DECODE: Jurnal Pendidikan Teknologi Informasi
ISSN Cetak : 2775-2984 | ISSN Online : 2775-1813
Vol. 3, No. 2, September 2023, Hal: 296-309, Doi: http://dx.doi.org/10.51454/decode.v3i2.192
https://journal.umkendari.ac.id/index.php/decode

APPLICATION OF THE COBIT 2019 FRAMEWORK TO ANALYSE THE SECURITY OF ACADEMIC INFORMATION SYSTEMS

M. Khairul Anam[1)]*, Silvyana Dwi Putri[1)], Devi Yuliana[2)], Eva Yumami[3)], Tri Putri Lestari[4)]

[1] Department of Information Technology, STMIK Amik Riau, Pekanbaru, Indonesia
[2] Department of Business Digital, Riau Institute of Technology and Business, Pekanbaru, Indonesia
[3] Department of Informatics engineering, Polytechnic State of Bengkalis, Bengkalis, Indonesia
[4]Department of Information System, Rokan Institute of Technology, Rokan Hilir
Email: khairulanam@sar.ac.id

Abstract

STMIK Amik Riau implements an integrated information system to support a fast and real-time information management process where each service has its security. In this study, the analysis used to determine the maturity level of information system security governance was the COBIT 2019 framework with a CMMI scale. In COBIT 2019 the domains used were DSS05 and APO13. Based on the result of the analysis, the results of the average value of the overall maturity level on the security of the academic information system of STMIK Amik Riau were currently at level 3, which was defined. It meant that the security of the information system was running well but needed to be evaluated and optimized continuously. The value of each sub domain was 3.08 for the DSS05 sub domain (user), 3.35 for DSS 05 sub domains (maintainer), and 2.5 for APO13 sub domains (maintainer). Then the average result obtained from the gap was 0.53, meaning that the current level of maturity level with the desired maturity level is not too far away and can be increased by providing recommendations.

Keywords*: APO; COBIT 2019; DSS.*

IMPLEMENTASI COBIT 2019 UNTUK MENGANALISIS KEAMANAN SISTEM INFORMASI AKADEMIK

Abstrak

STMIK Amik Riau menerapkan sistem informasi yang terintegrasi demi mendukung proses manajemen informasi yang cepat dan *real-time* yang dimana di setiap layanan memiliki keamanannya. Dalam penelitian ini analisis yang digunakan untuk mengetahui tingkat kematangan tata kelola keamanan sistem informasi menggunakan *framework* COBIT 2019 dengan skala CMMI. Dalam COBIT 2019 domain yang digunakan adalah DSS05 dan APO13. Berdasarkan hasil analisis yang didapatkan bahwa hasil nilai rata-rata keseluruhan *maturity level* pada keamanan sistem informasi akademik STMIK Amik Riau saat ini berada pada level 3 yaitu *defined* artinya keamanan sistem informasinya sudah berjalan dengan baik tetapi perlu dievaluasi dan di optimalkan secara terus menerus, dengan nilai masing-masing sub domainnya adalah 3,08 untuk sub domain DSS05 (pengguna), 3.35 untuk sub domain DSS 05 (pengelola), dan 2.5 untuk sub domain APO13 (pengelola). Kemudian adapun hasil rata-rata yang didapat dari kesenjangan (*gap*) adalah 0,53 yang artinya level tingkat kematangan yang ada saat ini dengan tingkat level kematangan yang diinginkan tidak terlalu jauh dan dapat ditingkatkan dengan memberikan rekomendasi.

Kata kunci: APO; COBIT 2019; DSS.

Submitted: 10 Mei 2023	Reviewed: 11 Mei 2023	Accepted: 31 Mei 2023	Published: 17 Juli 2023

INTRODUCTION

Academic is a field that studies curriculum. The function of academics is to increase knowledge in terms of education, be able to convey and accept ideas of thought, science, as well as be able to test them honestly, openly, and freely that can be managed by an agency, one of which is the campus (Suhana *et al.*, 2022). Campus as an educational institution that has many divisions and staff and students who need an academic information system in order to help speed up obtaining information needs and be able to provide good benefits for the institution. However, along with the development of technology, it is often misused by some irresponsible parties which can pose a threat from the use of technology (Rizal and Yani, 2016). The Academic Information System is a purpose-built system that facilitates the management of various academic-related data. It encompasses a comprehensive range of information, such as student records, lecturer profiles, recording of lecture outcomes, curriculum details, and lecture schedules (Syafariani and Devi, 2019). One of the universities which has implemented an academic system is STMIK Amik Riau (Anam *et al.*, 2019).

STMIK Amik Riau implements an integrated information system to support a fast and real-time information management process which includes various services such as E-KRS, E-KTM, E-EDOM, and other information where each service has security (Zoromi, 2013). According to (Garfinkel, 1995) information security is how we can prevent fraud (cheating) or detect fraud in an information-based system, in which the information itself has no physical meaning and even has a necessity where security is intended to keep the system from being secured.

Security is very necessary because it can protect the data and information of a company or an institution from the disclosure of unauthorized people, and can optimize the performance of a company or institution (Mahfouz Alhassan and Adjei-Quaye, 2017). Information system security is something that must be considered in system management because if there is a leakage of information, it can damage one performance which will affect other works and can interfere with the smooth running of the system (Akpan *et al.*, 2022). After conducting an interview with the person in charge of system management, currently STMIK Amik Riau has never conducted a security evaluation of its academic system using COBIT 2019, so it is necessary to evaluate and analyse it in order to find out the shortcomings or weaknesses in the system and can provide recommendations from the results of determining the level of maturity of the system to increase the level currently owned to the expected level. There are several kinds of frameworks that can be used such as COBIT (Astuti *et al.*, 2017), ITIL (Anam *et al.*, 2020), PMBOK (Bastori *et al.*, 2020), ISO (Daryanto *et al.*, 2022) and others.

This study utilized COBIT 2019 in which many studies use it, such as XYZ Hospital Information System Security Governance Analysis Using COBIT 2019 (Gusni *et al.*, 2021), Application of the COBIT 2019 Framework to Information Technology Audit at Sambas Polytechnic (Saleh *et al.*, 2021) and others. The reason was because COBIT 2019 is a standard that is considered complete in carrying out governance and has a comprehensive scope, namely, defining components to build and sustain governance systems, processes, organizational structures, policies and procedures, information flows, skills, and infrastructure and defining that design factors are things that companies must consider to build the most appropriate and effective governance system (Gusni *et al.*, 2021). In addition, the campus can achieve risk optimization, governance and information system management.

COBIT 2019 consists of five key domains: Evaluate, Direct, and Monitor (EDM); Align, Plan, and Organize (APO); Build, Acquire, and Implement (BAI); Deliver, Service, and Support (DSS); and Monitor, Evaluate, and Assess (MEA). There are two domains that will be used for the analysis of the STMIK Amik Riau information system, namely DSS and APO. DSS is one of the knowledge management systems that has a role in supporting the decision-making process for a company or organization. The APO domain spans strategies and tactics, and identifies risks that are the best way IT can contribute to achieving goals. After getting the results from DSS and APO, measurements was taken by using the CMMI model so that the results by conducting this analysis are expected to be able to determine the level of maturity level in the system and the campus can increase the level of recommendations in this study.

METODE

Research Methodology is a technique compiled by researchers to collect data and information in conducting research that is in accordance with the subject and object under study (Adelia *et al.*, 2020). With these data, it is expected qualified results. Figure 1 is the flow of this research methodology.

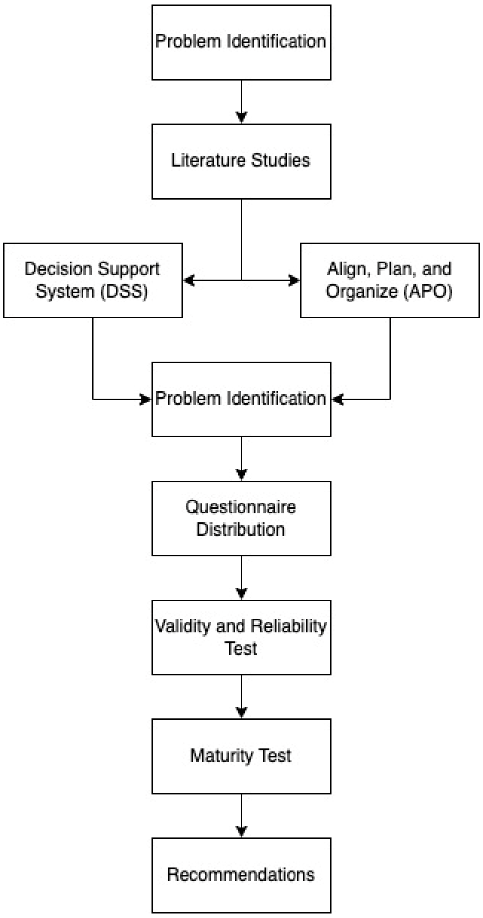
Problem Identification
Literature Studies
Decision Support System (DSS)
Align, Plan, and Organize (APO)
Problem Identification
Questionnaire Distribution
Validity and Reliability Test
Maturity Test
Recommendations

Figure 1. Research Methodology

Problem Identification

After establishing the research purpose, the initial step for researchers is to identify the specific problem to be addressed. This crucial process involves defining the boundaries of the problem to ensure that the study remains focused on its intended goals. In the present study, the problem identification process involved analyzing relevant studies and aligning them with the COBIT 2019 framework guidelines for information system security at STMIK Amik Riau. This analysis aimed to determine the maturity level of the system and assess its security level accordingly.

Literature Studies

The literature study carried out was by studying theories related to the topics discussed. Such as about COBIT 2019 and the domains that were used in this study, namely DSS and APO, as well as knowing the level of maturity through CMMI. Theories come from books, journals, and studies that support this research.

DSS and APO

This stage determined the sub domain and the questionnaire questions according to the selected sub domain with the determination of each sub-process.

1. Decision Support System (DSS)

Decision support system is one of the knowledge management systems that has a role in supporting the decision-making process for a company or organization. The sub domain was DSS 05 Manage Security Services. DSS 05 is a process that aims to protect the information of a company or institution and keep the level of risk thresholds in the company in line with existing security regulations (Imany *et al.*, 2019) as well as creating and managing information security roles and access rights and conducting security oversight. The sub-process consists of seven processes, namely:

a. DSS 05.01 (Protect against *malware*)
It implements and manages measurable prevention, investigations and improvements on (especially performing the latest updates on security and virus control) across campus lines to protect information systems and technology from *malware* (Krisdiyawan and Kuswantoro, 2017).

b. DSS 05.02 (Manage network and security connectivity)
It uses security measures and related management procedures to protect information systems on all connectivity (Wijaya and Andani, 2017).

c. DSS 05.03 (Manage device security)
It ensures that every device (such as laptops, servers, other mobile devices and software devices) is safe (protected) in accordance with the security requirements of the processing, storage or transmission of information (Woda and Bisma, 2020).

d. DSS 05.04 (Manage user identity and device remote access)
It ensures each user has access rights to the information they need regarding their business needs and coordinate with the business unit that manages the access rights (Imany *et al.*, 2019).

e. DSS 05.05 (Manage access to IT assets/devices)
It creates and implements procedures for granting, restricting and revoking access based on need. Access to the area must have the authority to enter and must also be monitored. All of these provisions shall apply to all faculty, student and outside staff (Firmansyah, 2021).

f. DSS 05.06 (Manage sensitive documents and output devices)
It creates physical security on IT devices for sensitive information system security (Woda and Bisma, 2020).

g. DSS 05.07 (Monitor infrastructure for security-related events/events)
Supervise infrastructure to prevent unauthorized access and ensure that events are integrated with the surveillance process (Imany *et al.*, 2019).

2. Align, Plan and Organize (APO)

It covers strategy and tactics and identifies concerns about how IT can best contribute to achievements. The sub domain was APO 13 Manage Security. APO 13 is a process that defines, executes, and oversees a system for information security management (Aritonang *et al.*, 2018).

The purpose of the process is to keep the impact and events of information security incidents at the risk threshold set by the manager (Imany *et al.*, 2019).

a. APO 13.01 (Create and maintain an information security management system)
   It creates and maintains an information security management system (SMKI) that provides a sustainable information security management approach, providing secure systems and business processes that are aligned with business needs and system security management (Gunawan and Tjahjadi, 2018).
b. APO13.02 (Define and regulate information security risk security plans)
   It manages information security design that describes how information security risks should be managed and aligned with agency strategies and infrastructure. It ensures that recommendations to implement security enhancements are based on an already approved and implemented business case (Shariff, 2018).
c. APO 13.03 (Monitoring and reviewing information security management systems)
   It manages and periodically communicates the needs and benefits of continuous improvement/improvement of information security. It is also collecting and analysing data, and improving effectiveness (Sepis, 2022).

Questionnaire Distribution

The data in this study was collected by using the RACI technique, which means Responsible, Accountable, Consulted, informed in the COBIT framework which was used for the determination process between the responsible parties in the organization. RACI Chart was explained below (Rachmat Widayanto and Rachmadi, 2019). The data was collected by distributing questionnaires to the chairmen of STMIK Amik Riau and SISFO who are part of the information system manager, and STMIK Amik Riau students who are users or recipients of information. Table 1 is the respondents in this study who were selected based on the RACI Model.

Table 1. Determination of RACI respondents

RACI	Description	Respondent
R (Responsible)	The person who serves as the person in charge and has the authority to make decisions in a case.	Chairman of STMIK Amik Riau
A (Accountable)	The person who is given the task of carrying out an activity or performing such work.	SISFO
C (Consulted)	The people deemed to have the authority to give necessary advice or advice.	Chairman of STMIK Amik Riau and SISFO
I (Informed)	Recipients of information or who must be given information or who must know the development of an activity carried out.	Students

1. Validity Test

Analysis of the questionnaire results was carried out to determine the level of validity and invalidity of the submitted questionnaire results. It is necessary to adjust the validity test. The test requirement is if the r count is ≥ r table, then the question is valid. If r count is ≤ r table, then the question is invalid. The result of the value obtained in the calculation was obtained by using the provisions of the existing facilities in the SPSS. The error level value used was 5%. The results showed that users were worth 0.413 with n=23 and managers were worth 0.997 with n=3.

2. Reliability Test

The calculation of the analysis of the questionnaire results taken by the researcher used the formulation of the calculation of alpha Cronbach interpretation. Cronbach's alpha performance was calculated by SPSS software. Reliability testing with Cronbach alpha can be seen from the Alpha value table, if the Alpha value is > from the r value of the table then it can be inferred that the value obtained is reliable. Conversely, if the Alpha value is < from the r value of the table then it can be said that the value obtained is not reliable.

Maturity Level

In measuring the maturity of the security level of the academic information system of STMIK Amik Riau, a questionnaire was used as a data collection method that had an index value of each of the criteria in the measurements carried out, namely using the following formula:

$$\text{Index} = \frac{\text{The number of answer scores}}{\text{Questionnaire}} \qquad (1)$$

Maturity level is part of COBIT which is used to measure or calculate IT process values which have levels from a scale of 0 to a scale of 5. Table 2 is the maturity level of COBIT.

Table 2. Maturity index

Maturity index	*Maturity Level*
0 – 0.49	*0 – Non-Existent*
0.51 – 1.50	*1 – Initial*
1.51 – 2.50	*2 – Repeatable but Intuitive*
2.51 – 3.50	*3 – Defined Process*
3.51 – 4.50	*4 – Managed and Measurable*
4.51 – 5.00	*5 – Optimized*

COBIT recommends that the current maturity level with the expected maturity level is only one level above it because each level must be met first before heading to the next one. After measuring the maturity level, the next step was to calculate the gap (GAP) which is the difference between the current maturity level and the maturity level which is expected by using the formula:

$$\text{Gap} = A - B \qquad (2)$$

Description:
A = degree of expected maturity.
B = degree of current maturity.
Analysis of this gap was carried out by identifying activities and improvements made by the information system security manager STMIK Amik Riau.

HASIL DAN PEMBAHASAN

Discussed the results and discussion of the implementation of the COBIT 2019 framework which was carried out to determine the maturity level in information system security at STMIK Amik Riau and provide recommendations for the desired conditions to increase the maturity level in accordance with the provisions desired by the determinants of the STMIK Amik Riau information system security decision. Before knowing the maturity level, the first step was to spread the questionnaire. Then the results of the questionnaire obtained from the response were processed. The following are the stages in processing questionnaire data.

Validity and Reliability

There were several results from respondents who filled out the questionnaire, where in testing the validity of the resulting higher value will show the accuracy of the data measurement tool, and while testing the reliability of the resulting indexes test will refer to how far the measurement tool is declared reliable.

1. **Validity Results**

Validity testing was carried out to determine the validity of a questionnaire of each variable. If the r count is ≥ r table, then it can be declared valid and if the r count is ≤ r table, then the data is declared invalid.
a. the results of the questionnaire validity on the users.
In this study, the error level value used was 5%, which was worth 0.413 with n = 23.

Table 3. User validity results.

Indicator	R Count	R Table	Description
Item 1	0.540	0,413	Valid
Item 2	0.842	0,413	Valid
Item 3	0.540	0,413	Valid
Item 4	0.557	0,413	Valid
Item 5	0.663	0,413	Valid
Item 6	0.842	0,413	Valid
Item 7	0.599	0,413	Valid
Item 8	0.740	0,413	Valid
Item 9	0.618	0,413	Valid
Item 10	0.535	0,413	Valid
Item 11	0.501	0,413	Valid
Item 12	0.609	0,413	Valid
Item 13	0.842	0,413	Valid
Item 14	0.501	0,413	Valid

From the results of the validity calculation in the table 3, it can be seen that r count is > r table in which fourteen questionnaires and all of them were declared valid because the result was more than the number of r tables, which was 0.413.
b. Validity results on the management questionnaire
The error level value used was 5% which was 0.997 with n=3.

Table 4. DSS05 validity results.

Indicator	R Count	R Table	Description
Item 1	1.000	0.997	Valid
Item 2	1.000	0.997	Valid
Item 3	1.000	0.997	Valid
Item 4	1.000	0.997	Valid
Item 5	1.000	0.997	Valid
Item 6	1.000	0.997	Valid
Item 7	1.000	0.997	Valid
Item 8	1.000	0.997	Valid
Item 9	1.000	0.997	Valid
Item 10	1.000	0.997	Valid

From table 4, it can be seen that there were ten valid data because the calculated r value was greater than the table r, which was 0.997.

Table 5. Validity results of APO13 maintainers

Indicator	R Count	R Table	Description
Item 1	1.000	0.997	Valid
Item 2	1.000	0.997	Valid
Item 3	1.000	0.997	Valid
Item 4	1.000	0.997	Valid
Item 5	1.000	0.997	Valid

Based on table 5, the results from the tests that had been carried out on three respondents with five questionnaires were declared valid because the results were more than the number of r tables, namely 0.997.

2. Reliability Results

To ensure the consistency of the questionnaire used in this research, a reliability test is necessary. Prior to conducting the test, a decision-making criterion is established with an alpha value of 0.60. Variables with values greater than 0.60 are considered reliable, while those with values lower than 0.60 cannot be deemed reliable. The following are the results of the reliability test conducted on the variables in this study:

a. The results of the questionnaire reliability on the user.

Table 6. User reliable results

Reliability Statistics	
Cronbach's Alpha	N of Items
.756	15

Based on the findings presented in Table 6, the results of the reliability test indicate that the Cronbach's alpha value for this variable exceeds the threshold value of 0.60, with a value of 0.756. This result signifies that all the statements included in the questionnaire are considered reliable and can be relied upon for further analysis.

b. The results the questionnaire reliability on the manager.

Table 7. Reliable results of managers

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.611	.456	14

Based on the findings presented in Table 7, the results of the reliability test indicate that the Cronbach's alpha value for this variable exceeds the threshold value of 0.60, with a value of 0.611. This result indicates that all the statements included in the questionnaire are considered reliable and can be trusted for further analysis.

Maturity Level Measurement

In measuring the maturity of the security level of the STMIK Amik Riau information system, a questionnaire was used as a data collection method that had an index value of each sub-domain process in the measurement to be carried out.

1. Assessment results

Following the completion of the questionnaire calculation process, the results revealed the values for each questionnaire item based on the total number of questions completed by 23 user respondents and three manager respondents. The following steps outline the calculation process for determining the index of each managed domain process.

a. User

To get the maturity value, it used equation 2, namely the number of questionnaire values divided by the number of questions.

Table 8. level maturity of DSS05 User

Sub domain process	Number of questionnaires	Number of questions	Value	Level	Description
DSS05.01	144	46	3.13	Lv 3	Defined
DSS05.02	139	46	3.03	Lv 3	Defined
DSS05.03	147	46	3.19	Lv 2	Defined
DSS05.04	139	46	3.02	Lv 3	Defined
DSSO5.05	133	46	2.89	Lv 3	Defined
DSS05.06	141	46	3.06	Lv 3	Defined
DSS05.07	150	46	3.26	Lv 3	Defined
Average			3.08	Lv 3	Defined

From table 8 which is the result of the recapitulation it can be seen that the DSS05 process is at level 3 with a maturity value of 3.08.

b. Manager

The following is *maturity* values for DSS05 and APO13 sub domains for managers.

Table 9. Manager-level maturity.

Domain process	Number of Questions	Number of questions	Proses sub domain	values	Level	Description	Average
DSS05	20	6	DSS05.01	3.33	Lv 3	Defined	3.35 Lv 3 (Defined)
	11	3	DSS05.02	3.66	Lv 3	Defined	
	7	3	DSS05.03	2.33	Lv 2	Repeatable	
	20	6	DSS05.04	3.33	Lv 3	Defined	
	11	3	DSSO5.05	3.66	Lv 3	Defined	
	11	3	DSS05.06	3.66	Lv 3	Defined	
	21	6	DSS05.07	3.5	Lv 3	Defined	
APO13	21	6	APO13.01	3.5	Lv 3	Defined	2,5

22	6	APO13.02	3.66	Lv 4	Managed	Lv 2 (Repeatable)
1	3	APO13.03	0.33	Lv 0	Non existent	

From the results of the recapitulation in table 9, it can be described, that currently the maturity level result in the DSS05 domain is 3.35 with level 3 which is defined, then in the apo13 domain it has level 2 with a maturity value of 2.5.

2. Gap analysis

Gap analysis helps to find deficiencies that must be overcome. It is easier to measure or identify them and in the long run, and help in making improvements. At this stage, the researcher performed a difference calculation, which was the result of the maturity level calculation that had been obtained previously by means of the expected maturity level value reduced by the current maturity level value.

a. Domain sub-process gap analysis

Table 10 is the result of the gap analysis subprocess. it can be seen that the gap obtained from the current maturity level as a whole in the domain will only increase 1 level from the expected maturity level. but there are several domains that have quite high gaps, especially PO13.03.

Table 10. Results of sub-process gap analysis.

Domain		**Maturity level**		
	Description	**Current maturity**	**Expected maturity**	**Gap**
DSS05.01	User	3.13	Lv 4 (3.51)	0.37
DSS05.02		3.02		0.48
DSS05.03		3.19		0.31
DSS05.04		3.02		0.48
DSS05.05		2.89		0.61
DSS05.06		3.06		0.44
DSS05.07		3.26		0.24
DSS05.01	Manager	3.33	Lv 4 (3.51)	0.17
DSS05.02		3.66		0
DSS05.03		2.33	Lv 3 (2.51)	0.18
DSS05.04		3.33	Lv 4 (3.51)	0.17
DSS05.05		3.66		0
DSS05.06		3.66		0
DSS05.07		3.5		0.01
APO13.01	Manager	3.5	Lv 4 (3.51)	0.01
APO13.02		3.66		0
APO13.03		0.33	Lv 1 (0.51)	0.17

b. Sub domain gap analysis

Table 11. Results of sub domain gap analysis.

Domain	Description	Maturity level Current maturity	 Expected maturity	Gap
DSS05	User	3.08	Lv 4	0.43
DSS05	Manager	3.35	(3.51)	0.16
APO13	Manager	2.51		1.00
Average				0.53

Based on the gap analysis shown in the table 11, there is a distance of 0.43 in the DSS05 domain from the user, 0.16 in the DSS05 domain from the manager, and 1.00 in the APO13 domain from the manager between the expected conditions. The biggest gap is in the APO13 domain. The average value of GAP is 0.53 which means that there is not too much difference for the expected conditions.

Recommendations

Recommendations were grouped into two views, namely recommendations from the user side and recommendations from the manager side.

1. User-side recommendations

There is already management related to access rights but it is too flexible, especially related to access to academic information system space at STMIK Amik Riau. So, it is recommended that the staffs who are responsible for it must make regulations that regulate the mechanism for requesting room access, asset access, and data access. Access granted must always be recorded and monitored. This mechanism must emphasize security. Granting access must be based on business needs, but it must not be too free to access the assets needed.

2. Recommendations from the management side

DSS05
They should create a custom logging that logs each security event or incident that occurs and each incident that occurs is assigned a unique identifier ID.

APO13

a. Conduct or revaluate access rights or redefine the terms of determination of parties entitled to access rights according to their functions.
b. Add infrastructure to run security management processes and conducting trainings aimed at improving human resource performance for the management team to optimize performance.
c. Security managers should implement recommendations that have been made from the results of the evaluation so that they can maximize performance.

CONCLUSION

The results of the overall average maturity level in the security of the academic information system of STMIK Amik Riau are currently at level 3, namely defined. The value of each sub domain is 3.08 for the DSS05 sub domain (user), 3.35 for the DSS 05 sub domain (manager), and 2.5 for the APO13 sub domain (manager). This level shows that the security governance of the information system at STMIK Amik Riau has been running or implemented but it needs updating, evaluation and must be ensured that the performance of the running process has supported the achievement of the goal of increasing the current level to the expected level by using gaps to find out the level gap.

The level gap for the expected level in system security at STMIK Amik Riau is not too big, which is worth 0.53 which means that STMIK Amik Riau can raise the level with several recommendations where the recommendations are related to system security. The recommendation is to make regulations that regulate the mechanism for requesting room access, asset access, and data access. Access granted must always be recorded and monitored. This mechanism must emphasize security and for granting access must be based on business needs, it must not be too free to access the assets needed. They must create a custom logging that logs each security event or incident that occurs and each incident that occurs is assigned a unique identifier ID.

Based on the conclusions described above, there are several suggestions that can be considered and evaluated for the security manager of the STMIK Amik Riau information system, namely the security manager is expected to consider implementing the proposal from the recommendations of the process submitted by the researcher. In addition, security managers are encouraged to make documentation after carrying out activities related to important data or infrastructure. This documentation is very useful as material for security evaluation in the future. Then the next researcher who will evaluate the security of the academic information system of STMIK Amik Riau can choose different process domains in COBIT 2019 and use different scales.

REFERENCES

Ardelia, F. F., Anam, M. K., Fitri, T. A., & Zoromi, F. (2020). Analisis Perspektif Pada Penerapan E-Money Menggunakan Delone and Mclean Is Success Model Di Bandara Sultan Syarif Kasim II Pekanbaru. *Jurnal Informatika dan Rekayasa Elektronik*, *3*(2), 100-110. https://doi.org/10.36595/jire.v3i2.256.

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network*, *2*(1), 123-138. 10.3390/network2010009.

Alhassan, M. M., & Adjei-Quaye, A. (2017). Information security in an organization. *International Journal of Computer (IJC)*, *24*(1), 100-116.

Anam, M. K., Lizarti, N., & Ulfah, A. N. (2019). Analisa Tingkat Kematangan Sistem Informasi Akademik STMIK Amik Riau Menggunakan ITIL V3 Domain Service Operation. *Fountain of Informatics Journal*, *4*(1), 8-12. 10.21111/fij.v4i1.2810.

Anam, M. K., Putra, A. R., Fadli, S., Firdaus, M. B., Suandi, F., & Lathifah, L. (2020). Audit teknologi informasi pada sistem perkreditan online terpadu bank xyz cabang perawang menggunakan itil v3. *Jurnal Manajemen Informatika dan Sistem Informasi*, *3*(2), 90-99. 10.36595/misi.v3i2.127.

Aritonang, I. J., Udayanti, E. D., & Iksan, N. (2018). Audit Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (APO13). *ITEJ (Information Technology Engineering Journals)*, *3*(2), 6-10.

Astuti, H. M., Muqtadiroh, F. A., Darmaningrat, E. W. T., & Putri, C. U. (2017). Risks assessment of information technology processes based on COBIT 5 framework: A case study of ITS service desk. *Procedia Computer Science*, *124*, 569-576. 10.1016/j.procs.2017.12.191.

Bastori, I., & Sriyana, S. (2020). Analisis Risiko Proyek PLTN Kalbar Dengan Pendekatan Model AHP dan PMBOK. *Jurnal Pengembangan Energi Nuklir*, *22*(1), 39-44. http://dx.doi.org/10.17146/jpen.2020.22.1.5976

Daryanto, D., Anam, M. K., Efendi, Y. and Rahmaddeni, R. (2022). Pengujian ISO 25010 Pada Smart Chair Akupresure Berbasis Internet Of Things (IoT). *JURNAL MEDIA INFORMATIKA BUDIDARMA*, 6(3), 1476-1483. 10.30865/mib.v6i3.4134.

Firmansyah, B. (2021). Sistem Informasi Manajemen Dan Layanan Aset Ti Menggunakan Framework Codeigniter. *TEKNIMEDIA: Teknologi Informasi dan Multimedia*, *2*(1), 8-16.

Garfinkel, S. (1995), *PGP: Pretty Good Privacy*, 1st ed.

Gunawan, R., & Tjahjadi, D. (2018). Audit Sistem Informasi Akademik Berbasis Web Menggunakan Framework Cobit 5.0 Pada Domain Apo13 Dan Dss05 (Studi Kasus: SIAT STMIK ROSMA KARAWANG). *Jurnal Interkom: Jurnal Publikasi Ilmiah Bidang Teknologi Informasi dan Komunikasi*, *13*(3), 29-40.

Gusni, R. S. A., Kraugusteeliana, K., & Pradnyana, I. W. W. (2021). Analisis Tata Kelola Keamanan Sistem Informasi Rumah Sakit XYZ Menggunakan Cobit 2019 (Studi Kasus pada Rumah Sakit XYZ). *Proceeding KONIK (Konferensi Nasional Ilmu Komputer)*, *5*, 434-439.

Imany, Y. D., Putra, W. H. N., & Herlambang, A. D. (2019). Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *3*(6), 5926-5935.

Krisdiyawan, R. D., & Kuswantoro, R. H. (2017). Audit keamanan sistem informasi pada rs mata dr. Yap yogyakarta menggunakan framework cobit 5. *Jurnal Ilmiah Manajemen Informasi dan Komunikasi*, *1*(1), 8-15.

Widayanto, S. R., Suprapto, S., & Rachmadi, A. (2019). Evaluasi Manajemen Teknologi Informasi Menggunakan Framework COBIT 5 Domain Monitoring, Evaluate, and Assess pada PT. PLN (Persero) Kantor Pusat. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *3*(7), 6956-6964.

Rizal, M., & Yani, Y. M. (2016). Cybersecurity policy and its implementation in Indonesia. *Journal of ASEAN Studies*, *4*(1), 61-78.

Saleh, M., Yusuf, I., & Sujaini, H. (2021). Penerapan Framework COBIT 2019 pada Audit Teknologi Informasi di Politeknik Sambas. *JEPIN (Jurnal Edukasi dan Penelitian Informatika)*, *7*(2), 204-209. 10.26418/jp.v7i2.48228.

Sepis, Y. T. (2022). Analisa Keamanan Sistem Informasi Menggunakan Framework COBIT 5 Dengan Domain DSS05 dan APO13 di PT XYZ. *TeIKa*, *12*(01), 35-42.

Shariff, M. N. (2018). Tata Kelola Penerapan Teknologi Informasi Pengelolaan Pajak Daerah di DPPKAD KAB. OKI Menggunakan Framework COBIT 5. *Seminar Nasional Teknologi Informasi dan Komunikasi (SEMNASTIK)*, 353-358.

Suhana, Mansyur, A., Liana, L. and Fauzan, M. (2022). Improving Student Academic Performance through Knowledge Sharing. *Hong Kong Journal of Social Sciences*, Vol. 60, 134-142.

Syafariani, R. F., & Devi, A. (2019, November). Web-Based Academic Information System. In *IOP Conference Series: Materials Science and Engineering* (Vol. 662, No. 2, p. 022042). IOP Publishing.

Wijaya, A. F., & Andani, A. T. (2017). Evaluasi Kinerja Sistem Informasi E-Filing Menggunakan Cobit 5 Pada Kantor Pelayanan Pajak Pratama Kota Salatiga. *Jurnal Terapan Teknologi Informasi*, *1*(1), 61-70, doi: 10.21460/jutei.2017.11.9.

Woda, J. R., & Bisma, R. (2020). Pembuatan Dokumen Prosedur Keamanan Informasi Yang Mengacu Pada Cobit 5 dan ISO 27001: 2013 Pada Badan Pengelola Keuangan Dan Aset Daerah Jawa Timur. *Journal of Emerging Information System and Business Intelligence (JEISBI)*, *1*(1), 51-59.

Zoromi, F. (2013). Perancangan Sistem Test Kompetensi Ujian Masuk Perguruan Tinggi (Studi Kasus STMIK-AMIK Riau). *Sains dan Teknologi Informasi*, *2*(1), 31-40.

How to cite:
Anam, M. K., Putri, S. D., Yuliana, D., Yumami, E., & Lestari, T. P. (2023). Application Of the Cobit 2019 Framework to Analyse The Security Of Academic Information Systems. *DECODE: Jurnal Pendidikan Teknologi Informasi, 3(2),* 296-309. http://dx.doi.org/10.51454/decode.v3i2.192