Journal of Renewable Energy, Electrical, and Computer Engineering
Vol. 2, No. 1, March 2022, 38-46
e-ISSN: 2776-0049
Research Original Article DOI: https://doi.org/10.29103/jreece.v2i1.6633

Information Technology Governance Audit Using COBIT 5 of DSS Domain (Deliver, Service, And Support) Framework at Malikussaleh University Lhokseumawe

Safwandi[1], Muthmainnah[2], & Misbahul Jannah[3]

[1] Technical Information Department, Faculty of Engineering, Universitas Malikussaleh, Bukit Indah, 24352, Lhokseumawe, Indonesia
[2] Information Systems Department, Faculty of Engineering, Universitas Malikussaleh, Bukit Indah, 24352, Lhokseumawe, Indonesia
[3] Electrical Engineering Department, Faculty of Engineering, Universitas Malikussaleh, Bukit Indah, 24352, Lhokseumawe, Indonesia
✉Corresponding Author: **muthmainnah@unimal.ac.id** | Phone: **+6285225766980**

Received: February 20, 2022 **Revision: March 18, 2022** **Accepted: March 27, 2022**

Abstract
Information technology is very important for companies or institutions to support the achievement of the company's strategic plans to achieve their goals, vision, and mission. Nowadays, an institution can improve the performance of information technology that goes hand in hand with the development of information technology to produce better technology by auditing information technology governance in the company. The purpose of this study is to analyze IT governance using the COBIT 5 framework in the DSS domain at Malikussaleh University Lhokseumawe. COBIT 5 provides a comprehensive framework that helps companies achieve their goals in corporate governance and IT governance. The framework helps companies create optimum value from IT by maintaining a balance between realizing benefits and optimizing risk and resource usage levels. By conducting an audit of information technology governance in the company, the company can find out whether the information technology that has been operating is in accordance with the business processes and company objectives and convey accurately based on the IT strategy. The results of the information technology governance audit based on COBIT 5 in the DSS Domain, on average are at 2.2 (Manage process) to 2.6 (*Established Process*).
Keywords: COBIT5; IT Governance; Capability Level;

Introduction
Information technology plays a very important role for companies or institutions to support the achievement of the company's strategic plan to achieve the goals of the company or institution's vision, mission and objectives [1] Nowadays, most of the management agrees on necessity of "organizational strategic player". As organization's strategy changes over time, it has to change too[2] Now the company can improve the performance of information technology that has been running with the development of information technology to produce better technology by conducting information technology governance audit on the company. By conducting information technology governance audit at the company, the company can find out whether the information technology that has been operating is in accordance with the business processes and objectives of the company and delivered accurately based on IT strategic [3]

Governance is helpful to guide and control an organization in achieving the previously planned goals. The presence of information technology governance would likely support an organization to perform its IT in order to be more focused and able to coordinate between the process and existing benefits [4] IT governance is a corporate governance framework that concentrates on the strategic IT resources particularly on its management and assessment. Moreover, the main objectives of IT governance are aimed to ensure that investments in IT resources add value to the corporation by risk reduction.[5] In carrying out the analysis, a standard is needed that can help make valid and reliable measurements occur. In this study, the standard used is COBIT 5. The COBIT (Control Objectives for Information and related Technology) standard was chosen because the COBIT framework provides the most detailed description of strategy and control in IT process settings that support the alignment of business strategies and IT objectives [6].

The studies regarding IT governance evaluation thru COBIT 5 framework have been conducted by various researchers. [7] The selection of COBIT 5 is appropriate for carrying out the information technology audit process because it covers all elements of information technology governance. It is not centered solely on technical issues in technology but also sees other resources that drive information technology governance towards organizational goals.

The domain used in this audit process is Deliver, Service, and Support (DSS) and the maturity test of each process from the domain using capability level was performed [8]

Literature Review

Information Technology Audit

Information technology studies are the process of gathering and evaluating evidence to determine whether a computer system can secure assets, maintain integrity, encourage the achievement of organizational governance effectively and use resources efficiently [9]. Information technology audit in general is a process of collecting data and evaluating evidence to determine whether a computerized application system has been implemented and has implemented an internal control system that is commensurate, all activities are properly protected or misused and data integrity is guaranteed, reliability and effectiveness and efficiency in organizing computer-based information. The implementation of audits is able to provide information related to the level of asset security, maintaining data integrity, encouraging the achievement of organizational goals effectively, using resources efficiently, and knowing the maturity level of information technology, as well as producing recommendations for achieving optimal maturity levels [10].

IT Governance

IT governance is defined as a structure of relationship and process that can guide an organization in its efforts to achieve the goals by providing added value from the use of information technology by taking into account the risks and results obtained [11] IT governance is the duty of executive management stakeholders to supervise and implement an IT strategy that aims to ensure alignment between IT and business, identify a matrix to ensure the business value of IT and to manage IT risk effectively [12]

COBIT 5

COBIT (Control Objectives for Information and related Technology) is a standard guide to information technology management practices and a set of best practices documentation for IT governance that can help auditors, management, and users to bridge the gap between business risk, control needs, and technical issues [13] COBIT 5 provides a comprehensive framework that helps companies achieve their goals in corporate governance and IT governance. The framework helps companies create optimum value from IT by maintaining a balance between realizing benefits and optimizing risk and resource usage levels. The COBIT Framework 5 makes a clear distinction between governance and management. These two disciplines cover different types of activities, require different organizational structures and serve different purposes.[14]. COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT[17]. Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders[18]. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector [15].

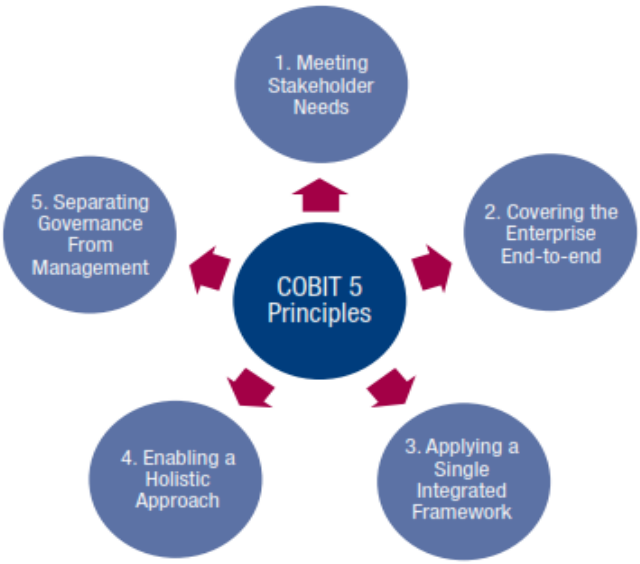

Figure 1. Basic Principles of COBIT

Domain Process of COBIT 5

The processes in COBIT 5 are divided into 2 areas, namely the area of governance and management as presented in Figure 2. The process description for each domain is presented in Table 1. The two areas consist of 5 domains and 37 processes [15]. The differences in the scope of governance and management are as follows:

1. Governance of Enterprise IT

Governance ensures that company goals can be achieved by evaluating the needs, conditions, and preferences of stakeholders through priorities and making decisions on agreed directions and goals. Governance control consists of evaluate, direct, and monitoring (EDM)[19].

2. Management of Enterprise TI

Management functions as a planner. It builds, carries out, and monitors activities that are in line with the direction set by the governance body to achieve company goals. Management controls consist of:

1. *Align, Plan and Organize* (APO)
   APO Process aligns, plans and organizes 2. *Build, Acquire and Implement* (BAI)
   BAI Process builds, obtains, and implements
3. *Deliver, Service and Support* (DSS)
   DSS Process consists of delivery, service, and support.
4. *Monitor, Evaluate and Assess* (MEA)
   MEA process supervises, evaluates, and assesses.

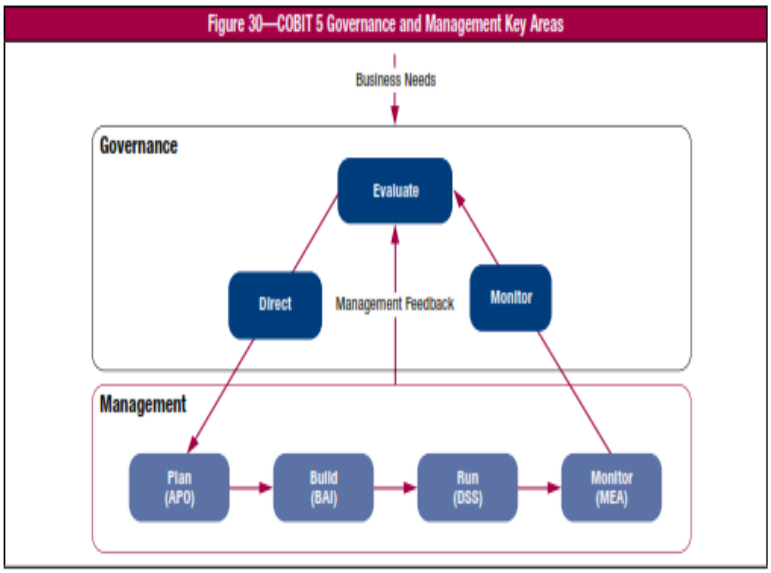

Figure 2. COBIT 5 Governance and Management Key Areas

Cobit 5 Process Reference Model

COBIT 5 is not prescriptive, but from the previous text it is clear that it advocates that enterprises implement governance and management processes such that the key areas are covered[20]. In theory, an enterprise can organise its processes as it sees fit, as long as the basic governance and management objectives are covered. Smaller enterprises may have fewer processes; larger and more complex enterprises may have many processes, all to cover the same objectives.

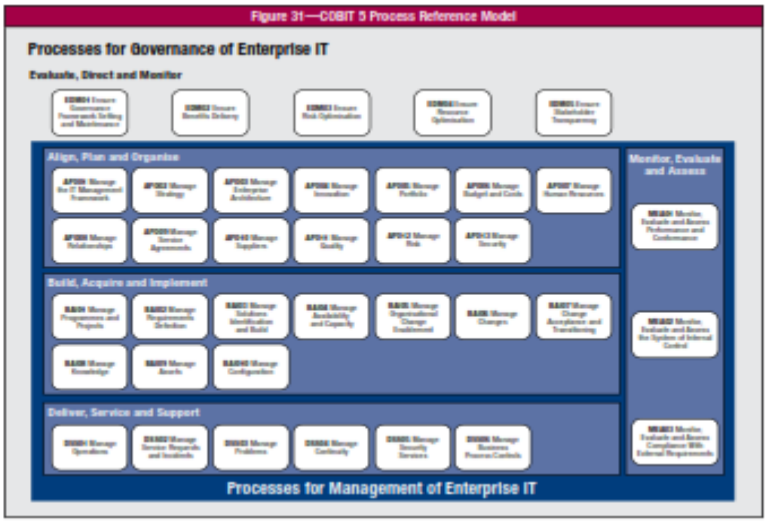

Figure 3. Process Reference Model

Capability Level

Capability model within COBIT 5 is based on ISO/IEC 15504, the standard on Software Engineering and Process Assessment Model. The capability level itself is a model that describes how a core process in an organization is implemented[21]. In addition, it also provides measurement on the performance of processes within the governance or management area. Within COBIT 5, there are six levels of capability as listed below:

1. Level 0 (Incomplete Process). This process is not implemented or fail to achieve the process objectives.
2. Level 1 (Performed Process). The process is implemented and achieves the process objectives.
3. Level 2 (Managed Process). The currently implemented process managed, monitored, and adjusted. The appropriate products are maintained and controlled.
4. Level 3 (Enablished Process). The previously managed process is now implemented using the process that is able to achieve its objectives.
5. Level 4 (Predictable Process). The currently implemented and established process is now operable in defining the limit to achieve the process result.
6. Level 5 (Optimizing Process). The process predicted and described before is continuously improved to fulfill the currently relevant business objectives.[16]

Research Methodology

Literature Study

In this study, a literature study was carried out to find the theoretical basis of previous research either through online journals and materials in the library. The studies through literature studies include reading, summarizing, and concluding. Furthermore, related literature studies used as supporting material to carry out and work on this research.

.

Literature Review

This research used literature study to search for the theories needed for research. This research is a survey approach. The analytical tool used in this research is the COBIT standard procedure issued by the ISACA (Information System Audit and Control Association). The process domain used is DSS (Delivery Service, and Support) in the DSS01 Manage Operations process, DSS02 Manage Service Requests and Incidents, DSS03 Managing Problems, and DSS06 Managing Business Process Control. The literature review conducted by the researcher aims to collect the theoretical materials, methods, and governance models needed. The purpose of literature study is to explore all data and information related to the problems and objects under study.

Review of Strategic Planning Process

The study of the strategic planning process is carried out to collect data about the institution which includes the vision, mission, and institutional structure as the object to be studied. This study is needed as material for researchers' understanding of the strategic planning process, objectives and current conditions of the institution

COBIT Domain Selection

COBIT domain selection was done by studying institutional documents and having discussions with IT division manager. The COBIT domain was selected to ensure that the process being discussed is in line with the objectives of the institution's strategic planning.

Data Collection

The research data consists of two types, namely primary data and secondary data. Primary data is data obtained or collected by researchers directly from data sources. In this study, primary data were obtained through:

1. *Questionnaire*. The data collection was carried out by distributing questionnaires on information technology governance in the institution. The questionnaire used to obtain quantitative data related to the company's IT process capability level: current capability level (as-is) and the expected level of capability (to be). Questionnaires were distributed within people involved in agency governance.
2. *Interviews*. Interviews were conducted to the respondents who previously filled in the questionnaire with the aim that the respondent's understanding of the questions contained in the questionnaire is the same as those intended by the researchers. Besides, interviews were also conducted to collect data and information related to information technology management. Interviews were addressed to parties related to planning and implementing IT governance and were used to test the truth and maturity of data and to obtain more complete data. Researchers analyzed the results of the interviews that had been carried out based on the rating scale on COBIT 5. Figure 3 shows the steps of the study. Secondary data is data obtained or collected by researchers from various existing sources.

Data Processing

After testing the data, then calculation of capability level based on model provided by COBIT was conducted on reliable and valid data. The analysis results produced the current IT process capability level and the capability level expected by

the institution. Furthermore, information technology processes that are at a low level need special attention to meet the expectations of institutional management.

Gap Analysis

At this stage, a comparison was made between the current IT process capability level conditions with the IT process capability level conditions expected by the company. The comparison aims to analyze the extent to which the current information technology process is in accordance with the conditions expected by the institution

Information Technology Governance Planning

At this stage, the authors designed information technology governance. The governance plan designed taking into account the plans for the improvements needed to information technology processes which were made based on the gap analysis obtained in the previous stage. The improvement plan contains recommendations that must be carried out by the institution with the aim of providing direction to management in order to achieve the expected target level of information technology process capability. Furthermore, the creation of a governance model was realized in the form of formulating institutional policy proposals related to information technology.

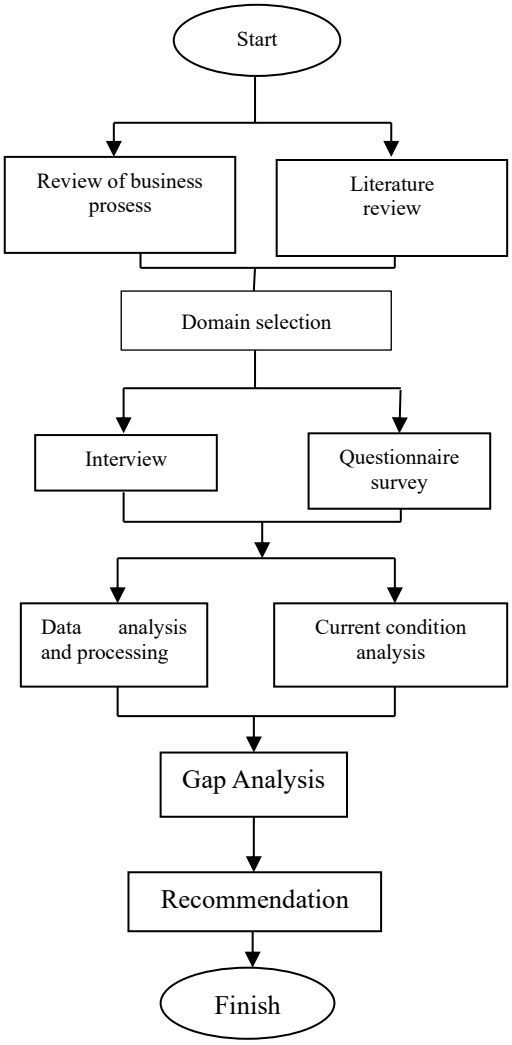

Figure 3.ResearchMethod

Result And Analysis

The result of calculation of each respondent's responses to questionnaire which has been added up with the score for each control process then were calculated the average value of the capability level to get the capability level value of all respondents as shown in Table 1 to table 6.

DSS01 *Manage Operations*

At this stage, the management of IT operational services that have been determined was analyzed with a description of the process of coordinating and carrying out the activities and operational procedures needed to provide internal IT services and results, including the implementation of predetermined standard operating procedures and the necessary

monitoring activities. The expected process capability model from DSS01 was at level 4, a process that can be predicted from the audit results, as can be seen in table 2. It can be concluded that the average of DSS01 Management Operations domain processing capability was at the level 2.4 (Managed Process).

Table 1. Capability Level Domain DSS01

N0.	Sub Domain	Current	Expected
DSS01.01	Perform operational procedures	3	4
DSS01.02	Manage outsourced IT services	2	4
DSS01.03	Monitor IT infrastructure	2	4
DSS01.04	Manage the environment	3	4
DSS01.05	Manage facilities	2	4
	Average	2.4	4

DSS02 Manage Service Requests and Incidents

This stage analyzed work, incident management and IT maintenance, with a description of the process of management of requests and service incidents for IT is carried out based on requests related to problems that arise with IT during work processes, incident management and IT maintenance. The goal is to achieve increased productivity and minimize disruption. The expected process capability model from DSS02 was at level 4, a process that can be predicted from the audit results (see table 3). It can be concluded that the average process capability of the DSS02 domain Manage Service Requests and Incidents was at level 2.2 (Managed Process).

Table 2. Capability Level Domain DSS02

N0.	Sub Domain	Current	Expected
DSS02.01	Define incident and service request Classification schemes.	2	4
DSS02.02	Record, classify and prioritize Requests and incidents.	2	4
DSS02.03	Verify, approve and fulfill service requests.	3	4
DSS02.04	Investigate, diagnose and allocate incidents.	2	4
DSS02.05	Resolve and recover from incidents.	3	4
DSS02.06	Close service requests and incidents.	2	4
DSS02.07	Track status and produce reports.	2	4
	Average	2.2	4

DSS03 *Manage Problems*

At this stage, increased availability, increased service levels, reduced costs, and increased customer comfort and satisfaction by reducing the number of operational problems were analyzed, with process descriptions of identifying and classifying problems and their root causes and providing timely resolution to prevent recurring events. Provide recommendations for improvement. The expected process capability model from DSS03 was level 4, a predictable process from the audit results (see table 4). It can be concluded that the average process capability of the DSS03 Manage Problems domain was at level 2.6 (*Established Process*).

Table 3. Capability Level Domain DSS03

N0.	Sub Domain	Current	Expected
DSS03.01	Identify and classify problems.	3	4
DSS03.02	Investigate and diagnose problems.	2	4
DSS03.03	Raise known errors.	3	4
DSS03.04	Resolve and close problems.	3	4
DSS03.05	Perform proactive problem management.	2	4
	Average	2.6	4

DSS04 *Manage Continuity*

At this stage, critical business operations were analyzed and information availability was maintained at a level acceptable to the company in the event of a significant disruption, with a process description establishing and maintaining a plan to allow business and IT to respond to incidents and disruptions in order to continue critical business processes and require IT services, and maintain the availability of information at a level acceptable to the company. The expected process capability model from DSS04 was at level 4, a predictable process from the audit results, which can be seen in table 5. It can be concluded that the average of process capability of the DSS04 Manage Continuity domain was at level 2.5 (Managed Process)

Table 4. Capability LevelDomainDSS04

N0.	Sub Domain	Current	Expected
DSS04.01	Define the business continuity policy, Objectives and scope.	3	4
DSS04.02	Maintain continuity strategy.	3	4
DSS04.03	Develop and implement business Continuity response.	2	4
DSS04.04	Exercise, test and review the BCP.	2	4
DSS04.05	Review, maintain and improve the continuity plan.	3	4
DSS04.06	Conduct continuity plan training.	2	4
DSS04.07	Manage backup arrangements	2	4
DSS04.08	Conduct post-resumption review.	3	4
	Average	2.5	4

DSS05 *Manage Security Services*

This stage analyzed minimizing the business impact of operational information security vulnerabilities and incidents, with a description of the process of protecting company information to maintain the level of information security risk that can be accepted by access and conducting company security monitoring complies with security policies. Defining and maintaining information security roles and rights of the expected process capability model from DSS05 was at level 4, a process that can be predicted from the audit results (see table 6). It can be concluded that the average process capability of the DSS05 Manage Security Services domain was at level 2.6 (*Established Process*)

Table 5 . Capability Level Domain DSS05

N0.	Sub Domain	Current	Expected
DSS04.01	Protect against malware.	3	4
DSS04.02	Manage network and connectivity security.	3	4
DSS04.03	Manage end point security.	3	4
DSS04.04	Manage user identity and logical access.	2	4
DSS04.05	Manage physical access to ITassets.	2	4
DSS04.06	Manage sensitive documents and output devices.	2	4
DSS04.07	Monitor the infrastructure for security- related events.	3	4
	Average	2.6	4

DSS06 *Manage Business Process Controls*

This stage analyzed the maintenance of information integrity and the security of information assets handled in business processes inside or outside the organization. The process descriptions included define and maintain appropriate business process controls to ensure that information is related to and processed by business processes, meets all relevant information control requirements, identifies relevant information control requirements and manages and operates adequate control to ensure that information processing meets these requirements. The expected process capability model from DSS06 was at level 4, a predictable process from the audit results (see table 7). It can be concluded that the average of process capability of the DSS06 Business Process Controls domain was at level 2.5 (Managed Process).

Table 6. Capability Level Domain DSS06

N0.	Sub Domain	Current	Expected
DSS04.01	Align control activities embedded in Business processes with enterprise objectives.	2	4
DSS04.02	Control the processing of information.	3	4
DSS04.03	Manage roles, responsibilities, access Privileges and levels of authority.	3	4
DSS04.04	Manage errors and exceptions.	2	4
DSS04.05	Ensurectraceability of information Events and accountabilities.	3	4
DSS04.06	Secure information assets.	2	4
	Average	2.5	4

Figure 4, Figure 5 and Table 7 pointing the level of capability processes of the entire process of the domain of Delivery, Service, and Support.

Table 7. Index Level Process Capability of domain Deliver Service and Support

Average Domain	Current	Expected	Optimized
DSS01	2.4	4	5
DSS02	2.2	4	5
DSS03	2.6	4	5
DSS04	2.5	4	5
DSS05	2.6	4	5
DSS06	2.5	4	5

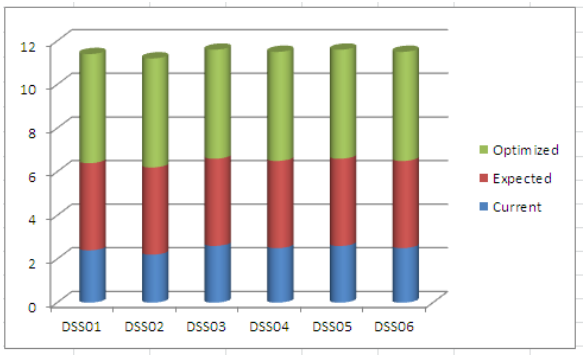

Figure 4. Column Graph of Process Capability Domain Deliver,Service and Support

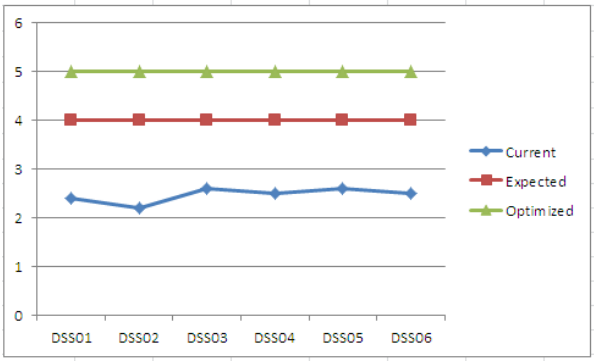

Figure 5.Line Graph of Process Capability Domain Deliver, Service and Support

Journal of Renewable Energy, Electrical, and Computer Engineering, 2 (1) (2022) 38-46

Conclusion

Based on the results of research and analysis carried out in the institution, it can be concluded that the analysis was carried out using COBIT 5 in the DSS (Delivery Service, and Support) domain with a calculation of the capability level, and an average value of 2.2 (managed process) to 2.6 (*Established Process*) was obtained. COBIT only provides control guidelines and does not provide operational implementation guidelines. So that it is expected that in the next research process it can use an audit model other than COBIT 5 as COBIT only focuses on control and measurement.

References

[1] Adriani. N. L,Mahardika.M.S.S andAryani. N.W.S,"Audit of Certification System GovernanceUsing COBIT5", International Journal of Engineering and EmergingTechnology,Vol.3,No. 2,2018.

[2] Andry J. F, "Audit of IT Governance Basedon COBIT 5 Assessments: A Case Study, "TEKNOSI, Vol. 02, No. 02, 2016.

[3] Jarsa.V.and Cristianto. K,"I T Governance Audit with COBIT 5 Frameworkon DSS Domain, "KINETIK,Vol. 3,No.4,Pp.279-286, 2018

[4] Putri. M. A. , Aknuranda. I and Mahmudy. W. F," Maturity Evaluation of Information Technology Governancein PT DEF Using Cobit 5 Framework," Journal of Information Technology and Computer Science Volume 2, Number 1, pp. 19-27, 2017.

[5] Sabatini. G, Setyohadi. D. B and Purnomo. Y. S Information Technology Governance Assessment in Universitas Atma Jaya Yogyakarta using COBIT 5 Framework", Electrical Engineering, Computer Science and Informatics (EECSI), 2017.

[6] Nyonawan. M, Suharjito and Utama. D. N,"Evaluation of Information Technology Governance in STMIK Mikroskil Using COBIT 5 Framework", International Conference on Information Management and Technology (ICIMTech), 2018.

[7] Kurnia. H. M, Shofa.R.N and Rianto, "Audit Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Berdasarkan Domain APO12", Jurnal SITECH, Vol 1, No 2, 2018.

[8] MahadyaSuta. I. B. L, Mahendra. I. G. N. A. GandSudarma. M, "Application of COBIT5 for Hospital Services Management Information SystemAudit", International Journal of Engineering and EmergingTechnology,Vol. 3,No. 2,2018.

[9] R.Weber,InformationSystemControlandAudit,The University Queensland, PrenticeHall,1999

[10] Turang. D. A. O, and Turang. M. C, "Analisis Audit Tata Kelola Keamanan Teknologi Informasi Menggunakan Framework Cobit 5 Pada Instansi", Kumpulan jurnaL Ilmu Komputer (KLIK) Volume 07, No. 2, 2020.

[11] Jaya. P. A. P, Widyantara. I. M. O. And Linawati , "Audit Penerapan Aplikasi Sistem Keuangan Pemerintah Daerah Kabupaten Klungkung Menggunakan COBIT DOMAIN PO dan ITIL , jurnal Teknologi Elektro, Vol. 16, No1, 2017

[12] Najwa. N. F and Susanto T.D, "Kajian Dan Peluang Penelitian Tata Kelola Teknologi Informasi, Ulasan Literatur Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) Vol. 5, No. 5, pp. 517-530 2018,

[13] Rusydi Umar. R, Riadi. I and Handoyo. E. "Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Integration, Scientific Journal of Informatics Vol. 6, No. 2, 2019

[14] Astikasari D. C and Chandra. S. E, "Evaluation of Information Technology Governance with COBIT 5 in XYZ, "International Journal of Engineering and Techniques, vol.4, no.4, pp.76–86,2018.

[15] ISACA, A Business Framework for the Governance and Management of Enterprise IT,United States of America: ISACA, 2012.

[16] Katili. M. R, Pateda. V, Djafri. M. G and Amali. L. N, "Measuring the capability level of IT governance: a research study of COBIT 5 at Universitas Negeri Gorontalo, International Conference on Education, Science and Technology, 2019.

[17] H. Nugroho, "conceptual model of it governance for higher education based on Cobit 5 framework.," *J. Theor. \& Appl. Inf. Technol.*, vol. 60, no. 2, 2014.

[18] S. De Haes, W. Van Grembergen, dan R. S. Debreceny, "COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities," *J. Inf. Syst.*, vol. 27, no. 1, hal. 307–324, 2013.

[19] C. Juiz, C. Guerrero, dan I. Lera, "Implementing good governance principles for the public sector in information technology governance frameworks," *Open J. Account.*, vol. 2014, 2014.

[20] A. Cater-Steel, M. Toleman, dan W.-G. Tan, "Transforming IT service management-the ITIL impact," 2006.

[21] A. Pasquini, E. Galiè, dan others, "COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process," *Proc. FIKUSZ*, vol. 13, hal. 67–76, 2013.