Jurnal Informatika dan Rekayasa Perangkat Lunak ISSN 2656-2855
Vol. 5, No. 1, Maret 2023, Hal. 80-88 e-ISSN 2685-5518

The IT Governance Measurement using Cobit 5 Framework in Quality Assurance Department

Ali Nurdin[1*], **Muharman Lubis**[2]
[1,2] Information Science , School of Industrial Engineering, Telkom University
[*]Email: alinurdinn@student.telkomuniversity.ac.id

Abstract

This research is conducted to measure and evaluate of IT governance at quality assurance department of XYZ university. The measurement used the COBIT 5 framework by Process Assesment Model. The objective of this research is performing the measurement and evaluation of the IT Governance in the Quality Assurance Department of XYZ University with DSS domains in COBIT 5 Framework. The approach utilized the primer data from interview and questionaire, and secondary data from observation and document stages. The result of this research show the most of the capability level process of IT Governance are at Level 1 (performed) they are 4 processes form DSS domain (DSS01, DSS04, DSS05, DSS06) and at Level 2 (DSS02, DSS03). The conclusion of this research show most of the process perform capability level 1 today.

***Kata kunci**: COBIT 5, IT Governance, quality assurance*

INTRODUCTION

Utilization of information technology today has become to be an important factor to achieving success in various business. The majority of organizations and company already put the information technology as a support system to improve performance and efficiency (Cearley et al., 2019).

Evaluation is a main factor to sustainable development that has been applied information technology can contribute the maximum within an organization. To evaluate the necessary framework to guide the technology control standards, and some of them are ISO, ITIL, COBIT, and others. In this study the authors use COBIT 5. COBIT 5 is used as a guide in the study because it is a model of framework information technology governance which includes a representative and comprehensive financial issues, planning, implementation, operation and control of each IT process (Nugroho, 2014).

The studies regarding IT governance evaluation thru COBIT 5 framework have been conducted by various researchers. Putri conducted an audit for maturity evaluation of IT governance by using COBIT 5 framework, particularly for domain Deliver, Service, and Support (DSS) in process of Manage Problem (DSS03). The result of study said that with DSS03 capability level 64.66%, the company (PT. DEF) was suggested to improve the process (Putri et al., 2017). Pereira did a study regarding Delphi to extract the advantageous knowledge from expert in appraisal of corporate governance of IT (CGIT) via COBIT 5 approach. According to expert's point of view on initial argument of COBIT 5 execution, the study delivered a set of process that is able to be operated in the first stage of CGIT realization. Here, the dominance of tactical and strategic processes should be considered well as a vital perception(Pereira et al., 2018).

COBIT 5 helps organizations to create an optimal IT value by maintaining a balance between realizing benefits and optimizing the level of risk and the sources used. COBIT 5 Framework has 5 domains and 37 processes that are used to conduct the audit. Selection of COBIT 5 is very appropriate to conduct IT audits for being able to cover all the elements of IT governance with not only focused on technical issues and on technology but also to identify other resources and drives the IT governance toward organizational goals (ISACA, 2012). The domain used in the audit process is Deliver, Service, and Support (DSS) which is one of the five domains of COBIT 5 which includes Management of IT Enterprise. DSS domain focuses on the delivery of data, services, and support provided for effective and efficient information systems, to determine the respondents, we used RACI chart to test the maturity of each process from using the domain-level capability. The purpose of this study is to make sure that use of IT services in

its evaluation is already contributing as needed. then the benefit of application is to support the achievement of the vision and goals of the Department. Hopefully this research, provide inputs that are beneficial for the development of service in Quality Assurance Divison of XYZ University.

LITERATURE REVIEW

The COBIT 5 framework is widely used as a tool for evaluating the performance of IT governance, previously Amalia conducted research in the form of an audit of the Call Center information system at PT Gemilang Surya Kahyangan and found an average maturity level of 2.05 (Amalia et al., 2022).

Then Elly conducted research at STMIK Mikroskil using the COBIT 5 framework with the domains EDM01, EDM02, EDM05, APO01, APO02, APO04, APO07, BAI01, DSS05, and MEA01. and found the average Maturity Level 3 (Elly and Halim, 2018).

Differently to previous research, this study uses the Deliver, Service and Support (DSS) domain of COBIT 5 Framework in making IT in service support management for users, and data management and operational facilities. This study refers to the RACI chart in determining the respondent's audit to be carried out. The results of this evaluation will be measured using process capability. The method used in this study is observation and interviews. The results of the evaluation will become findings which will then provide recommendations and suggestions, so that the XYZ University Internal Quality Assurance Department can propose achieving the vision and mission.

Differently to previous research, this study uses the Deliver, Service and Support (DSS) domain of COBIT 5 Framework in making IT in service support management for users, and data management and operational facilities. This study refers to the RACI chart in determining the respondent's audit to be carried out. The results of this evaluation will be measured using process capability. The method used in this study is observation and interviews. The results of the evaluation will become findings which will then provide recommendations and suggestions, so that the XYZ University Internal Quality Assurance Department can propose achieving the vision and mission.

2.1 Information Technology Audit

Information Technology Audit is an evaluation of an organization, system, process or product. Examination is carried out by a competent, objective and impartial court, which is called an auditor. The objective is to verify that the subject matter of the audit has been completed or carried out in accordance with agreed and accepted standards, regulations and practices. Information system audit is the process of collecting and evaluating evidence to determine whether a computer system can secure assets, maintain data integrity, and can support the achievement of organizational goals in an effective and efficient use of resources. Information technology audit in general is a process of collecting and evaluating all activities in the company's information system. Another term for computer audit Information technology audit is widely used to determine whether the company's information system assets have worked effectively, and integrated to achieve organizational targets (Murad et al., n.d.).

2.2 COBIT 5 Framework

The COBIT 5 framework is a development of COBIT 4.1 which is one of the frameworks used to carry out the audit process. COBIT is a comprehensive rating standard with comprehensive coverage as an auditing framework. Therefore, COBIT ratings can be used in many types of organizations. COBIT 5 is a business framework for corporate IT governance and management, as well as a collection of tools that support managers to bridge the gap between the need to control (control requirements), technical issues and business risk (ISACA, 2012).

COBIT was developed by the IT Governance Institute (ITGI), which is part of the Information Systems Audit and Control Association (ISACA). According to ISACA, COBIT 5 is a framework for governance and management of information technology and all that is related, which starts from the stakeholders needs for information and technology. The Deliver, Service, and Support (DSS) domain is one of the five COBIT 5

domains, which cover the Management of Enterprise IT (ISACA, 2011).

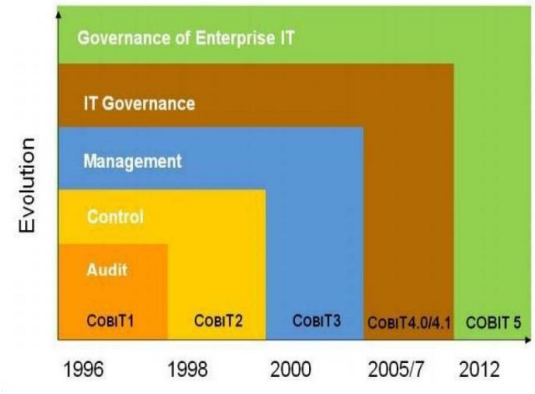

Fig 1.The evolution of COBIT (www.isaca.org)

COBIT 5 provides a comprehensive framework to help companies achieve their goals in enterprise IT governance and management (Steven De Haes et al., 2013). The COBIT 5 framework enables IT to organize and manage holistically for the entire enterprise, which takes full end-to-end business process business and responsible IT functional areas, where IT interests deal with internal stakeholders and external form principles (Rahat Afreen, 2018). COBIT 5 framework principles are illustrated in Fig. 2.

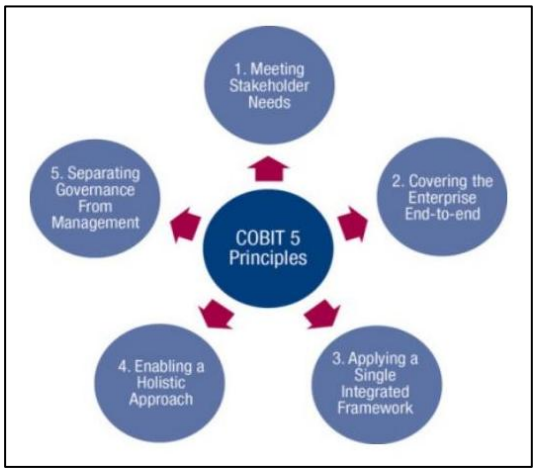

Fig 2. Cobit 5 framework principal (www.isaca.org)

The following is an explanation of the 5 COBIT 5 principles above (ISACA, 2012):

1. Meeting Stakeholder Needs: COBIT 5 provides all the processes needed to help companies meet the needs of stakeholders in the company through the use of IT.
2. Covering the Enterprise End-to-end: COBIT 5 integrates IT governance into enterprise governance.
3. Applying a Single Framework: COBIT 5 is known as a complete and standard IT governance framework that covers many existing governance frameworks.
4. Enabling a Holistic Approach: COBIT 5 has several enablers to help implement easy-to-understand governance and enterprise IT management systems.
5. Separate Governance from Management: COBIT 5 clearly distinguishes between governance and management. These 2 things lead to different activities, require different organizational structures and have different functions.

The following is a general explanation of the 5 COBIT domains (ISACA, 2011):

1. Evaluate, Direct and Monitor (EDM), is a domain that talks about assessment and evaluation, direction and supervision, the EDM domain has 5 sub domains. This EDM domain comes from the governance area of enterprise IT.
2. Align, Plan and Organize (APO), is a domain that talks about alignment, planning and processing of IT, the APO domain has 13 sub domains. The APO domain originates from the management of enterprise IT.
3. Build, Acquire and Implement (BAI), is the domain of IT development and implementation, the BAI domain has 10 sub domains. The BAI domain originates from the management of enterprise IT area.
4. Deliver, Service and Support (DSS), is a domain that talks about the delivery of IT services and support for companies or organizations, this domain has 6 sub domains. The DSS domain originates from the management area of enterprise IT.
5. Monitor, Evaluate and Assess (MEA), is the domain of monitoring, evaluating and testing IT processes in a company or organization, this domain has 3 sub domains. The MEA domain originates from the management area of enterprise IT.

To find out which processes will be analyzed according to the company's circumstances, in COBIT 5 we need to first map the enterprise goals and IT-related goals that exist within the company. Mapping can be done after we know the company's business

goals and map them first in COBIT 5 business goals.

The Deliver, Service and Support (DSS) domain is one of the domains in COBIT 5. The focus of the DSS domain is on aspects of information technology service delivery, processes and support that make it possible to achieve effective and efficient IT operations (ISACA, 2011).The DSS domain consists of 6 control objectives, which are as follows:

1. DSS01 Manage Operation.
2. DSS02 Manage Service Requests and Incidents.
3. DSS03 Manage Problems.
4. DSS04 Manage Continuity.
5. DSS05 Manage Security Services.
6. DSS06 Manage Business Process Controls.

The RACI diagram is part of the Responsibility Assignment Matrix (RAM), which is a form of mapping between resources and activities in each procedure. RACI stands for Responsibility, Accountable, Consulted and Informed. In COBIT 5, the RACI diagram is used to determine the appropriate respondents in the organization to be interviewed (ISACA, 2011).

The RACI diagram itself has an explanation for each part. The following is an explanation of each section:

1. R (Responsible), means that the part is the executor who must be responsible for carrying out and completing the activities for which they are responsible.
2. A (Accountable), means that the part is a party that must direct the course of the implementation of activities.
3. C (Consulted), means that the part is the party that will be the place of consultation during the implementation of the activity.
4. I (Informed), means that the part is the party that is given information regarding the implementation of activities.

2.3 Capability Level Process

In COBIT 4.1 the maturity assessment process uses the Maturity Model, while in COBIT 5 using Capability Models. The number of assessment levels in the Maturity Model and Capability Model is the same, namely six levels, but the difference is the structure of the framework that has been changed (ISACA, 2012). The following describes the level of Process Capability :

a. Level 0 Incomplete Process
   The process is not implemented or fails to achieve its process objectives. At this level, there is little or no evidence of any achievement of process goals.
b. Level 1 Performed Process
   Processes are implemented to achieve its business objectives.
c. Level 2 Managed Process
   P the implemented process is managed (planned, monitored, and adjusted) and the results are defined and controlled.
d. Level 3 Established Process
   Processes are documented and communicated (for organizational efficiency).
e. Level 4 Predictable Process
   The process is monitored, measured, and predicted to achieve results.
f. Level 5 Optimizing Process
   Predicted processes are then improved to meet relevant business objectives and future objectives.

The scope of the research carried out, namely the scope of the problem in the implementation of IT governance audits at the Internal Quality Assurance Depatment, has so far been carried out only when necessary. Therefore, a thorough audit and analysis of IT governance is needed where in this audit only focuses on the DSS domains in the COBIT 5 framework as a reference. The limitation of this research focuses on the existing IT in the Internal Quality Assurance Depatment. This research will focus on the audit process and analysis of IT governance in the Internal Quality Assurance Depatment as a whole, starting from the rules and procedures, the tools used, and the existing systems. So far, the use of existing IT is still not maximized, is still experiencing problems and has never been evaluated on existing IT governance in the Depatment. Another thing that is different from previous studies is that the authors also made in-depth observations of observing and using IT in the Internal Quality Assurance Depatment directly. The results of this research are in the form of findings that will become recommendations and suggestions so that IT governance in the Internal Quality Assurance Depatment can be maximized to support achieving business goals effectively.

RESEARCH METHODS

This research using quantitative descriptive method. Interviews were conducted to the head of administration as a source of information technology governance as a source of information in the Internal Quality Assurance Department.

3.1 Research Stage

In a research assignment at the Internal Quality Assurance Depatment, the method used is descriptive quantitative. This research conducted by case studies includes research objects, which means that research is carried out directly on research objects by collecting data, processing data and then concluding (Sholihat, 2018).The stages of the data collection method in this study are as follows: Literature study, collecting data through books, literature, various journal sources and other sources related to this research.

1) Observation, direct observation made by the author of the research object in order to obtain the necessary information and data.
2) Interviews, two-way communication or conversations conducted by researchers and respondents to collect information relevant to research objectives.
3) Data Processing, processing data from observations and interviews in accordance with the DSS (Delivery, Service, and Support) domain guidelines of COBIT 5 framework.

3.2 Respondent Mapping

Respondents are parties who are trusted to be asked to give opinions on something in question, in this study the authors conducted interviews with the second respondent, the reason the authors chose two respondents was because they were able to answer questions referring to RACI (Responsible, Accountable, Consulted, Informed) at the Quality Assurance Depatment Internals.

3.3 DSS Domain Selection Process

In using the DSS domain, it is necessary to select a process so that the measurements are in accordance with the needs of the organization with reference to the business objectives of the engineering and maintenance division. The first step is mapping between Enterprise Goals that are in accordance with the business goals of the engineering and maintenance division.[9] The result of this first mapping is obtaining 16 related goals, namely EG01, EG3, EG4, EG5, EG6, EG7, EG8, EG9, EG10, EG11, EG12, EG13, EG14, EG15, EG16, and EG17.

The results of the first mapping are then mapped with IT-related Goals. Then the process capability model (PCM) is used which is divided into two categories, namely primary (P) and secondary (S). The P symbol indicates that the item has a high priority, while S indicates that the item has a low priority. The mapping is described in Table 1 where all IT-related goals have relationships and are used in the next process.

Table 1. Mapping of Enterprise Goals with IT-related Goals.

	EG1	EG2	EG3	EG4	EG5	EG6	EG7	EG8	EG9	EG10	EG11	EG12	EG13	EG14	EG15	EG16
ITrG1	P	S			P	S	P	P	S	P	S	P			S	S
ITrG2		S	P													
ITrG3	P	S					S	S		S		P			S	S
ITrG4		P	S			P	S		P			S		S	S	
ITrG5	P				S		S	S	S	S	P		S			S
ITrG6	S	S		P					P		P					
ITrG7	P	S	S		P	S	P	P		P	S	S			S	S
ITrG8	S	S			S	S		P	S	P	S		P		S	S
ITrG9	S	S			S		P	P		P		S	S		S	P
ITrG10		P	P			P					P			P		
ITrG11	P						S	S	P	S	S	S	S			S
ITrG12	S	S			S		S	P	S	P	S	S	S			S
ITrG13	P	S			S				S			P				

The third selection process is the mapping of IT-related goals to the processes in the DSS so that the use of processes in COBIT 5 matches the needs of the organization. The mapping results are shown in Table 2.

Table 2. Match of Enterprise Goals with IT-related Goals.

	ITrG1	ITrG2	ITrG3	ITrG4	ITrG5	ITrG6	ITrG7	ITrG8	ITrG9	ITrG10	ITrG11	ITrG12	ITrG13	ITrG14	ITrG15	ITrG16	ITrG17
DSS01		S		P	S		P	S	S	S	P			S	S	S	S
DSS02				P			P	S		S				S	S		S
DSS03		S		P	S		P	S	S		P	S		P	S		S
DSS04	S	S		P	S		P	S	S	S	S	S		P	S	S	S
DSS05	S	P		P			S	S			S	S		S	S		
DSS06		S		P			P	S		S	S	S		S	S	S	S

From Table 2, the results of the mapping of the COBIT 5 process with IT-Related goals are obtained. Then use process capability model (PCM) which is divided into two categories, namely primary (P) and secondary (S). P indicates that the item has a high priority, while S indicates that the item has low priority. Therefore, all processes in the DSS domain are used as the scope of the information technology audit process in the internal quality assurance division.

RESULTS AND DISCUSSION

4.1 Capability Level Calculation

This process starts with collecting information from questionnaires and interviews that have been conducted during the audit process. From this information collection, the average existing capability level (As is) and target level (To be) are obtained.

Table 3. Capability Level

Domain Process	Capability Level	
	As is	To be
DSS01 Manage Operations	1	4
DSS02 Manage Service request and Incidents	2	4
DSS03 Manage Problems	2	4
DSS04 Manage Continuity	2	4
DSS05 Manage Security Services	1	4
DSS06 Manage Business Process Controls	2	4

Based on the acquisition of the capability level of each level in the COBIT 5 DSS domain, the average capability level is obtained at level 3 of the Established Process. This means that the activities have been carried out, the activities are written in Standard Operating Procedures/policies/rules or have implementation standards, and there is an appropriate allocation of responsibilities and resources.

The following is the capability level and target level obtained based on the audit process that has been carried out.

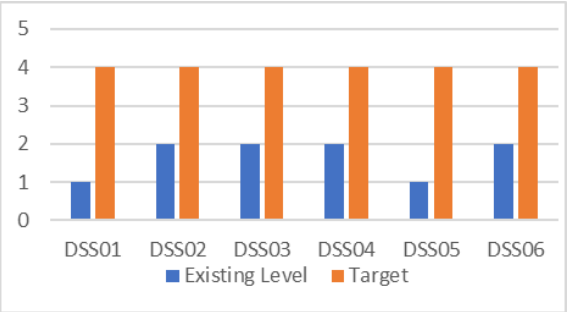

Fig 3. Existing level and target level

From Figure 3 it can be seen that the existing level in the internal quality assurance division is at level 3 Establish Process, so the target level specified is level 4 Predictable Process.

Based on the analysis results of calculating the maturity level of information technology governance in the Internal Quality Assurance Depatment, it can be seen that each sub domain has been implemented to achieve the business objectives of the Internal Quality Assurance Depatment.

The following is a more detailed discussion of the conditions regarding the existing DSS sub domains.

1. DSS01 (Manage Operations)

In this process, Information Technology (IT) operations in the Internal Quality Assurance Depatment have been running well, all activities in the use of IT have been running according to the coordination of the IT department with other parts. However, the results of the process capability level from the administrative section of the Internal Quality Assurance Depatment are only at level 1, namely the Performed Process. This is because the IT operations of the Internal Quality Assurance Depatment still do not have a Standard Operating Procedure (SOP) determined by the IT department, IT operations are only implemented without clear rules.

2. DSS02 (Manage Service Requests and Incidents)

In requesting existing IT services, the IT section of the Internal Quality Assurance Depatment already has clear SOPs for service requests, there is a documentation and communication process by IT where requests for services submitted must pass approval from management and superiors. Therefore the results of the capability level process from sub managing service assistance and incidents at the Internal Quality Assurance Depatment are at level 3, namely the Established Process, because they have been well documented and coordinated.

3. DSS03 (Manage Problems)

In this process, the IT department of the Internal Quality Assurance Depatment has managed the existing IT problems well, they have identified and addressed the problems directly, but no documentation has been carried out. The results of the capability level process from sub managing problems in the Internal Quality Assurance Depatment itself are at level 2, namely Managed Process.

4. DSS04 (Managed Continuity)

In this process what is done is to build and maintain a plan that allows business and IT to respond to problems and disruptions so that critical business processes continue to run and maintain the availability of information for the organization. The result of the process capability level of the sub managing sustainability at the Internal Quality Assurance Depatment is level 1, namely the Performed Process. The IT side of the Internal Quality Assurance Depatment still does not have clear SOPs to regulate IT operations, this results in unclear when IT will carry out maintenance of existing devices and when to back up data to maintain the continuity of the Internal Quality Assurance Depatment's business processes if at any time having trouble.

5. DSS05 (Manage Security Services)

The process carried out in this sub domain is protecting organizational information to maintain the level of information security in accordance with security policies. The result of the process capability level of the sub managing system security at the Internal Quality Assurance Depatment is level 1, namely the Performed Process. Computers in the Internal Quality Assurance Depatment already use antivirus and firewalls for security.

6. DSS06 (Manage Business Process Controls)

In this process what should be done by the organization is to define and maintain appropriate business process controls to ensure the activities carried out are in accordance with the expected goals.

The result of the process capability level of the sub managing business process control at the Internal Quality Assurance Depatment is level 1 where the Internal Quality Assurance Depatment has sought business control, for example through employee absences. Gap analysis is carried out to find out how far the current conditions are with the expected conditions. The current conditions are known from the results of the assessment analysis using COBIT 5, while the conditions expected to be obtained are based on targets set by the Internal Quality Assurance Depatment by taking into account existing resources. The following gaps are visible as shown in Fig. 4.

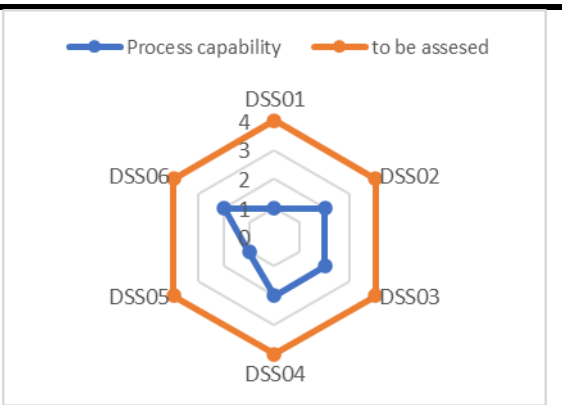

Fig 4. Gap Analysis

Recommendations for all Internal Quality Assurance Department sub domain processes are as follows:

1. IT parties of the Internal Quality Assurance Department need to make clear SOPs for computer and internet use, to minimize risks from computer and internet use. (DSS01)
2. IT parties need to carry out periodic monitoring so that they know how the operational conditions of IT or the existing systems in the Internal Quality Assurance Department are. (DSS01)
3. The Internal Quality Assurance Department needs to conduct periodic IT training for its employees, because so far the IT Internal Quality Assurance Department cannot focus on developing its operational system because they often only help other employees who cannot use IT properly. (DSS01)
4. The Internal Quality Assurance Department needs to add human resources for IT because so far IT has not been able to develop systems for the operations of the Internal Quality Assurance Department effectively due to a shortage of human resources. (DSS01)
5. IT parties need to do documentation when solving existing problems, this can be used as a reference for what problems are often encountered with existing computers or systems so that it is easier to repair if the same problem occurs in the future without the need to identify the problem again. In addition, it can also be used as a reference to find out which devices often experience problems, so that IT can replace devices instead of fixing them continuously. (DSS03)

6. IT needs to make system maintenance SOPs that help maintain the continuity of the Internal Quality Assurance Department's business processes because indirectly with these SOPs, IT will know when to do maintenance and back-up data from the system used in the Quality Assurance Department. (DSS04)
7. IT parties need to ensure that the antivirus is continuously updated regularly, apart from that IT also needs to make SOPs for using computers so that they can filter which devices are allowed to be used in operational activities so that the security of organizational information is maintained. (DSS05)
8. IT needs to make SOPs for maintenance of existing devices at the Internal Quality Assurance Department so that existing devices do not often experience damage, besides that with the SOP for device maintenance, IT will have a regular schedule for carrying out maintenance to minimize device damage. (DSS05)
9. IT parties need to make clear SOPs for computer and internet use and carry out control activities such as filtering several sites that can interfere with employee performance so that business processes are really well controlled. (DSS06)

CONCLUSION

Based on the results of research conducted using COBIT 5, it can be concluded that information technology governance in the Internal Quality Assurance Department in the DSS (Deliver, Service, Support) domain shows that the Internal Quality Assurance Department has implemented all DSS sub-domains. However, until now there has not been a complete documentation and proper management process. This can be seen from the results of the process capability level assessment of the existing sub domains showing that 4 of the 6 sub domains are still at level 1, Performed Process. With this research, it is hoped that the Internal Quality Assurance Department can improve existing information technology governance so that it can contribute to increasing the effectiveness and efficiency of the use of information technology to achieve the business objectives of the Internal Quality Assurance Department. The use of the COBIT 5 framework in this study can show the current position of information technology governance at what level so that it can correct existing deficiencies and determine targets to what extent information technology governance wants to be developed. The Internal Quality Assurance Department can correct deficiencies in its IT governance through implementing the recommendations found in this study. Problems such as not being up-to-date with system databases can be overcome by making system maintenance SOPs. In addition, problems such as broken computers and slow internet connections can be minimized and overcome by having SOPs for computer use at work and routine computer maintenance at the Internal Quality Assurance Department.

Further research can carry out an evaluation that is developed by evaluating the input process chain related to the DSS process subdomain to be able to find out the development of the capability level in the domain or process chain of other related subdomains and be able to use other domains available in the COBIT 5 framework. In COBIT 5 there is The 5 domains include DSS namely, EDM (Evaluate, Direct, and Monitor), MEA (Monitor, Evaluate and Assess), APO (Align, Plan, and Organize), and BAI (Build, Acquire, and Implement). In addition, you can use other frameworks to evaluate such as COBIT 2019, ITIL, BSC, etc.

REFERENCE

Amalia, D., Rahmawati, S., Riyandi, A., 2022. Audit Sistem Informasi Call Center Menggunakan Framework Cobit 5.0 Pada PT. Gemilang Surya Kahyangan. Dirgamaya : Jurnal Manajemen dan Sistem Informasi 2, 1–9.

Cearley, D., Jones, N., Smith, D., Burke, B., Chandrasekaran, A., Lu, C., Panetta, K., 2019. Gartner Top 10 Strategic Technology Trends for 2020 - Smarter With Gartner. Gartner.

Elly, E., Halim, F., 2018. Evaluasi Tatakelola Infrastruktur TI Dengan Framework Cobit 5 (Studi Kasus: STMIK–STIE Mikroskil). Sebatik 22. https://doi.org/10.46984/sebatik.v22i2.311

ISACA, 2012. COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT, Isaca.

ISACA, 2011. COBIT Process Assessment Model: Using COBIT 5, Information Security.

Murad, D.F., Fernando, E., Irsan, M., Kosala, R.R., Ranti, B., Supangkat, S.H., n.d. Implementation of COBIT 5 Framework for Academic Information System Audit Perspective: Evaluate, Direct, and Monitor.

Nugroho, H., 2014. Conceptual model of IT governance for higher education based on COBIT 5 framework. J Theor Appl Inf Technol 60.

Pereira, C., Ferreira, C., Amaral, L., 2018. An IT value management capability model for Portuguese universities: A Delphi study, in: Procedia Computer Science. https://doi.org/10.1016/j.procs.2018.10.082

Putri, M.A., Aknuranda, I., Mahmudy, W.F., 2017. Maturity Evaluation of Information Technology Governance in PT DEF Using Cobit 5 Framework. Journal of Information Technology and Computer Science 2. https://doi.org/10.25126/jitecs.20172123

Rahat Afreen, K., 2018. An Overview of COBIT Principals for Bring Your Own Policy Implementation. International Journal of Science, Engineering and Management (IJSEM) 3.

Sholihat, N.I., 2018. The Implementation of COBIT 4.1 and COBIT 5-Based IT Governance Audits in the Ministry of Finance of Indonesia. The Indonesian Journal of Accounting Research 21. https://doi.org/10.33312/ijar.341

Steven De Haes, Ph.D., Wim Van Grembergen, Ph.D., Roger Debreceny, Ph.D., 2013. IT Policy Framework based on COBIT 5 [WWW Document]. ISACA. URL https://www.isaca.org/resources/isaca-journal/past-issues/2013/it-policy-framework-based-on-cobit-5 (accessed 2.4.23).