity level of information systems with a framework sub-domain DSS05 framework COBIT 5 and PEGI.section explains the results of research and at the same time is given the comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily. The discussion can be made in several sub-sections.

#### 3.1 Academic Service Process Observation

This process conducted interviews directly with informants authorized by the security of academic information systems in Higher Education using academic information systems began to be active in 2008, the beginning of the information system created and developed by vendors (Gama Techno) After that, in 2017 there will be migrating to a new system where the system will be developed by universities. Where in the migration is caused by the development of information system technology, so it is deemed necessary to do the migration to maintain the stability and security of the information system.

The aim of the college's academic system itself is:

1. To manage academic activities in the college environment.
2. Providing facilities for the Civitas, lecturers, students, staff and BAA in the academic process.

Over time the use of information systems is also experiencing obstacles, problems and threats to the information system. The problems, obstacles and threats that often occur are as follows:

1. There are several systems that have not been well integrated.
2. When the KRS is online the server is down.
3. Frequent occurrence of forgetting usernames and passwords.
4. The process of connecting or data transmission is slow.
5. Virus and malware attacks.

The standardization and auditing process of tertiary institutions applies ISO 9000 which is used as a standard for a quality management system (QMS) that is integrated with all bureaus in all institutions. This process also discusses the determination of respondents who will provide detailed information related to information about the security of existing academic information systems. The sample selection of respondents uses a purposive sampling technique, namely the selection of the sample of respondents determined by the researcher on the grounds that identification of the sample of respondents is done by referring to personal competencies that interact directly with IT governance [19]. The interview got 2 respondents who were directly related to the information system security sector in the institution.

#### 3.2 Mapping DSS05 Based on COBIT 5 Framework

This process is the preparation of activity suitability in the DSS05 sub-domain with questions that will be made in the questionnaire. This process against malware consists of 6 activities, as in Table 1.

Table 1. Protect Against Malware Activity  
Protect against malware (DSS05.01)

| No | Activity Questions   |
|----|--|
| 1  | Obtain information about malicious software and how to handle it.                                  |
| 2  | Install and activate anti-virus on your PC.  |
| 3  | Is anti-virus on the PC always updated.  |
| 4  | Regularly review and evaluate information about potential malware threats.                         |
| 5  | Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information. |
| 6  | Conduct regular training on malware in the use of email and the Internet.                          |

#### 3.3 Questionnaire preparation with a combination of DSS05 and value PEGI





This process is carried out by establishing a questionnaire based on the standard on DSS05 Framework COBIT 5 by combining it with the values of the PEGI standard so that a questionnaire form is obtained that is able to answer the needs of the existing information system security in the installation. To make it easier to read the process, a difference in the color of each decision is made. as in Table 2.

Table 2. Mapping Color

| Status    | Color   | Values     |
|-----------|---|------------|
| Very Good |  | 3.5 - 4.0  |
| Good      |  | 2.5 - 3.49 |
| Less      |  | 1.5 - 2.49 |
| Very Less |  | 1.0 - 1.49 |


Where in this questionnaire there are 4 assessments in the process with PEGI as shown in Table 3.

Table 3. Criteria and Values

| Color   | Values     | Activities                  |
|---|------------|-----------------------------|
|  | 3.5 - 4.0  | Done with SOP and evaluated |
|  | 2.5 - 3.49 | Done with SOP               |
|  | 1.5 - 2.49 | Done                        |
|  | 1.0 - 1.49 | Are not done                |

From the IT process assessment in Table 3, combined with the DSS05 COBIT 5 framework standard in Table 1, as in Table 4.

Table 4. Questionnaire Form

| Protect against malware (DSS05.01)   |   |
|--|---|
| Activities   | Answer  |
| 1 Obtain information about malicious software and how to handle it.                                  |  |
| 2 Install and activate anti-virus on your PC.  |   |
| 3 Is anti-virus on the PC always updated.  |   |
| 4 Regularly review and evaluate information about potential malware threats.                         |   |
| 5 Filter incoming traffic, such as e-mail and downloads, to protect against unsolicited information. |   |
| 6 Conduct regular training on malware in the use of email and the Internet.                          |   |

### 3.4 Calculation of the maturity level of Academic service security

This section will explain the results of the analysis of the implementation and performance measurement of the maturity level of the academic information system obtained from questionnaires and interviews in accordance with the DSS05 framework framework COBIT 5. To identify the extent to which an institution has met with good information security standards, it can use an identification framework that is represented at a level of maturity that has a level of grouping of company capabilities, as described in Table 5.

Table 5. Maturity Criterion Value PEGI

| Criterion | Value      |
|-----------|------------|
| Very Good | 3.5 - 4.0  |
| Good      | 2.5 - 3.49 |
| Less      | 1.5 - 2.49 |
| Very Less | 1.0 - 1.49 |

The results of the questionnaire that has been given to the respondent and have been filled out by the respondent get results as in Table 6.

Table 6. Questionnaire Results

| DSS        | Responden 1 | Responden 2 |
|------------|-------------|-------------|
| DSS05.06.1 | 2           | 2           |
| DSS05.06.2 | 3           | 2           |
| DSS05.06.3 | 3           | 2           |
| DSS05.06.4 | 4           | 2           |
| DSS05.06.5 | 1           | 2           |

Next correlate between the level value and absolute value which is done by calculation in the form of an index using a mathematical formula. The mathematical Equation 1 to determine the index value is as follows [20].

$$Indeks = \frac{\sum \text{answers to the most questions}}{\sum \text{Questionnaire question}} \tag{1}$$

After the index is obtained, we can get the current level of maturity (existing) this value is the value of the accumulation of processes that are running in the institution. a case in Table 7.

*Table 7. Current Maturity Value*

| DSS05   | Nilai Existing |
|---|----------------|
| <i>Protect against malware</i>                                | 3,92           |
| <i>Manage network and connectivity security</i>               | 4,00           |
| <i>Manage endpoint security</i>                               | 3,50           |
| <i>Manage user identity and logical access</i>                | 3,88           |
| <i>Manage physical access to IT assets</i>                    | 3,71           |
| <i>Manage sensitive documents and output devices</i>          | 2,30           |
| <i>Monitor the infrastructure for security-related events</i> | 3,20           |

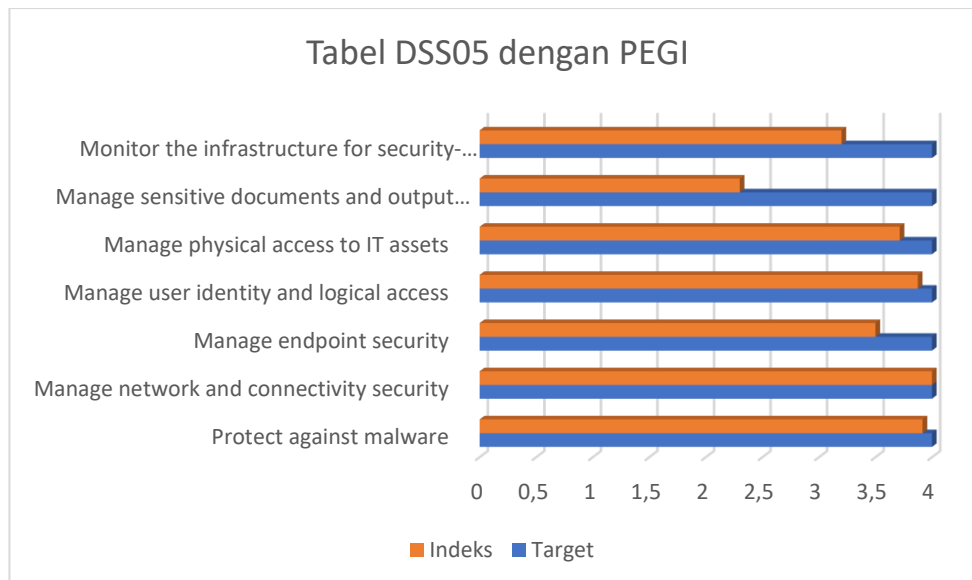
### 3.5 Gap Calculation

Once the value of the existing Maturity Level is obtained and the recommended Maturity Level (target) has been determined, the gap between the current condition and the target to be achieved will be analyzed and opportunities for the gap to be optimized will be identified, as in Table 8.

*Table 8. Maturity Gap Value*

| DSS05  | Target | Indeks Maturity Level Existing |
|--|--------|--------------------------------|
| Protect against malware                                | 4      | 3,92                           |
| Manage network and connectivity security               | 4      | 4,00                           |
| Manage endpoint security                               | 4      | 3,50                           |
| Manage user identity and logical access                | 4      | 3,88                           |
| Manage physical access to IT assets                    | 4      | 3,71                           |
| Manage sensitive documents and output devices          | 4      | 2,30                           |
| Monitor the infrastructure for security-related events | 4      | 3,20                           |

From Table 8 is a comparison between the desired target and the achievement of the maturity value of existing information technology security processes that have been carried out so far. So that it can be drawn a maturity gap in the form of a graph like Figure 5.



*Figure 5. Gab Maturity*

### 3.6 Gap Analysis

The discussion section provides in-depth reviews (insights) of the data obtained in the study. In this section tables or graphs can be presented which are the results of data processing. Based on the Gap analysis obtained from the

results of the target level to be achieved and the level achieved in DSS05, as in Figure 5, then here is some Gap Maturity Level Analysis. As in Table 9 as follows.

Table 9. Maturity Level Gap Analysis

| DSS05  | Maturity Level |
|--|----------------|
| Protect against malware                                | Very Good      |
| Manage network and connectivity security               | Very Good      |
| Manage endpoint security                               | Very Good      |
| Manage user identity and logical access                | Very Good      |
| Manage physical access to IT assets                    | Very Good      |
| Manage sensitive documents and output devices          | Good           |
| Monitor the infrastructure for security-related events | Good           |

From the overall value of the level of death on DSS05 will be calculated on average, so that the level of maturity of the institution's security will be obtained Equation 2.

$$\begin{aligned}
 \text{Maturity Level DSS05} &= \frac{\sum \text{Maturity Level}}{\text{Many Processes}} \\
 \text{MLDSS5} &= \frac{i(DSS05.01) + i(DSS05.02) + i(DSS05.03) + i(DSS05.04) + i(DSS05.05) + i(DSS05.06) + i(DSS05.07)}{MP} \\
 \text{MLDSS5} &= \frac{3.92 + 4 + 3.50 + 3.88 + 3.70 + 2.30 + 3.20}{7} \\
 \text{MLDSS05} &= 3.50 \\
 \text{Level of maturity DSS05} &= 3,50
 \end{aligned}
 \tag{2}$$

From the calculation results, the achievement value is 3.50 so that the institution's maturity can be set at the Very Good level.

#### 4. Conclusion

Sub-domain DSS05 Manage security services is a good procedure to be used in implementing and conducting megabits related to academic information system security services and PEGI is a good assessment method in an institution's audit system. Based on research conducted at the tertiary institution, the score of the fatality level was 3.50 thus establishing that the current level of maturity is at a very good level. At this level, institutions are increasingly exposed to technological developments. Institutions have applied the concept of quantification in every process, and are always monitored and controlled for their performance.

#### References

- [1] R. Umar, I. Riadi, and E. Handoyo, "Analysis of Information Technology Governance Using the COBIT 5 Framework in Domain Delivery, Service, And Support (DSS)," *Semin. Nas. Teknol. Inf. dan Komun. - Semant. 2017 Anal.*, pp. 41–48, 2017.
- [2] L. F. Fathoni *et al.*, "Application Information System Based Health," vol. 2, no. 1, pp. 37–46, 2016.
- [3] I. Muslimin, S. P. Hadi, and E. Nugroho, "An Evaluation Model Using Perceived User Technology Organization Fit Variable for Evaluating the Success of Information Systems," vol. 4, no. 2, pp. 86–94, 2017. <https://doi.org/10.15294/sji.v4i2.12012>
- [4] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," vol. 5, no. 2, pp. 235–247, 2018. <https://doi.org/10.15294/sji.v5i2.16545>
- [5] I. Riadi and M. E. Rauli, "Live forensics analysis of line app on proprietary operating system," vol. 4, no. 4, 2019. <https://doi.org/10.22219/kinetik.v4i4.850>
- [6] E. Kurniawan, "Security Level Analysis Of Academic Information Systems Based On Standard Iso 27002 : 2013 USING SSE-CMM," *Int. J. Comput. Sci. Inf. Secur.*, vol. 16, no. January, 2018. <https://doi.org/10.29407/intensif.v2i1.11830>
- [7] I. Riadi, S. Sunardi, and E. Handoyo, "Security Analysis of Grr Rapid Response Network using COBIT 5 Framework," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 10, no. 1, pp. 29, 2019. <https://doi.org/10.24843/LKJITI.2019.v10.i01.p04>
- [8] P. O. Rahmanda, R. Arifudin, and M. A. Muslim, "Implementation of Analytic Network Process Method on Decision Support System of Determination of Scholarship Recipient at House of Lazis Charity UNNES," vol. 4, no. 2, pp. 199–211, 2017. <https://doi.org/10.15294/sji.v4i2.11852>

- [9] M. Sumagita, I. Riadi, U. A. Dahlan, K. Yogyakarta, and D. I. Yogyakarta, "Analysis of Secure Hash Algorithm ( SHA ) 512 for Encryption Process on Web Based Application," vol. 7, no. 4, pp. 373–381, 2018.
- [10] E. Hicham, B. Boulafourd, M. Makoudi, and B. Reagraui, "Information security, 4TH wave," *J. Theor. Appl. Inf. Technol.*, vol. 43, no. 1, pp. 1–7, 2012.
- [11] I. Riadi, Y. Iwan, and E. Handoyo, "Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI," 2020. <https://doi.org/10.1088/1757-899X/821/1/012003>
- [12] F. Latifi and H. Zarrabi, "A COBIT5 Framework for IoT Risk Management," *Int. J. Comput. Appl.*, vol. 170, no. 8, pp. 40–43, 2017.
- [13] R. Umar, I. Riadi, and E. Handoyo, "Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Integration ( CMMI )," *Sci. J. Informatics*, vol. 6, no. 2, pp. 193–202, 2019. <https://doi.org/10.15294/sji.v6i2.17387>
- [14] O. K. Sulaiman, "Network Security System Analysis With Switch Port Security" vol. 1, no. 1, pp. 9–14, 2016. <https://doi.org/10.24114/cess.v1i1.4036>
- [15] R. Fadhlurrahman, M. C. Saputra, and A. D. Herlambang, "Evaluation of the Implementation of E-government in Batu City Government Using Indonesia's E-government Rating Framework ( PeGI )," vol. 2, no. 12, pp. 5977–5982, 2018.
- [16] J. F. Andry, "Audit of IT Governance Based on COBIT 5 Assessments: A Case Study," *TEKNOSI*, vol. 02, no. May, 2017. <https://doi.org/10.25077/TEKNOSI.v2i2.2016.27-34>
- [17] A. Yudhana *et al.*, "Designing Information Systems Using Enterprise Architecture Planning ( Studi Kasus Pada Kecamatan di Kota Samarinda )," *khazanah Inform.*, vol. 4, no. 2, pp. 114–123, 2018. <https://doi.org/10.23917/khif.v4i2.7039>
- [18] A. Fitriansyah, H. Budiarto, and J. Santoso, "Indonesian E-Government Rating Method (PeGI) for Information Technology Governance Audits," *Semin. Nas. Sist. Inf. Indones.*, pp. 2–4, 2013.
- [19] P. Rahayu and D. I. Senses, "Assessment of e-Government Implementation in the Ministry of Education and Culture PUSTEKOM based on the PEGI method," *J. Sist. Inf. Bisnis*, vol. 02, pp. 139–145, 2017. <https://doi.org/10.21456/vol7iss2pp139-145>
- [20] Rusydi Umar, I. Riadi, and E. Handoyo, "A Analysis of Information Systems Security Based on COBIT 5 Framework Using Capability Maturity Model Integration (CMMI)," *J. Sist. Inf. Bisnis*, vol. 01, pp. 47–54, 2019. <https://doi.org/10.21456/vol9iss1pp47-54>