BAREKENG: Journal of Mathematics and Its Applications
December 2024 Volume 18 Issue 4 Page 2779–2794
P-ISSN: 1978-7227 E-ISSN: 2615-3017
https://doi.org/10.30598/barekengvol18iss4pp2779-2794

EVALUATION IT GOVERNANCE COMPUTER NETWORK AT CENTRAL BUREAU OF STATISTICS (BPS) MALUKU PROVINCE USING COBIT 2019 DSS01 AND DSS05 DOMAINS

Juins Carlo Radjulan[1*], Ade Iriani[2], Johan Tambotoh[3]

[1,2,3]*Department of Information Systems, Faculty of Information Technology, Universitas Kristen Satya Wacana*
Jl. Dr. O. Notohamidjojo No.1-10, Salatiga, 50715, Indonesia

*Corresponding author's e-mail: * **radjulanjuins@gmail.com***

Article History:

Received: 19th, June 2024
Revised: 11th, August 2024
Accepted: 9th,September 2024
Published:14th, October 2024

Keywords:

COBIT 2019;
Computer Network;
Central Bureau of Statistics Maluku Province.

ABSTRACT

This research aims to evaluate IT governance on the capability maturity level of computer networks at BPS Maluku Province using the COBIT 2019 Framework focusing on the DSS domain, namely DSS01 and DSS05. The research method uses qualitative and quantitative approaches by observing research objects, conducting interviews, and collecting data using a questionnaire distributed to the Maluku Province BPS office environment using saturation sampling techniques. The stages of this research were adapted to the COBIT 2019 framework. This research was measured using a Likert scale and utilized script apps, Google Cloud Platform, which was integrated with a web-based programming language. The results of this research show that the maturity level or capability maturity level in the DSS domain, namely the DSS01 subdomain, is 3.48 with a percentage of 69.70%. DSS05 is 3.47, with a rate of 69.47%. These two subdomains are still in the established process, level 3 with a GAP value of 2 for capability maturity level and the DSS01 domain GAP percentage of 30.30%. The DSS05 percentage is 30.53%, with a primarily achieved scale. Hopefully, this research will become a reference for improvements to several aspects that have been assessed and recommended so that computer network governance for services and activities at BPS Maluku Province becomes better.

How to cite this article:

J. C. Radjulan, A. Iriani and J. Tambotoh., "EVALUATION IT GOVERNANCE COMPUTER NETWORK AT CENTRAL BUREAU OF STATISTICS (BPS) MALUKU PROVINCE USING COBIT 2019 DSS01 AND DSS05 DOMAINS," *BAREKENG: J. Math. & App.*, vol. 18, iss. 4, pp. 2779-2794, December, 2024.

Journal homepage: *https://ojs3.unpatti.ac.id/index.php/barekeng/*
Journal e-mail: *barekeng.math@yahoo.com; barekeng.journal@mail.unpatti.ac.id*

Research Article · Open Access

1. INTRODUCTION

The Central Bureau of Statistics (BPS) is a non-ministerial government institution directly responsible to the President regarding collecting, processing, and providing statistical data relating to various social, economic, and demographic aspects [1]. Maluku Province BPS has implemented IT Standard Operating Procedures (SOP) in all service implementation and business processes to carry out each activity. Based on the Regulation of the Head of BPS Number 73 of 2016 concerning Principles of Information Technology Governance within the BPS, it is stated that every level of organization at BPS must and must comply with the principles of IT governance, as well as referring to the integration of government data through the Government System Electronic Based (SPBE). The implementation of the SPBE evaluation is aimed at measuring IT governance and improving e-government and the quality of public services as the key to successful digital transformation, including computer networks. Network evaluation can help monitor network performance, ensure that all connected devices function correctly, ensure compliance, and identify threats before they become major, high-risk problems [2]. According to data from the National Cyber and Crypto Agency (BSSN), cyber attacks against Indonesia in 2023 reached 403,990,813 anomalies through computer network traffic [3]. Therefore, one of the solutions that can be done to prevent this is to evaluate computer network governance because these things are interconnected, and it is essential to do so to avoid incidents that are detrimental to government agencies, including BPS Maluku Province.

In practice the Statistical Reference Network Team (JRS), which is fully responsible for all IT governance at BPS Maluku Province, has never carried out an evaluation and does not know the maturity level of the computer network, which is an important part of the IT infrastructure. This condition is a problem because it can affect services and activities at BPS Maluku Province which always relies on computer networks in its business processes. Therefore, it is necessary to carry out this research to evaluate IT governance regarding the level of computer network maturity. Research on IT governance has actually been carried out to measure the level of maturity or capability maturity level using the Control Objectives for Information and related Technology (COBIT) framework as in the research Yaniar et al. [4], Komalasari et al. [5], with the background of research objects at BPS. Then previous research, for example in research Sipayung et al. [6], Andry et al. [7], Saleh et al. [8], which discusses evaluation using COBIT.

The development of COBIT has led to the emergence of COBIT 2019 which is very flexible, lies in the coverage of specific topics and is focused on areas such as compliance with certain regulations [9]. Computer networks are an important part of IT infrastructure so they can be linked to COBIT 2019 as an IT governance framework [10]. However, there is still little previous research that specifically examines computer networks, such as research conducted by Dwi et al. [11], Hermawan et al. [12], by measuring the level of maturity of computer networks using the COBIT 2019 framework on domain parameters chosen based on collecting information on the research object. The results of this research indicate that the maturity level of network services from the APO12 (Managed Risk), DSS02 (Managed Service and Incidents) and DSS05 (Managed Security Services) domains is considered effective for evaluation so that network services can be improved periodically. Based on the background and mapping of these studies, it can be seen that the characteristics of the implementation of computer network IT governance in each research object are different, thus encouraging this research to be carried out to evaluate IT governance on the level of computer network maturity at BPS Maluku Province.

This research uses the COBIT 2019 framework because it is complete and flexible and can guide IT governance evaluation [13]. The domain that is the main focus of the assessment in this research is Deliver, Service, and Support (DSS) in Domains DSS001 and DSS05 because this area is considered the most critical, covering operations management and security of IT services and contains governance principles that are very relevant to internal computer networks every activity. DSS001 and DSS05 were chosen because they are tailored to the needs of this research object so that this research can formulate evaluation results for future computer network governance development. This research aims to evaluate IT governance on the capability maturity level of computer networks using the COBIT 2019 framework at BPS Maluku Province by measuring the value of each DSS01 and DSS05 subdomain activity, referring to relevant previous research and using qualitative and quantitative research methods. The results of this research are in the form of recommendations based on measuring the maturity level of computer network governance to illustrate the implementation of IT governance from the management and user side within the Maluku Province BPS environment. This research also provides evidence of the effective use of the COBIT 2019 framework as a reference in the future for evaluating and improving IT governance on computer networks.

2. RESEARCH METHODS

This research uses qualitative and quantitative methods in collaboration with the COBIT 2019 framework.

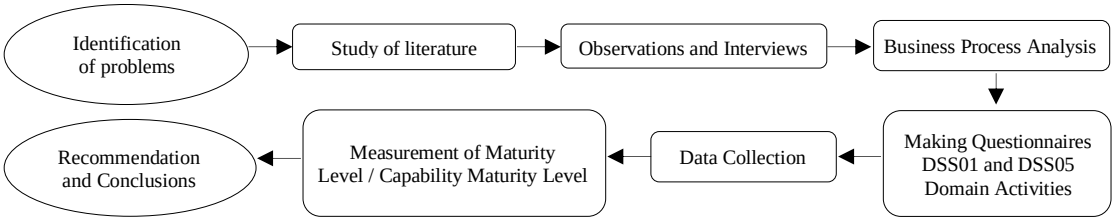

Figure 1. Research flow

As shown in **Figure 1**, research begins with problem identification to formulate the issue or problem that will be the main focus of the research. Next, a literature study was carried out to obtain information from journals, books, and articles related to this research that had already been published and were to be studied as a reference **[14]**. Observations are carried out by including specific factors and characteristics that are not limited to people, but each thing observed is based on the situation in the field **[15]**. Interviews in this research were conducted to obtain information and an overview of the problem so that the research information received was accurate **[16]**. Business process analysis in this research is to discover the IT processes occurring in the object of this research. The questionnaire was created by considering activities in the DSS01 and DSS05 domains. Data collection was carried out by distributing questionnaires to respondents and related stakeholders. The next stage is to measure the maturity or capability maturity level from the data collection results. The results of measuring the maturity or capability maturity level are then recommended.

2.1 Literature Review

Previous research relevant to this research is by Dwi et al. **[11]** at the College of Health Sciences. This research explains the advantages of using COBIT 2019 in being able to accurately and in detail measure the maturity level of network services in institutions focused on the Delivery, Service, and Support (DSS) domain, where the results in this domain obtain a process value at level 3 established process. It is assessed that each process has achieved its objectives, performance can be improved, and improvements can be made consistently.

Setiawan and Wasilah **[17]**, conducted research at the South Lampung Regency Communication and Informatics Service Office from a sample of 30 respondents. The models or domains that are the focus of this research are DSS03 and DSS05. This research shows that the capability level and maturity level values in the DSS03 objective domain are 1,84, with a percentage of 36,90% categorized as Partial. In comparison, the DSS05 domain gets a value of 2,57 with a rate of 51,50% and is in the Largely category. The expected to-be value is 4,00, while the as-is Domain DSS03 gets a value of 2,15, and the DSS 05 domain receives a value of 1,43. The results of this research are recommended and implemented to improve IT governance at the South Lampung Regency Communication and Information Office.

Other relevant research from Hermawan et al. **[12]**, carrying out evaluations to measure capability levels, assess GAP values, and suggest improvements to bank network infrastructure can use the COBIT 2019 governance framework and toolkit for factor design as well as being a tool to determine domains, where the research results show that the objective domain is APO12 (Managed Risk), DSS03 (Managed Problem), and DSS04 (Managed Continuity) have a capability value of level 3. On the other hand, the objective domains DSS02 (Managed Service Request and Incidents) and DSS05 have a capability value of level 2. The results of this research are considered to be a good solution for measuring management network infrastructure governance.

According to Pangaribuan and Fernandez **[18]** conducted research using COBIT 2019 to analyze IT utilization. The data collection method uses qualitative methods. Refer to the capability level suggestions in APO04 and DSS05. The results of the APO04 domain have a 2-level gap, and the DSS05 domain has a 3-level gap, which is considered to be an evaluation of processes related to innovation and technology adoption. The difference between previous research and this research lies in the methods, framework, and domains measured, as presented in **Table 1**.

Table 1. Research Comparison

Researcher	Method	Framework	Domain	Similarities
(Dwi Putra et al., 2020)	Qualitative	COBIT 2019	DSS02 and DSS05	Method : Qualitative Framework : COBIT 2019 Domain : DSS05
(Setiawan and Wasilah, 2022)	Descriptive	COBIT 2019	DSS03 and DSS05	Method : - Framework : COBIT 2019 Domain : DSS05
(Hermawan et al., 2023)	Qualitative and Qualitative	COBIT 2019	APO12, DSS03, DSS02 and DSS05	Method: : Qualitative and Qualitative Framework : COBIT 2019 Domain : DSS05
(Pangaribuan And Fernandez, 2023)	Qualitative	COBIT 2019	APO04 and DSS05	Method : Qualitative Framework : COBIT 2019 Domain : DSS05

Applying the COBIT 2019 framework from previous research has proven effective for evaluating IT governance in computer networks for both research objects in organizations, companies, and government agencies. In contrast to previous research compared in **Table 1**, the main focus of this research is on the DSS01 and DSS05 domains. Thus, the COBIT 2019 framework is a best practice for IT governance and management that can be applied **[19]**.

2.2 Framework COBIT 2019

COBIT 2019 is a further development framework from COBIT 5 which is considered the most complete globally because it includes existing framework standards **[13]**, **[20]**.

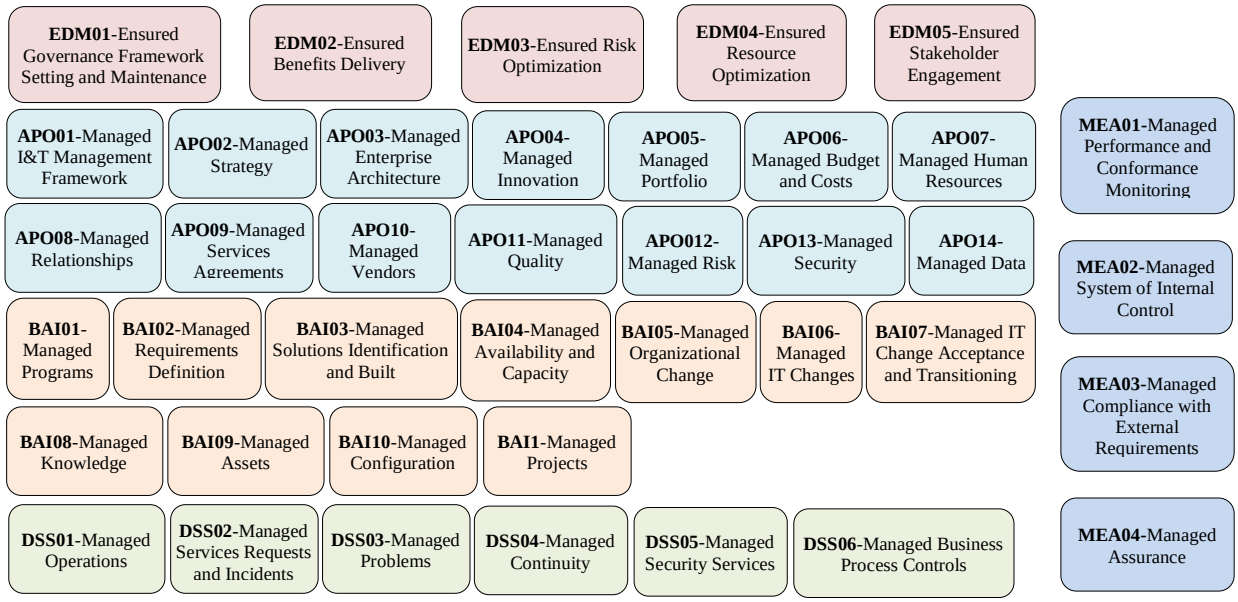

Figure 2. Core model COBIT 2019 (Source : ISACA, 2018)

As seen in **Figure 2**, the basic concept of the 2019 COBIT Framework, which comprehensively covers Governance and Management Objectives (GMO), is 40 core governance and management objectives, the processes contained therein, and other related components. There are processes aimed at governance, which are grouped in the EDM (Evaluate, Direct, and Monitor) domain. In contrast, those for management purposes are grouped in the APO (Align, Plan, and Organize), BAI (Built, Acquire, and Implement), domains DSS (Deliver, Service, and Support), and MEA (Monitor, Evaluate, and Assess). COBIT 2019 is a framework tool to help ensure governance bridges the gap between what needs to be done and how to do it at existing levels of risk and resource utilization **[7]**. The application of the COBIT 2019 framework is an evaluation framework that can help IT management, which is centered on managing operational activities **[22]**. COBIT 2019 can also help organizations set priorities by implementing more accurate governance designs **[23]**. The

governance components in COBIT 2019 contain seven components: processes, organizational structure, principles, policies and frameworks, information, culture, ethics and behavior of people, skills and competencies, services, infrastructure, and applications [24].

2.3 Deliver, Service, and Support (DSS)

The DSS domain is one of the governance domains incorporated in the core model of the COBIT 2019 framework and covers operational implementation for IT services, including security on computer networks [25]. In the COBIT 2019 framework mapping, the DSS domain is included in the Enterprise Goals (EG01), whose activities are related to the competitive products and services portfolio, and included in the Alignment Goals (AG05), whose activities are associated with the Delivery of Information and Technology (I&T) services in line with business requirements. The DSS domain in the COBIT 2019 framework includes:

1. DSS01 Managed Operations.
2. DSS02 Managed Services Request And Incidents.
3. DSS03 Managed Problems.
4. DSS04 Managed Continuity.
5. DSS05 Managed Security Services.
6. DSS06 Managed Business Process Controls.

This research only focuses on the DSS01 domain, which includes managed operations, and the DSS05 domain, which includes managed security services. In this section, the author describes the indicators that will be measured within the conceptual framework of the data collection method in Table 2.

Table 2. Conceptual Framework of Data Collection Methods

Domain	Data Collection	Data Source
DSS01 Managed operations	Observations, interviews, documents and questionnaires	Field observations, JRS Team / stakeholder interviews, strategic plan documents and IT SOP.
DSS05 Managed security services	Observations, interviews, documents and questionnaires	Field observations, JRS Team / stakeholder interviews, strategic plan documents and IT SOP.

Data Source : (Dwi Putra et al., 2020)

There are management practices in the DSS01 and DSS05 subdomains that are used as a reference for making questionnaire statements in this research. Activities represent the variables to be measured with subdomains. DSS01 has five subdomains, namely DSS01.01, DSS01.02, DSS01.03, DSS01.04, and DSS01.05, and there are several activities in each subdomain, which is the denominator value in calculating the maturity level. The total number of activities in the DSS01 domain is 33, as presented in Table 3.

Table 3. Management Practice and Activities Subdomain DSS01

Subdomain	Management Practice	Number of Activities
DSS01.01 Perform operational procedures	Carry out operational procedures and operational tasks reliably and consistently.	5
DSS01.02 Manage outsourced I&T services	Manage IT service operations to maintain protection of corporate information and reliability of service delivery.	4
DSS01.03 Monitor I&T infrastrlucture	Monitor IT infrastructure and related events. Records chronological information to reconstruct and review the timeline of operations and other activities surrounding or supporting operations.	6
DSS01.04 Manage the environment	There are stages for protection against environmental factors with special equipment and devices to monitor and control the environment.	7
DSS01.05 Manage facilities	Management of facilities, including electrical and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.	11

Data Source : Source : (ISACA, 2018)

Meanwhile, the DSS05 subdomain has 7 subdomains, namely DSS05.01, DSS05.02, DSS05.03, DSS05.04, DSS05.05, DSS05.06, and DSS05.07, with a total number of activities of 47, as presented in **Table 4**.

Table 4. Management Practice and Activities Subdomain DSS05

Subdomain	Management Practice	Number of Activities
DSS05.01 Protect against malicious software	Implement preventive measures, (especially up-to-date security patches and virus control) to protect IT systems from malicious software (e.g., ransomware, malware, viruses, worms, spyware, spam).	5
DSS05.02 Manage network and connectivity security	There are security measures and related management procedures in place to protect information through all connectivity methods.	9
DSS05.03 Manage endpoint security	Ensure that IT device endpoints are secured at a level that meets specified security requirements.	10
DSS05.04 Manage user identity and logical access	Ensure that all users have access rights to information according to their needs.	8
DSS05.05 Manage physical access to I&T assets	Implement procedures to grant, restrict access to locations, buildings and areas, according to business needs. Access to locations, buildings and areas must be recorded and monitored. This applies to everyone entering the premises, including staff, temporary staff, clients, vendors, visitors or other third parties.	7
DSS05.06 Manage sensitive documents and output devices	Establish appropriate inventory management physical safeguards regarding sensitive IT assets, such as critical documents.	5
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events	Ensure security tools, technology and detection are integrated with general event monitoring and incident management.	5

Data Source : Source : (ISACA, 2018)

2.4 Data collection

Data collection was carried out by distributing questionnaires to target respondents not only from IT managers or the JRS Team but also from users in the BPS environment of Maluku Province with classification criteria of respondents by gender, age and position, namely the general section with a total data sample of 1 respondent, five leaders team, functional and intermediary sections were nine respondents and BPS partners were 20 people. We took a sample of 35 people from a total population of 40 with an overall or saturated sampling referring to the sample determination table by Isaac and Michael **[26]**. Respondent classification is presented in **Table 5**.

Table 5. Respondent Classification

No	Respondents Criteria		Number of Respondents	Total Respondents
1	Gender	Male	18	35
		Female	17	
2	Age	0-17	2	35
		18-29	18	
		30-49	15	
		Above 50	0	
3	Position	Head of General Affairs	1	35
		Team Leader	5	
		Staff	9	
		BPS Partners	20	

Online questionnaire used for data collection by applying a 5 Likert scale with a value of (Strongly Disagree) STS value = 1, (Disagree) TS value = 2, (Neutral) N value = 3, (Agree) S value = 4, and (Strongly Agree) SS value = 5 and utilize script apps, Google Cloud Platform (GCP) is integrated with a web-based programming language as a tool for this research questionnaire.

2.5 Data Measurement

To calculate the capability maturity level and percentage in this research, use **Equation (1)**.

$$CL = \frac{T \times Pn}{\sum A \times \sum R} \quad (1)$$

Meanwhile, to calculate the maturity level in percent, **Equation (2)** is used.

$$AL = \frac{T \times Pn}{\sum A \times \sum S} \times 100\% \quad (2)$$

Description:

CL : Maturity value or capability maturity level
T : Total respondents who voted
Pn : Choice of Likert score numbers
$\sum R$: Number of respondents
AL : Percentage value
$\sum A$: Number of activities on the subdomain
$\sum S$: Maximum total score

2.6 Process Capability Maturity Scheme

Based on the Capability Maturity Model Integration (CMMI) standard contained in the COBIT 2019 framework, each process is a governance and management objective that can operate at various levels of capability, starting from 0 to 5 in this study according to the level of capability and its characteristics are explained in **Table 6**.

Table 6. Cability Level Process

Level	Description
0	Capabilities still need to be created, and there is no approach to addressing governance and management objectives or whether or not best practices are implemented.
1	This process of achieving goals through the implementation of incomplete activities can be categorized as intuitive and need to be more organized
2	This process achieves goals through basic, complete implementation and a series of activities that can be characterized as performance.
3	The process of achieving goals in a much more organized manner using organizational assets. Processes are usually well-defined.
4	This process achieves goals and is defined well, and its performance can be measured quantitatively.
5	This process achieves goals, defines and improves performance well (quantitatively), can be measured, and carries out continuous improvements.

Data Source : (ISACA, 2018)

In this study, an assessment scale table was used to determine the percentage of analysis with a scale of N (not achieved), P (partially achieved), L (partially achieved), and F (fully achieved) presented in **Table 7**.

Table 7. Rating Scale According to ISACA

Scale	Description	Percentage
N	Not achieved	0-15%
P	Partially achieved	16-50%
L	Largely achieved	51-85%
F	Fully achieved	86-100%

Data Source : (Hermawan, 2023)

3. RESULTS AND DISCUSSION

3.1 DSS01.01 Subdomain Calculation (Performing Operational Procedures)

In the DSS01.01 subdomain, the activity that is the variable being measured is performed by operational procedures. Respondents were asked to assess the level of maintenance and implementation of operational procedures and tasks shown in **Table 8**.

Table 8. Domain Activity Measurement Results DSS01.01

Activity	STS	TS	N	S	SS
Total	0	10	72	84	9

$$CL = \frac{(0\times1)+(10\times2)+(72\times3)+(84\times4)+(9\times5)}{5\times35}$$

$$CL = \frac{617}{175} = 3.53$$

$$AL = \frac{(0\times1)+(0\times10)+(72\times3)+(84\times4)+(9\times5)}{5\times175}$$

$$AL = \frac{617}{875}\times100 = 70.51\%$$

The calculation results for the DSS01.01 subdomain obtained a value of 3.53 or 70.51%. These results indicate that the implementation of governance of performance activities and results of IT activities is well scheduled and is always responsive in monitoring incidents and problems related to operational procedures and taking appropriate action to improve the operations carried out.

3.2 DSS01.02 Subdomain Calculation (Manage Outsourced I&T Services)

This activity refers to facilities where agencies can collaborate with third parties for IT needs. The assessment results on the DSS01.02 domain are presented in **Table 9** bellow:

Table 9. Domain Activity Measurement Results DSS01.02

Activity	STS	TS	N	S	SS
Total	0	5	70	48	17

$$CL = \frac{(0\times1)+(5\times2)+(70\times3)+(48\times4)+(17\times5)}{4\times35}$$

$$CL = \frac{497}{140} = 3.55$$

$$AL = \frac{(0\times1)+(5\times2)+(70\times3)+(48\times4)+(17\times5)}{4\times175}$$

$$AL = \frac{497}{700}\times100 = 71.00\%$$

In the DSS01.02 subdomain, we obtained the maturity value calculation at 3.55 or 71.00%, which shows that implementing governance at points is good enough to ensure that internet or network service providers in agencies also have independent audit planning for the IT operational environment.

3.3 DSS01.03 Subdomain Calculation (Monitor I&T Infrastructure)

Respondents were asked to assess the implementation of monitoring and identifying a list of IT assets in infrastructure so that this can be measured in the DSS01.03 subdomain shown in **Table 10**.

Table 10. Domain Activity Measurement Results DSS01.03

Activity	STS	TS	N	S	SS
Total	0	4	123	72	11

$$CL = \frac{(0\times1)+(4\times2)+(123\times3)+(72\times4)+(11\times5)}{6\times35}$$

$$CL = \frac{720}{210} = 3.43$$

$$AL = \frac{(0\times1)+(4\times2)+(123\times3)+(72\times4)+(11\times5)}{6\times175}$$

$$AL = \frac{720}{1050}\times100 = 68.57\%$$

In the DSS01.03 subdomain, the calculated value was 3.43 for the maturity value of 68.57%. These results show that IT management is carried out quite well, considering that monitoring functions, recording events, and identifying problems are essential for evaluating risk and performance.

3.4 DSS01.04 Subdomain Calculation (Manage The Environment)

The DSS01.04 subdomain is assessed to ensure proactive action is taken to detect environmental threats such as fire, water, smoke, and humidity to the IT infrastructure. The results of the respondents' assessments are presented in **Table 11**.

Table 11. Domain Activity Measurement Results DSS01.04

Activity	STS	TS	N	S	SS
Total	0	0	126	86	7

$$CL = \frac{(0\times1)+(0\times2)+(126\times3)+(86\times4)+(7\times5)}{7\times35}$$

$$CL = \frac{809}{245} = 3.30$$

$$AL = \frac{(0\times1)+(0\times2)+(126\times3)+(86\times4)+(7\times5)}{7\times175}$$

$$AL = \frac{809}{1225}\times100 = 66.04\%$$

In the DSS01.04 subdomain, we obtained the maturity value calculation at 3.30 or 66.04%, which means that IT infrastructure protection management has been implemented well enough so that it can be protected from environmental threats.

3.5 DSS01.05 Subdomain Calculation (Manage Facilities)

IT facility management in the DSS01.05 subdomain is assessed to provide an overview of agency operations through the availability of supporting equipment such as generators. This subdomain also assesses computer network cable management according to network topology. The assessment results on the DSS01.05 domain are presented in **Table 12** bellow:

Table 12. Domain Activity Measurement Results DSS01.05

Activity	STS	TS	N	S	SS
Total	0	0	173	177	32

$$CL = \frac{(0\times1)+(0\times2)+(173\times3)+(177\times4)+(32\times5)}{11\times35}$$

$$CL = \frac{1393}{385} = 3.62$$

$$AL = \frac{(0\times1)+(0\times2)+(173\times3)+(177\times4)+(32\times5)}{11\times175}$$

$$AL = \frac{1393}{1925}\times100 = 72.36\%$$

In the DSS01.05 subdomain, we obtained the maturity value calculation at 3.62 or 72.36%. These results indicate that management in this subdomain is quite good regarding IT equipment and provides reports regarding facility incidents.

3.6 DSS05.01 Subdomain Calculation (Protect Against Malicious Software)

In the DSS05.01 subdomain, respondents were asked to assess the implementation of software protection in processing facilities, updating software regularly to avoid external threats, for example ransomware, malware, viruses, worms, spyware and spam. The results of this subdomain assessment can be seen in **Table 13**.

Table 13. Domain Activity Measurement Results DSS05.01

Activity	STS	TS	N	S	SS
Total	0	7	92	65	11

$$CL = \frac{(0\times1)+(7\times2)+(92\times3)+(65\times4)+(11\times5)}{5\times35}$$

$$CL = \frac{605}{175} = 3.46$$

$$AL = \frac{(0\times1)+(7\times2)+(92\times3)+(65\times4)+(11\times5)}{5\times175}$$

$$AL = \frac{605}{875}\times100 = 69.14\%$$

In the DSS05.01 subdomain, we obtained the maturity value calculation at 3.46 or 69.14%. These results indicate that management of this subdomain is relatively low due to limited human resources in the JRS team and a lack of training or regular knowledge sharing about the dangers of ransomware, malware, viruses, worms, spyware, and spam in the use of email and internet networks by training users not to open. However, it reports suspicious emails and does not install non-recommended or unapproved software.

3.7 DSS05.02 Subdomain Calculation (Manage Network and Connectivity Security)

In subdomain DSS05.02, respondents were asked to rate the implementation of approved security protocols for network connectivity. The results of the assessment on this subdomain are displayed in **Table 14**.

Table 14. Domain Activity Measurement Results DSS05.02

Activity	STS	TS	N	S	SS
Total	0	25	156	99	35

$$CL = \frac{(0\times1)+(25\times2)+(156\times3)+(99\times4)+(35\times5)}{9\times35} \qquad AL = \frac{(0\times1)+(25\times2)+(156\times3)+(99\times4)+(35\times5)}{9\times175}$$

$$CL = \frac{1089}{315} = 3.46 \qquad AL = \frac{1089}{1575}\times100 = 69.14\%$$

In the DSS05.01 subdomain, we obtained the maturity value calculation at 3.46 or 69.14%. These results indicate that system integrity protection is the steps taken to prevent, detect, and respond to interference or unauthorized changes to computer systems or software carried out in the network are good enough.

3.8 DSS05.03 Subdomain Calculation (Manage Endpoint Security)

Subdomain DSS05.03 respondents were asked to assess whether there is a mechanism for installing software such as an operating system in a safe manner and whether it has an official license from the company that created it. In this subdomain, an assessment is also carried out regarding the implementation of good filtering on network traffic in the installation and the availability of media for data backup, which are displayed in **Table 15**.

Table 15. Domain Activity Measurement Results DSS05.03

Activity	STS	TS	N	S	SS
Total	0	10	168	113	59

$$CL = \frac{(0\times1)+(10\times2)+(168\times3)+(113\times4)+(59\times5)}{10\times35} \qquad AL = \frac{(0\times1)+(10\times2)+(168\times3)+(113\times4)+(59\times5)}{10\times175}$$

$$CL = \frac{1271}{350} = 3.63 \qquad AL = \frac{1271}{1750}\times100 = 72.63\%$$

The results of the assessment calculations on the DSS05.03 subdomain regarding maturity level obtained a value of 3.63 or 72.63%. These results show that every operating system in the agency uses an official license. Meanwhile, network traffic filtering and the availability of data backup media have been implemented quite well.

3.9 DSS05.04 Subdomain Calculation (Manage User Identity And Logical Access)

In subdomain DSS05.04, respondents were asked to assess the existence of coordination with other teams in the agency to ensure that the computer systems and networks used in the agency were monitored stable to assist operations. The results of this subdomain are presented in **Table 16**.

Table 16. Domain Activity Measurement Results DSS05.04

Activity	STS	TS	N	S	SS
Total	0	0	152	104	24

$$CL = \frac{(0\times1)+(0\times2)+(152\times3)+(104\times4)+(24\times5)}{8\times35} \qquad AL = \frac{(0\times1)+(0\times2)+(152\times3)+(104\times4)+(24\times5)}{8\times175}$$

$$CL = \frac{992}{385} = 3.54 \qquad AL = \frac{992}{1400}\times100 = 70.86\%$$

In the DSS05.04 subdomain, we obtained the maturity value calculation at 3.54 or 70.86%. This means managing access rights by the roles, primary duties, and responsibilities of stakeholders and positions in the agencies and functions in the managed organizational structure has been carried out quite well.

3.10 DSS05.05 Subdomain Calculation (Manage Physical Access to I&T Assets)

In the DSS05.05 subdomain, respondents were asked to assess the implementation of access restrictions to locations, buildings, and areas such as server rooms by recording when entering vital IT objects are displayed in **Table 17**.

Table 17. Domain Activity Measurement Results DSS05.05

Activity	STS	TS	N	S	SS
Total	0	60	104	61	20

$$CL = \frac{(0\times1)+(28\times2)+(7\times3)+(0\times4)+(0\times5)}{7\times35} \qquad AL = \frac{(0\times1)+(28\times2)+(7\times3)+(0\times4)+(0\times5)}{7\times175}$$

$$CL = \frac{776}{245} = 3.17 \qquad AL = \frac{776}{1225}\times100 = 63.35\%$$

In the DSS05.05 subdomain, we obtained the maturity value calculation at 3.17 or 63.35%. Thus, this subdomain was deemed to have been carried out incorrectly and could pose a risk to the vital objects of this agency in the future.

3.11 DSS05.06 Subdomain Calculation (Manage Sensitive Documents and Output Devices)

In subdomain DSS05.04, respondents were asked to assess the availability of cryptographic methods to protect sensitive information or data stored electronically and regulate the receipt, use, deletion, destruction, and disposal of sensitive documents and IT devices displayed in **Table 18**.

Table 18. Domain Activity Measurement Results DSS05.06

Activity	STS	TS	N	S	SS
Total	0	3	87	61	24

$$CL = \frac{(0\times1)+(3\times2)+(87\times3)+(61\times4)+(24\times5)}{5\times35} \qquad AL = \frac{(0\times1)+(3\times2)+(87\times3)+(61\times4)+(24\times5)}{5\times175}$$

$$CL = \frac{631}{175} = 3.61 \qquad AL = \frac{631}{875}\times100 = 72.11\%$$

The results of the assessment calculations on the DSS05.06 subdomain regarding maturity level obtained a value of 3.61 or 72.11%. In this way, protecting sensitive information and documents and managing data is considered to have been carried out quite well.

3.12 DSS05.07 Subdomain Calculation (Manage vulnerabilities and monitor the infrastructure for security-related events)

DSS05.07 subdomain measurements were carried out to assess the implementation of cyber attack risk scenarios so that these scenarios can be easily recognized and can be prevented, presented in **Table 19**.

Table 19. Domain Activity Measurement Results DSS05.07

Activity	STS	TS	N	S	SS
Total	0	9	86	72	8

$$CL = \frac{(0\times1)+(9\times2)+(86\times3)+(72\times4)+(8\times5)}{5\times35} \qquad AL = \frac{(0\times1)+(9\times2)+(86\times3)+(72\times4)+(8\times5)}{5\times175}$$

$$CL = \frac{604}{175} = 3.45 \qquad AL = \frac{604}{875}\times100 = 69.03\%$$

The maturity value calculation for the DSS05.07 subdomain was found to be 3.45 or 69.03%. Thus, the implementation of JRS is quite capable of identifying security-related events.

3.13 Summary of Results

Summary of the results of measuring the maturity level or capability maturity level in the DSS01 domain data with subdomain DSS01.01 values of 3.53 or 70.51%, DSS01.02 of 3.55 or 71.00%, DSS01.03 of 3.43 or 68.57%, DSS01.04 was 3.30 or 66.04%, and DSS01.05 was 3.62 or 72.36%. The average value obtained was 3.48 or 69.70%, which is presented in **Table 20** below:

Table 20. DSS01 Domain Analysis Results

Subdomain	Description	Capability Maturity Level	Achievement Rate
DSS01.01	(Perform operational procedures)	3.53	70.51%
DSS01.02	(Manage outsourced I&T services)	3.55	71.00%
DSS01.03	(Monitor I&T infrastructure)	3.43	68.57%
DSS01.04	(Manage the environment)	3.30	66.04%
DSS01.05	(Manage facilities)	3.62	72.36%
	Average	3.48	69.70%

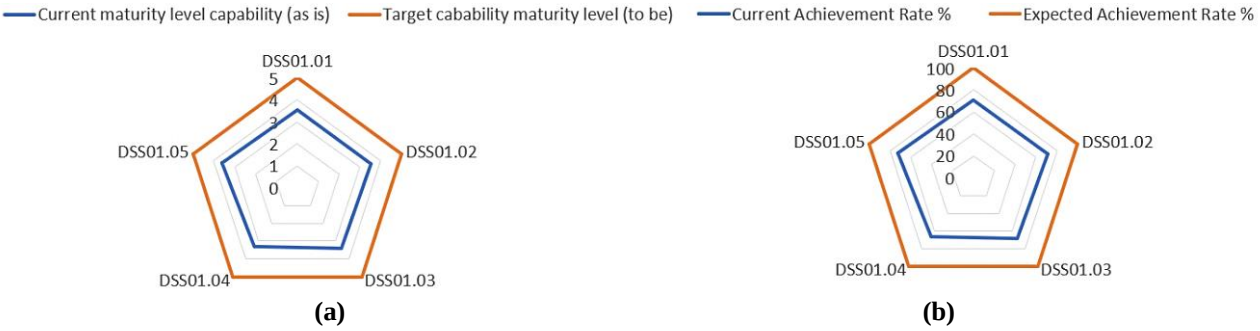

Figure 3. Graph of DSS01 Subdomain calculation results
(a) Capability maturity level (b) Achievement level

Based on **Figure 3**, the results of measuring the maturity level of the DSS01 domain have reached level 3.48 but have yet to reach the expected target of the capability maturity level, namely a value of 5.00. The percentage in this domain has reached 69.70% and has yet to reach the expected value, namely 100%. Meanwhile, in the summary of the results of measuring the maturity level or capability maturity level in the DSS05 domain data, the subdomain DSS05.01 value is 3.46 or 69.14%, DSS05.02 is 3.46 or 69.14%, DSS05.03 is 3.63 or 72.63%, DSS05.04 of 3.54 or 70.86%, DSS05.05 of 3.17 or 63.35%, DSS05.06 of 3.61 or 72.11% and DSS05.07 of 3.45 or 69.03% and the average value obtained was 3.47 or 69.47% which is presented in **Table 21** below:

Table 21. DSS05 Domain Analysis Results

Subdomain	Description	Capability Maturity Level	Achievement Rate
DSS05.01	(Protect against malicious software)	3.46	69.14%
DSS05.02	(Manage network and connectivity security)	3.46	69.14%
DSS05.03	(Manage endpoint security)	3.63	72.63%
DSS05.04	(Manage user identity and logical access)	3.54	70.86%
DSS05.05	(Manage physical access to I&T assets)	3.17	63.35%
DSS05.06	(Manage sensitive documents and output devices)	3.61	72.11%
DSS05.07	(Manage vulnerabilities and monitor the infrastructure for security-related events)	3.45	69.03%
	Average	3.47	69.47%

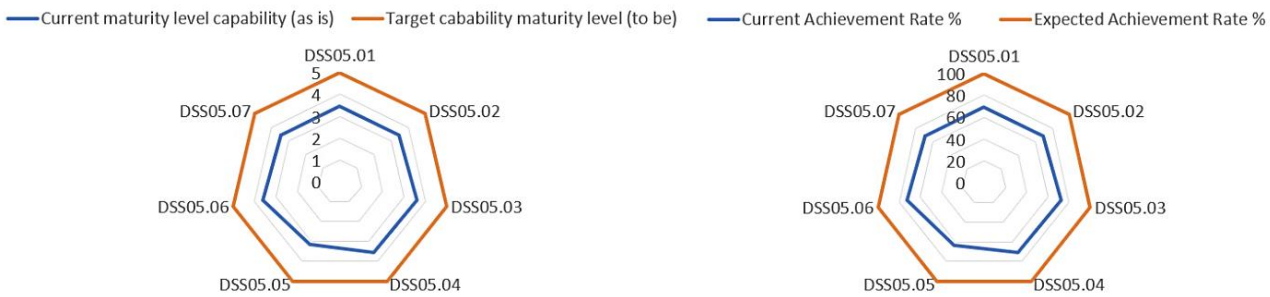

Figure 4. Graph of DSS05 subdomain calculation results
(a) Capability maturity level (b) Achievement level

Based on **Figure 4**, the results of measuring the maturity level of the DSS05 domain have also reached level 3.47 but have not yet reached the expected capability maturity level target, namely a value of 5.00. The percentage in this domain has also reached 69.47% and has yet to reach the expected value, namely 100%.

The analysis shows that the average results for these two domains have not reached the expected target, and it is known that the GAP in the DSS01 domain is 1.52 and DSS05 is 1.53, which means that each domain is still at level 3 or in the (L) largely scale achieved. The results of the GAP analysis can be seen in **Table 22** below:

Table 22. GAP Analysis Capability Maturity Level

Domain	Capability Maturity Level (As is)	Target Capability Maturity Level (to be)	Scale	GAP
DSS01	3.48	5.00	L	1.52
DSS05	3.47	5.00	L	1.53

Analysis of the level of achievement shows that the GAP domain DSS01 reached a value of 30.30% and a value of 30.53% for the DSS05 domain, which means that each domain is still below the target percentage and is included in the scale (L) largely scale achieved. The results of the GAP analysis can be seen in **Table 23** below:

Table 23. Achievement Level GAP Analysis

Domain	Current Level of Achievement	Expected Level of Achievement	Scale	GAP
DSS01	69.70%	100 %	L	30.30 %
DSS05	69.47%	100 %	L	30.53 %

Recommendations are the final result of this research so that they can be a reference for improving governance by the DSS01 and DSS05 domains in this research, as explained in **Table 24.**

Table 24. Recommendation

Findings	Recommendation
DSS01.01 (Manage Endpoint Security)	
The JRS team has not optimally managed performance activities in IT activities on a regular basis. However, the team is always responsive in monitoring incidents and problems related to operational procedures and taking appropriate action.	The recommendation that can be given is to plan activity management activities by referring to the agency's SOP and Strategic Plan documents so that the results achieved can be maximized.
DSS01.02 (Manage Outsourced I&T Services)	
Two network service providers are running to support business processes; the team can also collaborate with third parties to develop services on computer networks.	There needs to be performance planning, change management, configuration management, service requests, incident management, problem management, security management, and regular reporting.

Findings	Recommendation
DSS01.03 (Monitor I&T Infrastructure)	
The JRS team needs to identify and monitor the network optimally and regularly in the history log.	It would be good to have a special analysis method and use computer network tools to view history logs or use more complex hardware, such as a router that supports the latest network technology, as well as an exemplary configuration so that you can monitor computer network activity in detail and completely to provide a report if something happens. Incidents and can assist with investigations if requested at a later date.
DSS01.04 (Manage The Environment)	
In this subdomain, it was found that IT governance was not considered good enough in its implementation, one of which was related to alarms connected to fire protection systems or local emergency authorization networks such as fire brigades, which were still not implemented in agency networks.	It is necessary to understand IT SOP for the entire team and understand the importance of a fire protection system where the main components of the alarm include sensors, control units, and sirens that are connected to a network and can proactively detect threats from the environment to minimize the risk of an unexpected disaster desired.
DSS01.05 (Manage Facilities)	
There is no proper depiction of the computer network topology, so repairs to the infrastructure will become more complex. However, the availability of operational support tools is considered good.	It is necessary to design a computer network topology description so that it makes it easier for the JRS team to configure and minimize installation costs because the advantages or disadvantages have been calculated properly in the network topology picture.
DSS05.01 (Protect Against Malicious Software)	
This subdomain focuses on filtering in computer networks carried out by the JRS team against external threats such as malware, phishing, and spam emails to periodically review and evaluate new threats such as sabotage, IoT attacks, AI attacks, and deepfakes.	The JRS team is expected to take part in training, such as seminars or workshops on how to prevent outside threats so that they can recognize new methods that can harm the agency. The JRS team is also advised to share knowledge with all teams in the agency to remain alert to actions that are not recommended, such as installing applications from unknown sources or containing patches and cracks and opening emails or links that are not recognized or whose source is doubtful.
DSS05.02 (Manage Network and Connectivity Security)	
This subdomain shows that the agency still needs to optimally implement network filtering mechanisms such as firewalls or proxy servers so that it can have an impact on risks to network security, data, and network quality.	It is recommended that security protocols be implemented using suitable hardware, software, and filtering mechanisms to minimize risks, and it is necessary to test the protection and security capabilities of computer network systems regularly.
DSS05.03 (Manage Endpoint Security)	
There are other devices for data backup functions. Apart from that, a software installation mechanism has been implemented using an official license. Device locking has also been implemented according to good password standards.	The operating system updates and periodic password changes are regularly checked.
DSS05.04 (Manage User Identity and Logical Access)	
Access rights management is by stakeholder roles, duties, and responsibilities and is managed well.	Monitoring is needed to ensure that all users (internal, external, and temporary) and their activities on the IT system (data input applications, use of IT infrastructure, and system operations) can be identified and run well.
DSS05.05 (Manage Physical Access to I&T Assets)	
Findings in this subdomain describe the less-than-optimal implementation of SOPs in limiting and monitoring functions for vital IT objects, which can be a severe risk.	It is recommended that SOPs be updated regarding establishing perimeter boundaries for server rooms or vital IT objects by implementing mandatory rules and supported by real-time monitoring using CCTV connected to the network so that agencies can prevent problems and risks from occurring in the future.
DSS05.06 (Manage Sensitive Documents and Output Devices)	
This subdomain is considered to be quite good in its management and implementation.	This can be improved by learning new methods for protecting sensitive data electronically to avoid future threats.

Findings	Recommendation
DSS05.07 (Manage Vulnerabilities and Monitor The Infrastructure for Security-Related Events)	
This subdomain is considered not optimal in identifying events related to cyber security.	Regularly record security events and practice cyberattack scenarios such as phishing attack simulations.

4. CONCLUSIONS

The COBIT 2019 framework can be used to measure the level of capability maturity in computer network IT governance in BPS Maluku Province based on the results of measuring the average value of the two DSS01 and DSS05 domains, namely the DSS01 domain is 3.48 or 69.70%, the GAP is 1 .52 or 30.30% and the average DSS05 domain value is 3.47 or 69.47%, GAP is 1.53 or 30.53%. Thus, these two domains are included in the mainly achieved (L) scale; in other words, they are at level 3, so there are recommendations according to the findings in each sub-subdomain, measured as evaluation material. The limitations of this research lie in the time and small number of samples. Suggestions or recommendations that can be given to achieve a better level of maturity: agencies can pay attention to the components that make up IT governance based on the COBIT 2019 framework, especially processes, principles, policies, and procedures, so that the results obtained can be appropriate and maximized.

ACKNOWLEDGMENT

The highest appreciation is expressed to BPS Maluku Province for allowing the author to carry out this research, to all Lecturers at the Department of Information Systems, Faculty of Information Technology, especially the Supervisors and also Satya Wacana Christian University, which allowed the author to pursue postgraduate studies.

REFERENCES

[1] Pejabat Pengelola Informasi dan Dokumentasi Badan Pusat Statistik, "Informasi Umum BPS." Accessed: Jan. 25, 2024. [Online]. Available: https://ppid.bps.go.id/app/konten/0000/Profil-BPS.html

[2] P. Rosati, F. Gogolin, and T. Lynn, "Cyber-security incidents and audit quality." Accessed: May 13, 2024. [Online]. Available: http://doras.dcu.ie/25939/1/Rosati%20et%20al.%20%282020%29%20-%20Cyber-security%20Incidents%20and%20Audit%20Quality%20-%20Final%20Version.pdf

[3] Badan Siber dan Sandi Negara (BSSN), "LANSKAP KEAMANAN SIBER INDONESIA." Accessed: Jul. 13, 2024. [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[4] R. Yaniar Sianida, F. Nur Afiana, and R. Wahyudi, "IS Governance Evaluation Using COBIT 5 Framework on the Central Statistics Agency of Banyumas District," *Journal of Computer Science and Engineering (JCSE)*, vol. 1, no. 1, pp. 1–9, Feb. 2020, doi: 10.36596/jcse.v1i1.9.

[5] Y. Komalasari *et al.*, "Audit Pendataan Registrasi Sosial Ekonomi Kabupaten XYZ Dengan COBIT 4.1." [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/infortech168

[6] A. B. Sipayung, R. Yunis, and E. Elly, "Evaluation Of Information Technology Governance at Mikroskil University Using COBIT 2019 Framework with BAI11 Domain," *International Journal of Research and Applied Technology*, vol. 2, no. 2, pp. 128–143, Dec. 2022, doi: 10.34010/injuratech.v2i2.8085.

[7] J. F. Andry and A. K. Setiawan, "IT GOVERNANCE EVALUATION USING COBIT 5 FRAMEWORK ON THE NATIONAL LIBRARY," *Jurnal Sistem Informasi*, vol. 15, no. 1, pp. 10–17, Apr. 2019, doi: 10.21609/jsi.v15i1.790.

[8] M. Saleh, I. Yusuf, and H. Sujaini, "Penerapan Framework COBIT 2019 pada Audit Teknologi Informasi di Politeknik Sambas," *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, vol. 7, no. 2, p. 204, Aug. 2021, doi: 10.26418/jp.v7i2.48228.

[9] M. Lestari, A. Iriani, and H. Hendry, "Information Technology Governance Design in DevOps-Based E-Marketplace Companies Using COBIT 2019 Framework," *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 6, no. 2, pp. 233–252, Aug. 2022, doi: 10.29407/intensif.v6i2.18104.

[10] D. Espinosa, C. Arias, P. Palma, and F. Fernàndez-Peña, "Impact of an Augmented Reality Environment in Learning Computer Networks Principles," 2024, pp. 125–133. doi: 10.1007/978-981-99-8894-5_11.

[11] S. Dwi Putra, A. Yudhana, A. D. Dahlan Jl Soepomo Sh, K. Umbulharjo, K. Yogyakarta, and D. Istimewa Yogyakarta, "Evaluasi Tata Kelola Layanan Jaringan Menggunakan COBIT 2019 Pada Sekolah Tinggi Ilmu Kesehatan," vol. 5, no. 2.

[12] S. D. Hermawan, I. Hermadi, and Y. Nurhadryani, "Evaluasi Capability Level Infrastruktur Jaringan TI Bank XYZ Menggunakan Cobit 2019," *Syntax Literate ; Jurnal Ilmiah Indonesia*, vol. 7, no. 12, p. 18274, Jan. 2023, doi: 10.36418/syntax-literate.v7i12.10851.

[13] Information Systems Audit and Control Association, *COBIT® 2019 Framework : introduction and methodology*.

[14] O. Purwaningrum, "STUDI LITERATUR : FRAMEWORK COBIT 5 PADA TATA KELOLA TEKNOLOGI INFORMASI," *SCAN - Jurnal Teknologi Informasi dan Komunikasi*, vol. 16, no. 2, Oct. 2021, doi: 10.33005/scan.v16i2.2598.

[15] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatig, dan R&D*. Bandung: Alfabeta, 2018.
[16] T. D. N. B. Mira, E. Sediyono, and A. Iriani, "Audit Evaluasi Pemanfaatan Sistem Informasi Akademik di Universitas Kristen Wira Wacana Sumba Menggunakan Framework Cobit 5," *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 6, no. 1, p. 337, Jan. 2022, doi: 10.30865/mib.v6i1.3334.
[17] R. A. Setiawan and W. Wasilah, "Evaluasi Tata Kelola Dan Manajemen Teknologi Informasi Menggunakan Framework Cobit 2019 Pada Dinas Komunikasi Dan Informatika Kabupaten Lampung Selatan".
[18] B. A. M. Pangaribuan and S. Fernandez, "Tata Kelola Teknologi Informasi Menggunakan COBIT 2019 Pada Val," *JURNAL ILMIAH KOMPUTER GRAFIS*, vol. 16, no. 1, pp. 196–208, 2023, doi: 10.51903/pixel.v16i1.1247.
[19] R. K. Sari, R. H. Ginardi, and A. S. Indrawanti, "Perancangan Tata Kelola Teknologi Informasi Berbasis COBIT 2019: Studi Kasus di Divisi Information Technology PT Telkom Indonesia Kota Bandung," *JURNAL TEKNIK ITS*, vol. Vol. 12, no. No. 1, 2023.
[20] A. Safitri, I. Syafii, and K. Adi, "Measuring the Performance of Information System Governance using Framework COBIT 2019," *Int J Comput Appl*, vol. 174, no. 31, pp. 23–30, Apr. 2021, doi: 10.5120/ijca2021921253.
[21] Information Systems Audit and Control Association., *COBIT 2019 Framework Governance and Management Objectives*. Information Systems Audit and Control Association, 2018.
[22] A. F. B. Magalhães, C. M. do Nascimento, C. N. Carr, and I. H. M. da Silva, "Estrutura de Governança de T.I: Aprimorando a eficiência e eficácia com o modelo COBIT como framework," in *TECNOLOGIAS AVANÇADAS E SUAS ABORDAGENS -V1*, Seven Editora, 2023. doi: 10.56238/tecavanaborda-016.
[23] A. Fernandes *et al.*, "A Flexible Method for COBIT 2019 Process Selection," 2020. [Online]. Available: https://aisel.aisnet.org/amcis2020/strategic_uses_it/strategic_uses_it/3
[24] Rini Audia and B. Sugiantoro, "Evaluation and Implementation of IT Governance Using the 2019 COBIT Framework at the Department of Food Security, Agriculture and Fisheries of Balangan Regency," *IJID (International Journal on Informatics for Development)*, vol. 11, no. 1, pp. 152–161, Aug. 2022, doi: 10.14421/ijid.2022.3381.
[25] A. Simatupang and H. J. Adrianto, "Audit Tata Kelola Teknologi Informasi dalam Mendukung Penerapan Good Corporate Governance (Studi Kasus PT XYZ)," *Jurnal Sistem Informasi Bisnis*, vol. 14, no. 2, pp. 162–170, Apr. 2024, doi: 10.21456/vol14iss2pp162-170.
[26] S. Isaac and W. B. Michael, *Hand Book in Research and Evaluation*, 2nd Edition. San Diego, California: Edit Publishers, 1981.