Scientific Journal of Informatics
Vol. 6, No. 2, Nov 2019
p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Integration (CMMI)

Rusydi Umar[1], Imam Riadi[2], Eko Handoyo[3]

[1]Department of Informatics, Universitas Ahmad Dahlan, Indonesia,
[2]Department of Information System, Universitas Ahmad Dahlan, Indonesia,
[3]Department of Cmputer Engineering, Universitas Muhammadiyah Lamongan, Indonesia,
Email: [1]rusydi_umar@rocketmail.com, [2] imam.riadi@mti.uad.ac.id, [3]ekokurro17@gmail.com

Abstract

A secure academic information system is part of the college. The security of academic information systems is very important to maintain information optimally and safely. Along with the development of technology, academic information systems are often misused by some irresponsible parties that can cause threats. To prevent these things from happening, it is necessary to know the extent to which the security of the academic information system of universities is conducted by evaluating. So the research was conducted to determine the Maturity Level on the governance of the security of University Ahmad Dahlan academic information system by using the COBIT 5 framework on the DSS05 domain. The DSS05 domain on COBIT 5 is a good framework to be used in implementing and evaluating related to the security of academic information systems. Whereas to find out the achievement of evaluation of academic information system security level, CMMI method is needed. The combination of the COBIT 5 framework on the DSS05 domain using the CMMI method in academic information system security is able to provide a level of achievement in the form of a Maturity Level value. The results of the COBIT 5 framework analysis of the DSS05 domain use the CMMI method to get a Maturity level of 4,458 so that it determines the achievement of the evaluation of academic information systems at the tertiary level is Managed and Measurable. This level, universities are increasingly open to technological developments. Universities have applied the quantification concept in each process, and are always monitored and controlled for performance in the security of academic information systems.

Keywords: CMMI, COBIT 5, Security SIA, Managed and Measurable, Maturity Level,

1. INTRODUCTION

Companies or institutions place information technology as a thing that can support the achievement of the company's strategic plan to achieve the goals of the company or 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 evaluated and evaluated[1]. Information systems are systems that contain SPD networks (systems processing data), which are equipped with communication channels used in data organization systems[2]. There are various concepts of information systems, compatibility is one of the keys to the successful implementation and acceptance of information systems[3]. Along with the development of technology, it is often misused by some irresponsible parties that can cause threats[4]. Academic

information systems must provide the 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 used optimally and safely[5]. The application of information security systems aims to overcome all problems and constraints, both technically and non-technically which can affect the performance of the system such as availability, confidentiality and integrity factors so that the level of information security can be assessed[6], as in Figure 1.

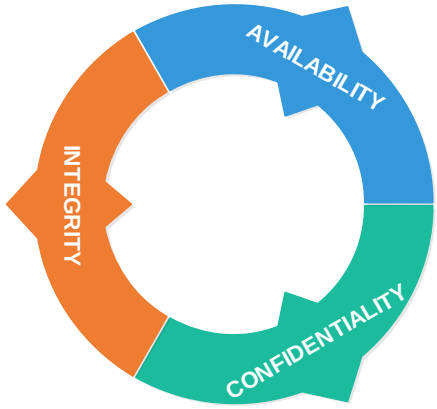

Figure 1 Information security aspects

The existence of a security problem triggers a procedure for controlling access rights to an information system[7]. A good information system security must apply the standard Deming cycle of quality[8]. The security of academic information 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 set of best practices documentation for IT governance that can help auditors, management, and users to bridge the gap between business risk, control needs, and technical issues[8]. All organizations can adjust COBIT 5 for their various purposes, and are able to evaluate the organization in achieving its intended goals[9]. Domain DSS (Deliver, Service and Support) is related 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 integrated in the domain that provides services well[8]. DSS domains have sub-domain DSS05 wherein this sub-domain is a more intensive procedure for information security. The method that can be used in evaluating the achievement of evaluation is CMMI. Capability Maturity Model Integration (CMMI) is a model approach to assess the scale of capability and maturity of a software organization. The history of CMMI at the beginning was known as the Capability Maturity Model (CMM) which was built and developed by the Software Engineering Institute in Pittsburgh in 1987[10].

This study aims to conduct an evaluation related to the security management of academic information systems that have been implemented at Ahmad Dahlan University. This study aims to obtain the value of the level of information system security of an institution, so that recommendations and innovations can be made for the security of information systems in these institutions.

2. METHODS

The combination of both is expected to be able to provide good results in evaluating the security of academic information systems at the college. As in Figure 2.

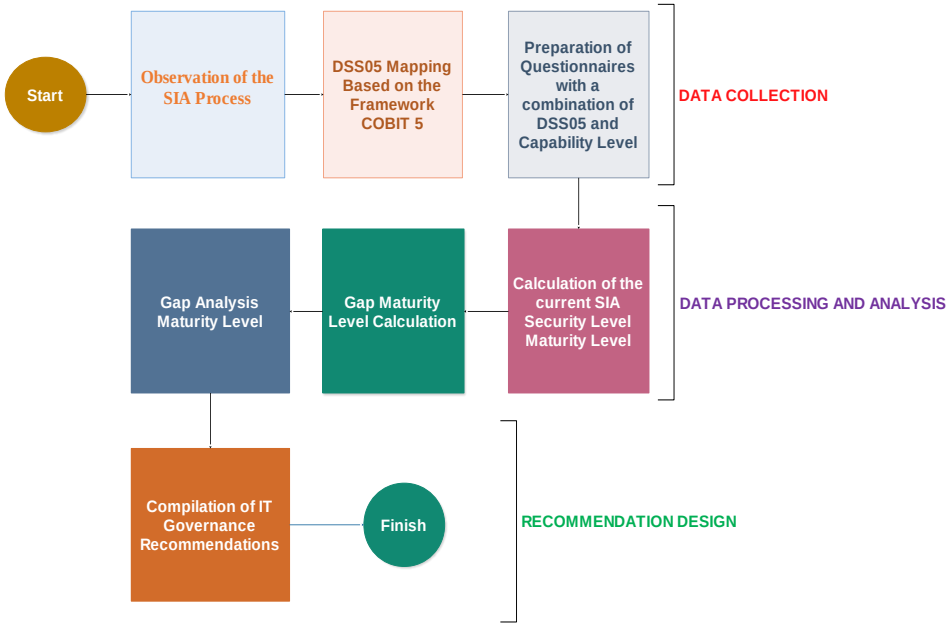

Figure 2. Flowchart Method

2.1. DSS05 Framework COBIT 5.

The DSS05 sub-domain is managing security services where these sub-domains are grouped in 7 processes. The seven processes carry out some activities or statements of the 49 statements as follows[11]As in Figure 3.

Figure 3. DSS05 Method

2.2. Capability Maturity Model Integration (CMMI)

CMMI is a maturity method that can be used to improve processes within the institution. The purpose of using the CMMI within an institution is to improve the process of developing and improving the software product of the institution[12].

According to[13] CMMI has Capability Level. Capability Level is a model to describe how each core process runs within an institution. Capability Level has 6 levels for each core process,as in Figure 5.

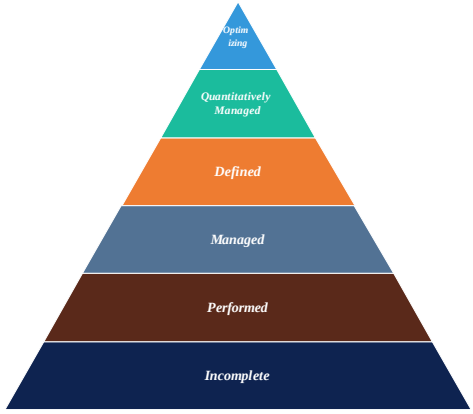

Figure 5. Capability Level CMMI

According to [13] The CMMI model places, institutions in 5 Maturity Levels or CMMI levels, as in Figure 6.

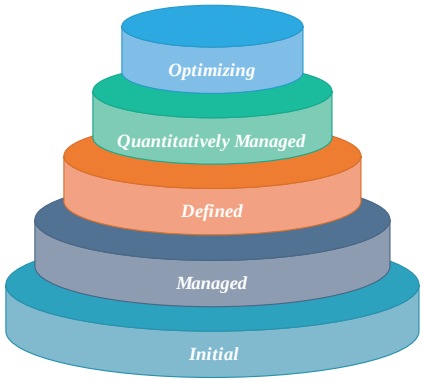

Figure 6. Maturity Level CMMI

3. RESULT AND DISCUSSION

Analysis of the implementation and measurement of the maturity level of the information system with the framework COBIT 5 sub-domain DSS05 and CMMI.

3.1 Observation of the Academic Information System Process

This process conducts interviews directly with the resource person who has authority in the security of the academic information system at BISOM.

As time goes on the use of information systems also experiences, obstacles, problems and threats to information systems. 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 online KRS happened the server was down.
3) It often happens to forget your username and password.
4) The process of data connection or transmission is slow.
5) Virus and malware attacks.

The selection of respondent samples using purposive sampling technique, which is the selection of respondents 'samples determined by researchers on the grounds that identification of respondents' samples is done by referring to personal competencies that interact directly with IT governance[14]. Interviews get 2 respondents who are directly concerned with the field of information system security within the institution.

3.2 DSS05 Mapping Based on the COBIT Framework 5

This process is a compilation of DSS05 domain conformity activities with questions to be made in the questionnaire. because of the limitations of our writing, we only list one of the 7 DSS05 sub-domain processes, namely DSS05.01. The DSS05.01 process 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 periodic training on malware in the use of e-mail and the Internet.

3.3 Preparation of Questionnaires with a combination of DSS05 and Capability Level

This process is carried out by questionnaires based on the standard on DSS05 Framework COBIT 5 by combining. To simplify the reading process, the color differences for each decision are made in Capability Level and Maturity Level as in Table 2.

Table 2 Process Color Maps

Color	**Information**	
	Capability Level	***Maturity Level***
Red	*Incomplete*	*Non-Existent Initial*
Purple	*Performed*	*Initial / Ad Hoc*
Yellow	*Managed*	*Repeatable But Invinitve*
Blue	*Defined*	*Define Process*
Orange	*Quantitatively Managed*	*Managed and Measurable*
Green	*Optimizing*	*Optimized*

Where in this questionnaire there are 6 assessments for processes with capability level CMMI as in Table 3.

Table 3 Assessment of IT processes with CMMI capability level

Nilai	***Capability Level CMMI***	**Proses TI**
0	*Incomplete*	Are not done
1	*Performed*	Done, not periodically
2	*Managed*	Performed periodically
3	*Defined*	Done with SOP
4	*Quantitatively Managed*	Performed and monitored
5	*Optimizing*	Done, monitored and developed

3.4 Calculation of Security SIA Maturity Level

This section will explain the results of the analysis of the implementation and measurement of the performance of the maturity level of academic information systems obtained from the results of questionnaires and interviews in accordance with the framework 5 COBIT domain DSS05. as described in Table 4.

Table 4. Value of maturity level criteria

Criteria	**Information**
0 – 0.50	*Non-Existent Initial*
0.51 – 1.50	*Initial / Ad Hoc*
1.51 – 2.50	*Repeatable But Invinitve*
2.51 – 3.50	*Define Process*
3.51 – 4.50	*Managed and Measurable*
4.51 – 5.00	*Optimized*

Furthermore, the correlation between level values and absolute values that are done by calculation in the form of an index uses a mathematical formula. The mathematical equation to determine the index value is as follows[15]:

$$Indeks = \frac{\sum Most\ Question\ Answers}{\sum Questionnaire\ Questions} \quad (1)$$

After getting the index, we can get the current Maturity Level (present). This value is the accumulated value of the process that is running on the institution. as in Table 5.

Table 5 Existing Maturity Value

DSS05	***Value of Maturity Level Existing***
Protect against malware	5,00
Manage network and connectivity security	5,00
Manage endpoint security	4,39
Manage user identity and logical access	4,88
Manage physical access to IT assets	4,64
Manage sensitive documents and output devices	3,10
Monitor the infrastructure for security-related events	4,20

3.5 Gap Maturity Level Calculation

Once the existing Maturity Level values are obtained and Maturity The recommendation level (target) has been determined, then the gap between the current condition and the target to be achieved will be analyzed and identified opportunities from the gap to be optimized, as in Table 6.

Table 6 Value of Maturity Level gap

DSS05	**Target**	***Indeks Maturity Level Existing***
Protect against malware	5	5.00
Manage network and connectivity security	5	5.00
Manage endpoint security	5	4.39
Manage user identity and logical access	5	4.88
Manage physical access to IT assets	5	4.64
Manage sensitive documents and output devices	5	3.10
Monitor the infrastructure for security-related events	5	4.20

3.6 Gap Analysis Maturity Level

Based on Gap analysis obtained from the results of the target level to be achieved and the level achieved on DSS05, as in Graph 1, then here is some Gap Maturity Level Analysis. As in Table 7.

Table 7 Gap Maturity Level Analysis

DSS05	***Maturity Level***
Protect against malware	*Optimized*
Manage network and connectivity security	*Optimized*
Manage endpoint security	*Managed and Measurable*
Manage user identity and logical access	*Optimized*
Manage physical access to IT assets	*Optimized*
Manage sensitive documents and output devices	*Define*
Monitor the infrastructure for security-related events	*Managed and Measurable*

The overall value of Maturity Level on DSS05 will be calculated on average so that it will get the level of Maturity Level in the organization or institution as in Formula (2).

$$Maturity\ Level\ DSS05 = \frac{\sum Maturity\ Level}{many\ processes} \quad (2)$$

$$MLDSS5 = \frac{\begin{array}{c} i(DSS05.01) + i(DSS05.02) + i(DSS05.03) + \\ i(DSS05.04) + i(DSS05.05) + \\ i(DSS05.06) + i(DSS05.07) \end{array}}{mp}$$

$$MLDSS05 = \frac{5 + 5 + 4{,}388 + 4{,}875 + 4{,}642 + 3{,}1 + 4{,}2}{7}$$

$$Maturity\ Level\ DSS05 = 4{,}458$$

From the calculation results obtained the value of achievement is 4,458 so that it can be set Maturity Level of organization or institution is at the Managed and Measurable level.

3.7 Compilation of IT Governance Recommendations

After Maturity Level has been determined, the recommendation preparation process will be carried out. Recommendations that can be given to improve the quality of information system security in the agency:

1) Protect against malware (DSS05.01) is on the Optimized level where in this level the BISKOM has been able to perform procedures well and is able to develop malware related ones.
2) Manage network and connectivity security (DSS05.02) is at the level of Optimized wherein at this level the BISKOM has been able to carry out

procedures well and is able to carry out developments related to security of activities.

3) Manage endpoint security (DSS05.03) in the Managed and Measurable level where in this level the BISKOM has been able to carry out procedures well, only agencies must carry out routine evaluations, at least once a month on information systems that are feared to be potential new threats.
4) Manage user identity and logical access (DSS05.04) is on the Optimized level where in this level the BISKOM has been able to carry out procedures properly and is able to develop related access rights of each user.
5) Manage physical access to IT assets (DSS05.05) is on the Optimized level where in this level the BISKOM has been able to perform procedures well and is able to carry out development related to physical security.
6) Manage sensitive documents and output devices (DSS05.06) in the Define Process level, in this BISKOM has implemented physical security, accounting practices in terms of documents relating to the situation.
7) Monitor the infrastructure for security-related events (DSS05.07) is in the Managed and Measurable level where in this level the BISKOM of has been able to carry out procedures properly using intrusion detection tools, to monitor infrastructure.

4. CONCLUSION

Sub-domain DSS05 Manage security services is a good procedure to be used in the implementation and mega-audit related to the security of academic information systems and CMMI is a good assessment method in an institution's audit system. Based on the research conducted at the BISKOM received a Maturity Level of 4,458 thus stipulating that the current maturity level is on the Managed and Measurable level.

5. REFERENCES

[1] R. Umar, I. Riadi, and E. Handoyo, "Analisis Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Pada Domain Delivery, Service, And Support (DSS)," in *Seminar Nasional Teknologi Informasi dan Komunikasi - SEMANTIKOM 2017*, 2017, pp. 41–48.

[2] L. F. Fathoni *et al.*, "Application Information System Based Health Services Android," *J. Ilmu Tek. Elektro Komput. dan Inform.*, vol. 2, no. 1, pp. 39–48, 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.

[4] Y. W, I. Riadi, and A. Yudhana, "Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing," in *Annual Research Seminar*, 2016, vol. 2, no. 1, pp. 300–304.

[5] E. Kurniawan and I. Riadi, "Security level analysis of academic information systems based on standard ISO 27002:2003 using SSE-

CMM," *Int. J. Comput. Sci. Inf. Secur.*, vol. 16, no. 1, pp. 139–147, 2018.
[6] Rosmiati, I. Riadi, and Y. Prayudi, "A Maturity Level Framework for Measurement of Information Security Performance Imam Riadi," *Int. J. Comput. Appl.*, vol. 141, no. 8, pp. 975–8887, 2016.
[7] N. Hermaduanti and I. Riadi, "Automation framework for rogue access point mitigation in ieee 802.1X-based WLAN," *J. Theor. Appl. Inf. Technol.*, vol. 93, no. 2, pp. 287–296, 2016.
[8] E. Hicham, B. Boulafdour, M. Makoudi, and B. Regragui, "Information security, 4TH wave," *J. Theor. Appl. Inf. Technol.*, vol. 43, no. 1, pp. 1–7, 2012.
[9] F. Latifi and H. Zarrabi, "A COBIT5 Framework for IoT Risk Management," *Int. J. Comput. Appl.*, vol. 170, no. 8, pp. 40–43, 2017.
[10] V. Konttinen, *Towards Disciplined Software Development*, no. May. 2016.
[11] J. F. Andry, "Audit of IT Governance Based on COBIT 5 Assessments: A Case Study," *J. Teknol. dan Sist. Inf.*, vol. 2, no. 2, p. 27, 2016.
[12] P. D. Syafitri, "Penilaian Kualitas Pengembangan Sistem Informasi Pada Perusahaan Distributor," *J. Sist. Inf. Bisnis*, vol. 10, no. 01, pp. 15–27, 2016.
[13] CMMI Product Team, *CMMI® for Development, Version 1.3*. 2010.
[14] P. Rahayu and D. I. Sensuse, "Penilaian Implementasi e-Government di PUSTEKOM Kemendikbud berbasis metode PEGI," *J. Sist. Inf. Bisnis*, vol. 02, pp. 139–145, 2017.
[15] A. Prasetyo and N. Mariana, "Analisis Tata Kelola Teknologi Informasi (It Governance) pada Bidang Akademik dengan Cobit FrameWork Studi Kasus pada Universitas Stikubank Semarang," *J. Teknol. Inf. Din.*, vol. 16, no. 2, pp. 139–149, 2011.