Indonesian Journal of Engineering, Science and Technology
IJENSET
Volume 01 – Issue 01, February 2024
e-ISSN: xxxx-xxxx; p-ISSN: xxxx-xxxx
Journal Link: https://jurnal.umla.ac.id/index.php/ijenset/index

ANALYSIS OF NETWORK SERVICE SECURITY MATURITY LEVEL USING COBIT 2019 FRAMEWORK

Dimas Adi Kurniawan[1], Mala Rosa Aprillya[2] and Eko Handoyo[3*]

*Corresponding Author Email: eko_handoyo@umla.ac.id

[1,2&3]*Study Program of Computer Engineering; Faculty of Science Technology and Education;Universitas Muhammadiyah Lamongan; Lamongan 62218; Indonesia*

Article Information

Submitted	:	25th August 2023
Revised	:	5th May 2024
Accepted	:	5th May 2024
Paper page	:	1-13
DOI	:	xxx

ABSTRACT

The background of this research is to analyze the maturity level of network service security using the COBIT 2019 framework with maturity levels. This research was conducted to determine the maturity level of network service security using the COBIT 2019 domain DSS05 framework. The research method used is descriptive quantitative with the 2019 cobit approach, DSS05 domain, DSS05.01 subdomain to DSS05.07 subdomain, using a maturity level. The data obtained from the results of the questionnaire based on the DSS05 sub domain include, 826 DSS05.01, 810 total DSS05.02, 820 total DSS05.02, 799 total DSS05.04, 762 total DSS05.05, 725 .06 DSS05, DSS05. 07 is 782. Then it will be calculated using the maturity level formula and will get results that have been measured based on the DSS05 subdomain, the DSS05.01 subdomain index result is 3.67 at level 4, the DSS05.02 index result is 3.6 at level 3, the DSS05.03 index result 3.64 at level 4, DSS05.04 index result 3.55 at level 4, DSS05.05 index result 3.38 at level 3, DSS05.06 index result 3.22 at level 3, and DSS05 .07 result index of 3.47 at level 3.

Keywords—*Analysis, Cobit, Network, Maturity, Security*

I. INTRODUCTION

The use of information technology is currently growing rapidly in all fields, along with the increasing functional needs of the organization to achieve the desired goals (Putra, 2022). Technological developments affect social, cultural and economic dynamics of society (Fitriani, 2018). Technology that is successful in supporting the dynamics of people's lives is getting better, with character and strength (Rahmawati, 2008)). It is hoped that this increase will be able to develop in accordance with technological advances so as to support the intellectual abilities of the

community to compete in the future. Discussing technological issues means discussing the development and progress of human civilization (Fitriani, 2018). The higher the human etiquette, the more it supports the ability to communicate and socialize. Technology and communication support products are currently growing rapidly in people's lives. Both in supporting work needs and personal needs. Information technology is a general term for all technologies that support humans in creating, changing, storing, communicating and or disseminating information (Fitriani, 2018). Investment in the field of information technology in an organization mostly aims to be able to make a positive contribution to the performance of individual members of the organization and its institutions. Information technology, especially computer technology, has the potential to improve individual and organizational performance, therefore many decision makers invest funds in information technology (Rahmawati, 2008). Besides that, the rapid development of information technology in the work environment has made the use of information technology an urgent problem (Rahmawati, 2008).

The use of information technology is currently growing in all fields, along with the increasing functional needs of organizations to achieve goals (Putra, 2022). In government agencies the use of Information Technology is very important in supporting the effectiveness of public services so knowledge and efficient resources are needed (Agoan, 2017). Alignment between information technology management goals that match the vision, mission, and business goals and strategies must be considered. In the use of information technology is closely related to the network. The internet network is currently being used by various groups of children, adolescents, to adults, even parents have all used the internet both for social networking, information search, and other needs related to the internet (Nurcahyo, 2020).

Security on the network is very necessary, because computer users are very aware that the convenience of using computers in our daily lives is the most basic thing, because of its functions such as automation, aerospace, medicine and health, scientific research, criminal investigations and so on, computers have an important role irreplaceable (Munawar, 2020). There is a lot of information in the industry that is highly confidential, because this information cannot be understood by irrelevant people, otherwise it will cause irreparable losses (Munawar, 2020). It is precisely because of the high confidentiality of computer information that some people with malicious intent have the idea of committing a crime and always hope to get some benefits from computer network security vulnerabilities. Computer network security technology continues to develop, and the criminal technology of these criminals also continues to develop (Munawar, 2020). There are important things that need to be done, namely doing a good job in preventing computer network security, to minimize the possibility of computer crime (Munawar, 2020).

Computer network security does not consist of one aspect, but contains four important links: software, network hardware, Internet of Things services and shared resources. According to the definition of computer network security by the International Organization for Standardization, computer network security refers to the protection of hardware, software and data resources in a computer system from being destroyed, modified or security holes due to accidental or malicious reasons, so that the computer system continues to operate reliably, as well as regular computer services (Munawar, 2020).

So it cannot be denied that the internet is a necessity for everyone. One of the Internet Service Provider (ISP) users is Muhammadiyah Lamongan University. For an agency engaged in the education sector, which is not far from network services. To achieve this goal, it is

necessary to evaluate it so that it can measure the maturity level of network service security and find out the level of the agency using a COBIT 2019 framework. COBIT (Control Objectives for Information and Related Technology), is one of the important standards and effective to apply.

The Control Objective for Information and related Technology (COBIT) is a framework for the governance and management of enterprise information and technology. Enterprise information and technology refers to all information technology and processing implemented by the enterprise, not just by the information technology and department. The COBIT framework divides governance and management activities.

According to COBIT, governance includes activities to ensure that stakeholder needs, conditions and choices are evaluated to determine appropriate business objectives, ensure direction is set by taking into account priorities and decision-making, and ensure that the performance and compliance of each element of the company is monitored based on agreed objectives. Meanwhile, management includes planning, building, executing and monitoring activities carried out in accordance with the directions set by governance in order to achieve company goals (ISACA, 2018).

Updates to COBIT 2019 are based on COBIT 5, another authoritative source and will be supported in future by the user community. The COBIT 2019 product suite is open and designed for customization. COBIT 2019 provides several publications including (ISACA, 2018): 1. COBIT 2019 Framework: Introduction and methodology. Explains the key concepts of COBIT 2019. 2. COBIT 2019 Framework: Governance and management objectives. Describes the 40 core objectives of governance and management, existing processes, and other components. 3. COBIT 2019 Design Guide: Designing technology and information governance solutions. Describes the design of factors that can affect governance and includes workflows for designing customized governance systems for enterprises. 4. COBIT 2019 Implementation Guide: Implementing and optimizing technology and information governance solutions. This is a change from the COBIT 5 implementation guideline and the development of a road map for continuous improvement of governance.

COBIT 2019 has two principles, namely principles that explain the core requirements of a governance system for technology and information companies and principles as a governance framework that can be used to build a governance system for companies. The following are COBIT 2019 principles as a governance system for technology and information companies:

1. Companies need a governance system to meet stakeholder needs and generate value or benefits from the use of technology and information.
2. Governance systems for enterprise IT are built from multiple components of various types and work together holistically.
3. The governance system must be dynamic as the factor design changes.
4. The governance system must clearly distinguish between governance and management structures and activities.
5. The governance system must be adapted to the needs of the company using a series of design factors as parameters.
6. The governance system should cover the entire company.

The following are the 2019 COBIT principles as a governance framework that can be used to build a corporate governance system:

1. The governance framework should be based on a conceptual model, identify the main components and the relationships between these components, and be able to maximize optimization and deliver possibilities. automation
2. The governance framework should allow for flexibility and openness.

3. The governance framework can align standards, frameworks and key regulations as appropriate.

COBIT 2019 divides the focus of objectives into two, namely governance and management objectives. From this goal is divided into five domains. In governance objectives, grouped in a domain named Evaluate, Direct and Monitor (EDM) which has 5 core models. The EDM domain discusses the governance structure of evaluating strategic choices, directing senior management in making strategic choices and overseeing every achievement of the strategy. In management objectives, they are grouped into four domains, namely (ISACA, 2018):

1. Align, Plan, and Organize (APO) discusses the overall organization, strategy, and supporting activities. There are 14 core models in the APO domain.
2. Build, Acquire and Implement (BAI) discusses the definition of threats, results, and implementation of technology and information and ensures alignment between technology and information solutions and business processes. There are 11 core models in the BAI domain.
3. Monitor, Evaluate, and Assess (MEA) discusses performance monitoring and conformity of technology and information with targets, internal goals and external needs. There are 4 core models in the MEA domain.
4. Deliver, Service, and Support (DSS) discusses operational delivery of information technology and its supporting services. There are 6 core models in the DSS domain.

Delivery, Service, and Support (DSS05)

DSS05 is a process in COBIT 5 with a focus on managing security services in organizations to maintain information security risks within predetermined safe limits (ISACA, 2012). Base Practices and Work Products based on the assessment of this process are Installation Operation Procedure Documents and Software Monitoring, data classification activities, Firewall & Antivirus Logs, Access Rights Operation Procedure Documents, Software Licensing Operation Procedure Documents and IT Security Operation Procedure Documents. In addition, there is also a data classification implementation that has been carried out but no written documents have been found explaining the data classification carried out by the company.

Delivery, Service and Support (DSS), includes actual delivery, service or services, and support or provision of services for the business, including data management and information protection related to business processes.

DSS is a COBIT 2019 domain that deals with operational IT, such as service delivery, security and continuity management, user service support, and data management and operational facilities. In a DSS domain there are sub-domains

1. Protect against malware (DSS05.01) implement and maintain enterprise-wide preventive, detective and remedial measures to protect information systems and technology from malware.
2. Manage network security and connectivity (DSS05.02) using security measures and related management procedures to protect information from all connectivity methods.
3. Manage endpoint security (DSS05.03) provides assurance that endpoints (eg laptops, desktops and servers) are guaranteed to be at the same level or greater than the approved security requirements.
4. Manage user identities and logical access (DSS05.04) to ensure that all users have information access rights according to business needs. They and coordinate with the business division that manages access rights.
5. Manage physical access to IT assets (DSS05.05) determine and implement procedures for granting, limiting and revoking access to physical buildings.

Building conditions and areas according to business needs, including emergencies. Access to buildings, structures and areas must be justified, recognized, recorded and monitored.

6. Manage sensitive documents and output devices (DSS05.06) install physical safeguards. In terms of documents related to the palace. So that all document output is standardized in security.
7. Monitor infrastructure for security related events (DSS05.07) using intrusion detection tools, to monitor infrastructure for unauthorized access rights and ensure each event is integrated with event monitoring and event management.

One of the measurement tools for the performance of an information technology system is the maturity level model, this type of maturity is used to control information technology processes with an assessment method with the aim that the organization can determine the maturity level of current information technology and the organization can continuously align and try to improve level up to the highest level so that the governance aspects of information technology run smoothly (Syaputra, 2020).

This study aims to determine the level maturity of network services at the Muhammadiyah University of Lamongan, so that efforts in improve network services more controllable, effective, and efficient. IT service request if possible incidents in network governance universities as well as related security services system. Safety identification includes actions related to prevention, identification, and response to security threats system.

II. METHOD

A. Research materials and tools

Research materials that will be used by the authors include the results of surveys and observations that have been made. These ingredients include: Muhammadiyah Lamongan University network data and network service security data at Muhammadiyah Lamongan University.

In this study, the authors used research tools in the form: Questionnaire, Interviews with related parties (head of IT, IT staff) and Cobit Framework 2019.

B. Research procedure

In this study, the procedure for collecting information used as research material is:

List of questions

Questionnaires were carried out directly to related parties to find out how the level of maturity and security quality of network services at Muhammadiyah University Lamongan was, data collection used the questionnaire method by collecting data consisting of 35 questions based on the DSS05 sub domain that had been created and addressed to 45 sources. people consisting of 3 IT people, 17 lecturers and 25 students. From the questionnaire that has been distributed which is in accordance with the 2019 Cobit framework standard and is given an assessment with a Likert scale where in this questionnaire there are 5 assessments as in the following table:

Table 1. Questionnaire Assessment

Mark	Category
1	Don't agree
2	Doubtful
3	Agree
4	Strongly agree
5	Strongly disagree

Interviews

interviews were conducted to obtain information in the form of questions and answers with respondents as a support for the results of the questionnaire.

C. Research Flow

To determine the maturity level of network service security, the authors use the method of quantitative descriptive analysis. Quantitative descriptive analysis method was used in this

study to determine and explain the results of the questionnaires that have been distributed.

(1) Identification of problems

Problem identification is carried out to find or find out the security quality of network services, then look for the maturity level of network services that will be used as research objects using the cobit 2019 Domain DSS05 framework.

(2) Literature Study

Literature study is carried out by looking for references to data sources in the form of journals, articles, books or other relevant sources related to the object of research.

(3) Data Collection

Data collection was in the form of interviews conducted to obtain more information about the object of research and questionnaires by making a list of questions based on the standards contained in the 2019 COBIT framework regarding the maturity level of network service security. The selected respondents were 45 people, namely 3 IT people, 17 lecturers and 25 students.

(4) Data Processing Maturity Level

Table 2. Maturity level criterion value

Level	Criteria	Information
1	0,0 – 1,50	Initial
2	0,51 – 2,50	Managed and measurable
3	2.51 – 3,50	Defined process
4	3,51 – 4,50	Managed and measurable
5	4,51 – 5.00	Optimised

Data processing in the form of data that has been obtained is then collected, is quantitative in nature by direct assessment of the relevant parties using a checklist with a Likert scale. After obtaining the total results for each DSS05 sub domain, it will then be calculated using a maturity index which will determine the current maturity level and analyze the maturity level gap by calculating the current maturity level with the desired target.

$$Maturity\ index = \frac{total\ value\ of\ the\ answer}{total\ value\ of\ the\ questionnaire}$$

According to (CMMI Product Team, 2010) the CMMI model places institutions at 5 Maturity Levels or maturity levels in CMMI, namely:

- Level 1: Initial or Initial process. In this condition, any institution at this level is an institution that has not implemented CMMI.
- Level 2: Managed or Managed. Institutions have several processes that are often used in every development project, but there is no overall uniformity.
- Level 3: Defined or Defined. The institution has carried out a defined process and all teams understand how the process should work.
- Level 4: Quantitatively Managed or managed quantitatively. Institutions are increasingly structured and open with the existing system. They began to apply the concept of quantification in every process, and always monitored and controlled in every work process. optimization is constantly monitored and analyzed. So as to provide an optimal system.
- Level 5: Optimizing or Optimizing. This level is the peak level in the CMMI model. At Maturity Level 5, an institution has achieved all of the specific and generic goals at Level 2, 3, 4, and 5. The focus on continuous process improvement through technological innovation and process

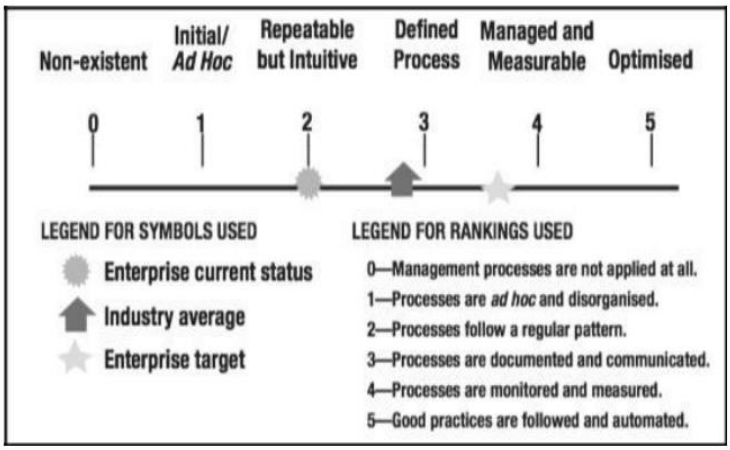

Figure 1. Maturity Level Scale

Information :

- Level 0: Non-existent: There is no related process at all.
- Level 1: Initial/Ad hoc: The stage where management is aware of the importance of paying attention to related processes, but the implementation that occurs is still reactive, according to sudden needs that exist and is not organized.
- Level 2: Repeatable but intuitive: The stage where management already has a pattern for managing related processes based on repeated experiences that have been done before. However, this pattern has not been standardized.
- Level 3: Defined (Defined process): The stage where management has succeeded in creating and communicating related process management book standards even though it has not been carried out in an integrated manner.
- Level 4: Managed and measurable: The stage where existing activities and standards have been formally implemented and integrated. And there are also indicators to measure performance progress quantitatively for management.
- Level 5: Optimizing (Optimised): The stage where management has committed to the existing process so that it can become a best practice that is always being developed.

III. RESULT AND DISCUSSION

A. DSS05 Validation With Security Aspects

This validation is a DSS05 analysis of the Cobit 2019 framework with security parameters namely Confidentiality, Integrity and Availability. DSS05.01 which protects against malicious software states that security validation is confidential, DSS05.02 processes network security and connectivity states that security validation is confidential, DSS05.03 manages endpoint security states that security validation is confidential and integrity, DSS05.04 managing user identity and logical access stating that security validation is confidential and available, DSS05.05 managing physical access to assets and IT stating that security validation is integrity and availability, DSS05.06 managing sensitive documents and output devices stating that security validation is integrity, DSS05.07 manage vulnerabilities and monitor infrastructure for security-related events.

Interview result

Table 3. Security Aspect

No	DSS code	C	I	A
1	DSS05.01	✓		
2	DSS05.02	✓		
3	DSS05.03	✓		✓
4	DSS05.04	✓		
5	DSS05.05		✓	
6	DSS05.06		✓	
7	DSS05.07		✓	

Network Switch is a network component that has the function of connecting to several computer devices in several networks. This stage allows users to exchange data and information to the desired device. Then the Access Point functions as an internet signal generator, besides that it also functions as a comprehensive connectivity arrangement. In addition, the Network Server is a device that is useful for channeling wired to wireless connections.

IT Backbone including the need for access to information is unavoidable with one another and is expected to be able to communicate well, for example students can access lecture information, academic services, payment status information and other activities that will always use information technology. Muhammadiyah Lamongan University is required to be able to serve the entire academic and non-academic community. The need to develop an IT backbone as the backbone of a computer network is absolutely necessary and really good because without a backbone, all internal and external communications can be disrupted. In addition, there are also the results of research interviews which reveal that the development of Muhammadiyah University of Lamongan 2019 – 2024 leads to increased services in the field of Information Technology and the development of a world class university with a variety of information technology-based services.

a. Information Technology Infrastructure Consolidation
b. Improving services in the academic field based on information technology (cybercampus)
c. Improving service facilities supporting the teaching and learning process by using e-learning.
d. Improving e-mail, blog and hosting facilities for the academic community.
e. Providing the best graduates of Muhammadiyah Lamongan University with provision in the field of information technology through seminars, courses.
f. Establish cooperation with information technology vendors such as Google, Microsoft, Cisco and other vendors related to information technology.

B. Network Service Security Maturity Level

The results of the questionnaire that has been given to the respondent and have been filled in by the respondent then get the results.

Sub domain DSS05.01Protect against malicious software with the answer criteria that can be Strongly Agree frequency 9 and a percentage of 20%, Agree with a frequency of 19 and a percentage of 42%, Doubtful with a frequency of 10 and a percentage of 22%, Disagree with a frequency of 5 and a percentage of 11%, Strongly disagree with a frequency of 2 and a percentage of 4%.

Sub domain DSS05.02 Manage network security and connectivity with the criteria for answers that can Strongly agree frequency 11 and a percentage of 24% , Agree with a frequency of 14 and a percentage of 31%, Doubtful with a frequency of 14 and a percentage of 31%, Disagree with the frequency 4 and a percentage of 8%, Strongly disagree with a frequency of 2 and a percentage of 4%.

Sub domain DSS05.03 Manage endpoint security with the answer criteria obtained Strongly Agree frequency 8 and percentage of 17% , Agree with frequency of 19 and percentage of 42%, Doubtful with frequency of 9 and percentage of 20%, Disagree with frequency of 8 and a percentage of 17%, strongly disagree with a frequency of 1 and a percentage of 2%.

Sub domain DSS05.04 Manage user identity and logical access with the criteria for answers that can Strongly agree frequency 12 and percentage as much as 27% , Agree with frequency 15 and percentage 33% , Doubtful with frequency 6 and percentage 13% , Disagree with frequency 11 and percentage 24%, Strongly disagree with frequency 1 and percentage 2%.

Sub domain DSS05.05 Managing physical access to IT assets with the criteria for answers that can Strongly agree frequency 9 and percentage of 20%, Agree with frequency 15 and percentage of 33%, Undecided with frequency of 8 and percentage of 18%, Disagree with frequency 12 and percentage 26%, Strongly disagree with frequency 1 and percentage 2%.

Sub domain DSS05.06 Manage sensitive documents and output devices with the answer criteria that can Strongly agree frequency 8 and percentage as much as 18%, Agree with frequency 14 and percentage 31%, Undecided with frequency 5 and percentage 11%, Disagree with frequency 10 and percentage 22%, Strongly disagree with frequency 6 and percentage 13%.

Sub domain DSS05.07 Manage vulnerabilities and monitor infrastructure for security-related events with the response criteria obtained Strongly Agree frequency 7 and percentage of 15%, Agree with frequency of 16 and percentage of 36%, Undecided with frequency of 13 and percentage of 29 %, Disagree with a frequency of 8 and a percentage of 18%, Strongly disagree with a frequency of 1 and a percentage of 2%.

Table 4. Maturity Level Calculation

DSS05 subdomain	total value of the questionnaire	the total value of the answer
DSS05.01	225	826
DSS05.02	225	810
DSS05.03	225	820
DSS05.04	225	799
DSS05.05	225	762
DSS05.06	225	725
DSS05.07	225	782

Then the maturity index will be calculated, namely the number of answers divided by the total value of the questionnaire. And get the following results :

Table 5. Current Maturity Index

	current maturity index
DSS05.01	3,67
DSS05.02	3,6
DSS05.03	3,64
DSS05.04	3,55
DSS05.05	3,38
DSS05.06	3,22
DSS05.07	3,47

From the data table above, we will compare the current maturity level with the maturity target of 5, then we will get a maturity gap as shown in the Figure 2

The GAP maturity level above can then be analyzed so that the Maturity Level for each sub-domain is determined as shown in the table 6.

Table 6. Maturity Level sub domain DSS05

Level	Sub Domain DSS05	Maturity Level
4	DSS05.01	Manage and Measurable
3	DSS05.02	Defined Process
4	DSS05.03	Manage and Measurable
4	DSS05.04	Manage and Measurable
3	DSS05.05	Defined Process
3	DSS05.06	Defined Process
3	DSS05.07	Defined Process

Furthermore, the security level can be determined by the maturity level of all activities carried out in DSS05 as follows:

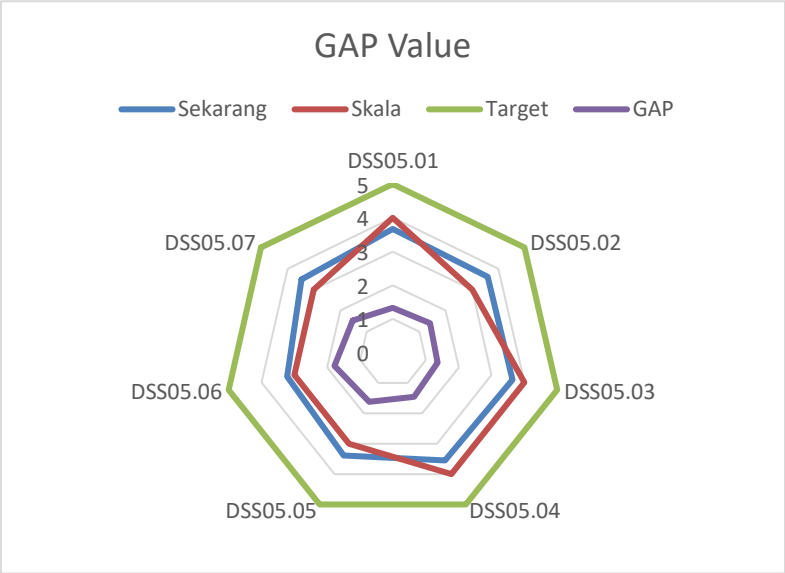

Figure 2: The GAP value is obtained from the target value minus the current maturity level.

$$Maturity\ level\ DSS05 = \frac{maturity\ level}{many\ processes}$$

$$= \frac{(01)+(02)+(03)+(04)+(05)+(06)+(07)}{Banyak\ Proses}$$

$$= \frac{(3{,}69)+(3{,}6)+(3{,}64)+(3{,}55)+(3{,}38)+(3{,}22)+(3{,}47)}{7}$$

$$= 3{,}50$$

So the achievement value of 3.50 indicates the maturity level in defined. This level means that the institution has implemented a defined process and all teams understand how the process should work. Uses organizational standards and adapts them to address project and job characteristics. Focus on achieving project objectives and organizational performance.

C. Recommendations

Based on the Gap analysis obtained from the results of the target level to be achieved and the level achieved in DSS05, as shown in Figure 4.1 Recommendations that can be given to improve the quality of the maturity level of network service security in the agency:

1. Protecting from malicious software (DSS05.01) is at level 4, namely Managed and measurable in agencies that have carried out procedures properly and are capable of carrying out developments related to malicious software.
2. Processing network security and connectivity (DSS05.02) is at level 3, namely Defined process in agencies that are already capable of carrying out developments related to network security and connectivity. Implement policies against threats that will arise to security connectivity.
3. Manage endpoint security (DSS05.03) is at level 4, namely Manage and measurable for agencies that are able to carry out procedures very well and are able to carry out developments related to device operating systems in a safe way and evaluate the security of network services.
4. Manage user identity and logical access (DSS05.04) is at level 4, namely Managed and measurable in agencies that are able to carry out procedures very well and are able to carry out developments related to access rights that each user has.
5. Managing physical access to IT assets (DSS05.05) is at level 3, namely Defined process in agencies that are capable of carrying out developments related to physical security access.
6. Manage sensitive documents and output devices (DSS05.06) are at level 3, namely Defined processes in agencies that are

capable of developing physical safeguards in accordance with protection targets.

7. Manage vulnerabilities and monitor infrastructure for security-related events (DSS05.07) is at level 3, namely the Defined process at the agency is capable of carrying out security-related developments that have been made when monitoring identifies potential security incidents.

IV. CONCLUSION

The quality of network service security at Muhammadiyah University of Lamongan has met security standards measured regarding the DSS05 analysis in the 2019 Cobit framework with security parameters namely confidentiality, integrity and availability. Information system security at this level is already good, but still requires innovation and development to be ready, fast and precise in handling security threats. Agencies must actively read security technology developments and all forms of threats. The maturity level of network service security using the Cobit 2019 framework with a very good maturity level at Muhammadiyah University of Lamongan has been measured based on the DSS05 sub-domain, DSS05.01 sub-domain with an index result of 3.67 indicating at level 4, DSS05.02 with an index result of 3, 6 indicates at level 3, DSS05.03 with an index result of 3.64 indicates at level 4, DSS05.04 with an index result of 3.55 indicates at level 4, DSS05.05 with an index result of 3.38 indicates at level 3, DSS05. 06 with an index result of 3.22 indicates at level 3, and DSS05.07 with an index result of 3.47 indicates at level 3.

V. ACKNOWLEDGEMENT

This research was completed with the support of supervisors 1 and 2 as well as all parties involved in the research process. Therefore, thanks to Mala Rosa Aprillya and Eko Handoyo as supervisors. And thank you to Muhammadiyah Lamongan University for facilitating this research.

VI. REFERENCES

Nurcahyo A. C., M. Pradana and R. Hammad, "Analysis of Maturity Level of Network Services Based on an Internal Perspective Using Cobit 4.1 at Immanuel Christian University, Yogyakarta," *Management and Sustainable Development Journal*, pp. 15-31, 2020.

CMMI Product Team, "CMMI for Service," vol. Version 1.3, 2010.

Umar, R. I. Riadi and E. Handoyo, "Information System Security Analysis Based on COBIT 5 Framework Using Capability Maturity Model Integration (CMMI)," *J. Sist. Inf. Bisnis*, pp. 9(1),47., 2017.

Umar R., I. Riadi and G. M. Zamroni, "Mobile Forensic Tools Evaluation For Digital Crime Investigation," *International Journal on Advanced Science, Engineering and Information Technology (IJASEIT)*, Vols. 8(3), 949, 2018.

Afifah N., M. A. Firdaus and D. R. Indah, "Maturity Level Evaluation Using Cobit 5.0 DSS02 in the Indihome Service Process PT. Indonesian Telecommunications," *(Doctoral dissertation, Sriwijaya University)*, 2018.

Agoan T. S., H. F. Wowor and S. Karouw, "Analysis of Information Technology Maturity Level in the Communication and Informatics Office of Manado City Using the Cobit 5 Domain Evaluate, Deirect, Monitor (EDM) and Deliver, Service, and Support (DSS)," *Journal of Informatics Engineering*, p. 10(1), 2017.

Aleksi A. and M. Afrina, "Measuring the Maturity Level of IT Services at the Sriwijaya University Library UPT Using the 2019 Cobit Framework," *(Doctoral dissertation, Sriwijaya University).*

Anastasia P. N. and L. H. Atrinawati, "Information Technology Governance Design Using the Cobit 2019 Framework in Hotels," *Information Systems Journal (E Journal),* p. 12(2), 2020.

Cobit F. M. and Z. S. Santi, "Analysis of Computer Network Security Systems at PT. Malindo".

Gusni R. A., K. Kraugusteeliana and I. W. Pradnyana, "Analysis of the Information System Security Management of the Jakarta Police Sespima Bhayangkara Hospital Using Cobit 2019," *In Proceedings of the National Student Seminar on Computer Science and Its Applications,* vol. 2, no. 2, pp. 420-429, 2021.

ISACA, "Business Framework for the Governance and Management of Enterprise IT," 2011.

Kristanto T. and L. A. Lestari, "Analysis of E-Government Maturity Levels Using the Cobit 5 Framework (case study: Surabaya City Trade and Industry Office)," *Sesindo,* 2016.

Putra S. D., H. Heman and A. Yudhana, "Evaluation of Network Service Governance Using Cobit 2019 at Colleges of Health Sciences," *Resistor,* vol. 5, no. (2), pp. 119-126, 2022.

Syaputra S. D., "Journal of Information Technology Governance Using the Cobit 5 Framework PT Santani Agro Persada".

Yusuf Y., E. T. Gunawan and R. Sarita, "Analysis of Service Maturity Level at PT Telkom Sampit Using Cobit 5 DSS02 and DSS03 Domains," *Journal of Information System Research (JOSH),* vol. 2, no. (4), pp. 283-287, 2021.

M. R. S. E. &. D. A. Aprillya, "System Dynamics Simulation Model to Increase Paddy Production for Food Security.," *Journal of Information Systems Engineering and Business Intelligence,* vol. 5 (1), p. 67, 2019.

Aprillya M. R., E. Suryani and A. Dzulkarnain, "System Dynamics Simulation Model to Increase Paddy Production for Food Security.," *Journal of Information Systems Engineering and Business Intelligence,* vol. 5 (1), p. 67, 2019.

Fitriani D., "Analysis of the Effect of Using Information Technology on Employee Performance at PT. Jiwasraya Insurance Pontianak," vol. 4(1), pp. 160-170, 2018.

Jordy W., L. W. Santoso and Y. Yulia, "Implementation of IT Risk Management at Bank X Using the 2019 Cobit Framework," *Journal Infra,* vol. 10(1), pp. 64-70, 2022.

Munawar Z. and N. I. Putri, "Computer Network Security in the Big Data Era," *Journal of Information Systems Works Children of the Nation,* vol. 2(1), pp. 14-20, 2020.

Prasetyo A. and N. Mariana, "Analysis of Information Technology Governance (IT Governance) in the Academic Field with the Cobit Framework Case Study at Stikubank University Semarang," *DYNAMIC Information Technology Journal,* vol. 16(2), pp. 139-149, 2011.

Prasetyo T. A. and M. N. Sitokdana, "Ministry of Data and Information Center Governance Analysis xyz Using Cobit 2019," *Journal of Applied Computer Science and Teknology,* vol. 2(2), pp. 95-107, 2021.

Rahim F. R., D. S. Suherman and M. Murtiani, "Analysis of Teacher Competence in Preparing Information Technology-Based Learning Media for the Industrial Revolution Era 4.0," *Journal of Eskata Education,* vol. 1, no. 5, 2019.

Rahmawati D., "Analysis of Factors Influencing the Utilization of Information

Technology," *Journal of Economics and Education,* 2008.

Rosmiati , I. Riadi and Y. Prayudi, "Maturity Level Framework For Measurement of Information Security Performance," *International Journal of Computer Applications,* vol. 141, no. 8, pp. 975-8887, 2016.

Saleh M., I. Yusuf and H. Sujaini, "implementation of the 2019 Cobit Framework on Information Technology Audits at the Sambas Polytechnic," *Journal of Informatics Education and Research,* vol. 7(2), pp. 204-209, 2021.

Setiawan R. A. and W. Wasilah, "Evaluation of Information Technology Governance and Management Using the 2019 Cobit Framework at the Communication and Informatics Office of South Lampung Regency," *Prosiding Seminars National Darmajaya,* vol. 1, pp. 8-15, 2022.

Wulung G. L., Y. Rindengan and S. R. Sentinuwo, "2021," *Implementation of Cobit 5 Dwliver, Service, and Support to Measure the Maturity of the Manado City Communication and Information Service,* 2021.

Yunus I. R., N. Agitha and S. A. Anjarwani, "Analysis of Information Technology Governance in NTB Provincial Hospital Network Infrastructure Services Using Cobit 4.1," *Journal of Information Technology, Computers, and Their Applications,* vol. 1, no. 1, pp. 19-30, 2019.

Santi Z., "Computer Network Security System Analysis at PT. Malindo.".

Umar R., I. Riadi and E. Handoyo, "Analysis of Information Technology Governance Using the Cobit 5 Framework on Domain Delivery, Service, and Support (DSS)," *In National Seminar on Information and Communication Technology - SEMANTIKOM,* pp. 41-48, 2017.