KINETIK, Vol. 3, No. 4, November 2018, Pp. 279-286
ISSN : 2503-2259
E-ISSN : 2503-2267

IT Governance Audit with COBIT 5 Framework on DSS Domain

Vernando Jarsa[*1], Kevin Christianto[2]
[1,2]Universitas Bunda Mulia Jakarta Utara
vernandojarsa@gmail.com[*1], kchristianto@bundamulia.ac.id[2]

Abstract

Information technology in organizations plays an important role for the continuity of their current business processes. Almost every organization already has information technology and dependence on their information technology. With the existence of information technology, it can help business process in the organization runs smoothly, and according to desired by every organization. But not infrequently the information technology that has been operating has problems that are very annoying and hinder the business process of the organization. Problems that exist in this company is at the time of maintenance and custom or repair process undertaken by the company. With the existence of the problem, the writer wanted to audit the existing governance in companies that have problems regarding aspects of information technology delivery. The author uses the COBIT 5 framework on the DSS domain (Deliver, Service, and Support) and focuses on the sub domains of DSS01 Manage Operations, DSS02 Manage Service Requests and Incidents, DSS03 Manage Problems, and DSS06 Manage Business Process Controls. The assessment method used is a capability model consisting of five capability levels. Based on the audit of information technology governance conducted by researchers using COBIT 5, then the conclusion of this study is the average capability level of the overall process obtained most of the process has reached level 1 performed process.

Keywords: *COBIT 5, Business Process, Capability Level*

1. Introduction

The development of technology and information systems is now progressing very rapidly and plays an important role to improve the competitiveness of their organizations [1]. With the development of information technology makes every company must apply information technology in accordance with business processes and goals of the company. Implementation of information technology costs are not small but the application of information technology is very important and very necessary to support the existing business processes in the company.

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 know whether the information technology that has been operating in accordance with the business processes and objectives of the company and deliver accurately based on IT strategic [2]. In performing information technology processing, need a measuring tool that can be used as a reference to solve the problem [3]. So, the authors conduct information technology governance audits using the COBIT 5 framework. COBIT 5 is one of the frameworks that has a renewal version that brings together modern thinking in the IT engineering and governance of companies and can help companies achieve their goals for corporate governance and IT governance [4]. The author gives assessment using a capability model which is a measurement tool of governance performance or management process can know the performance of process that need to be improved [5]. Based on the above explanation, the authors conduct an audit of information technology governance at PT. Andal Software Prosperous.

PT. Andal Software Sejahtera engaged in the manufacture and maintenance of payroll applications. PT. Andal Software Sejahtera has been established since 1988 and has had customers more than 500 customers. PT. Andal Software Sejahtera wants to help other companies to have payroll software in order to reduce the work and expenses in the company. The problems that exist in the company is in the process of maintenance and custom or repairs that has been done by the company because the process is experiencing problems when

Jarsa, V., & Christianto, K. (2018). IT Governance Audit with COBIT 5 Framework on DSS Domain. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 3(4). doi:http://dx.doi.org/10.22219/kinetik.v3i4.665
Receive June 29, 2018; Revise July 04, 2018; Accepted July 06, 2018

combining the work in a project. Therefore, the author's contribution to the company is to find out the problems that exist in the company so that the authors can perform audits to obtain the capability level that has been achieved by the company at this time and to know the next steps that can be done to improve the process by conducting an audit of technology governance information using the COBIT 5 framework.

In this study the authors took three previous studies relevant to the research theme taken by Johanes Fernandes Andry in 2016 in a journal entitled "Audit of IT Governance Based on COBIT 5 Assessments: A Case Study", which revealed that the application of IT Governance however is a challenge for every organization to ensure IT is aligned with business goals. The purpose of this study is to illustrate the performance of information technology governance to determine the extent of information technology governance skills in the Training Center are currently running, with several aspects to consider in an organization. The result of this study is the average in the DSS domain has reached the value of 2.2 to 2.8 which means it is in the managed process [6]. Tedi S. Agoan, Hans F.Wowor and Stanley Karouw in 2017 in a journal entitled "An analysis of the maturity level of information technology at the Manado communication and informatics office using the COBIT 5 domain Evaluate, Direct, Monitor (EDM) and Deliver, Service , and Support (DSS) ", which revealed that the use of IT in agencies needs to be analyzed for the level of maturity assessment or self-assessment in knowing the condition of IT and organization and internal to know how far the benefits of the use of IT in agencies. The results of this study are the average reached maturity level 3 (established process) for the domain Evaluate, Direct, Monitor (EDM) and maturity level 2 (manage process) for the domain Deliver, Service, Support (DSS) [7]. The next previous research was conducted by Pistia Octaviyanti and Johanes Fernandes Andry in 2018 in a journal entitled "Enterprise Asset Management Audit Using the COBIT Framework 5", which reveals that the Enterprise Asset Management (EAM) system can assist companies in asset management and EAM implementation which can either extend the life of the assets to the company. The purpose of the EAM system audit is to optimize value contribution, manage change in a controlled manner, and manage assets so as to provide more profit for the company. The result of this research is capability level on process of EDM02 reach level 3, capability level on process of BAI06 is 2,75, and capability level in BAI09 process is 2,8. The result of gap analysis on EDM02 process is 1, at BAI06 equal to 0,25, and at BAI09 0,2 to reach expected level [8].

2. Research Method

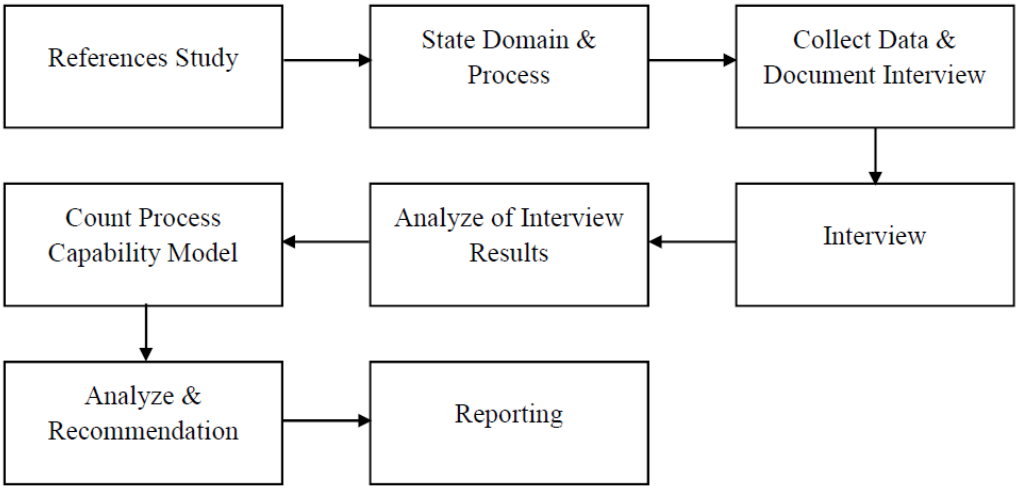

Figure 1. Research Method [8]

Here is an explanation of the flow or stages of research conducted by researchers based on Figure 1, namely:

1. The researcher conducts literature study by finding the theories needed for this research.
2. Researchers stated that the domains and processes used in this research are DSS01 Manage Operations, DSS02 Manage Service Requests and Incidents, DSS03 Manage Problems, and DSS06 Manage Business Process Controls.

3. At the analytical stage the researcher system collects data relating to activities on the domain of DSS01 Manage Operations, DSS02 Manage Service Requests and Incidents, DSS03 Manage Problems, and DSS06 Manage Business Process Controls. and make interview questions according to the domains and sub domains used.
4. The researcher interviewed the party responsible for the company's information system based on the domain of DSS01 Manage Operations, DSS02 Manage Service Requests and Incidents, DSS03 Manage Problems, and DSS06 Manage Business Process Controls.
5. Researchers do the analyze on the results of interviews that have been done based on the assessment scale on COBIT 5, there are 5 levels on the capability level, which are as follows:
   a. Level 0: Incomplete process; the process is not implemented or failed to achieve the purpose of the process. There is little or no evidence of achieving the objectives of the process systematically.
   b. Level 1: Performed process; the implementation of the process has reached its goal. Attributes at this level are:
      PA 1.1 Process performance; measures the extent to which the objectives of a process have been achieved.
   c. Level 2: Managed process; process 1 at level 1 is implemented into a process regulation (planned, monitored, and evaluated) and the work product of the process is properly defined, controlled and maintained. Attributes at this level are:
      PA 2.1 Performance management: measures the extent to which the implementation of the process is governed.
      PA 2.2 Work product management: measures the extent to which the work product is produced by a well-regulated process.
   d. Level 3: Established process; the process at level 2 is implemented using a defined process and able to achieve process results. Attributes at this level are:
      PA 3.1 Process definition: measures the extent to which a process is defined to support the execution of a process.
      PA 3.2 Process deployment: measures the extent to which process standards are implemented effectively.
   e. Level 4: Predictable process; process at level 3 runs with a defined boundary to achieve process results. Attributes at this level are:
      PA 4.1 Process measurement: measures the extent to which measurement results are used to ensure the implementation of processes can support the achievement of organizational goals.
      PA 4.2 Process control: measures the extent to which the process is managed quantitatively to produce a stable and predictable process in accordance with defined boundaries.
   f. Level 5: Optimizing process; the process at level 4 is continually upgraded to meet current and future organizational goals. Attributes at this level are:
      PA 5.1 Process innovation: measures the extent to which process changes are identified from the implementation of the process and from the innovation approach to the implementation of the process.
      PA 5.2 Process optimization: measures the extent to which changes are defined, manages the implementation of processes effectively to support the achievement of process improvement objectives.
6. The author calculates the interview result according to the capability model to determine the capability level of the company by calculating the average capability level of each subdomain, that is by formula: total number of subdomain / subdomain value. Example: ((DSS01-01 + DSS01-02 + DSS01-03 + DSS01-04 + DSS01-05) / 5 = average of capability level from DSS01 domain).
7. Researchers conduct analysis and provide recommendations on information systems that need to be improved in order to improve the information system in accordance with what is expected by the company.
8. The last stage in this research is to make a report of the results of research that has been done.

3. Results and Discussion

At this stage the researcher will discuss about the result of information technology governance audit using COBIT 5 framework with capability model assessment that can measure

the performance of the process at the company so it can know the value of each process. The results and discussion of this information technology governance audit are values of capability and recommendation of each process in the domain. The domains used in the research are Deliver, Service and Support (DSS) consisting of DSS01 Manage Operations, DSS02 Manage Service Requests and Incidents, DSS03 Manage Problems, and DSS06 Manage Business Process Controls.

3.1 DSS01 Manage Operations

This process discusses coordinating and executing the operational activities and procedures required for internal IT and IT outsourcing services, including the application of predefined SOPs and required monitoring activities. The purpose of this process is to produce IT operational services in accordance with the wishes of the organization.

In the DSS01 domain, the company has not maintained, performed and implemented operational procedures consistently because there are no specific SOPs for IT. There are only SOPs in general and for IT infrastructure, especially in monitoring event logs and periodic review of the event logs; outsourced IT services to safeguard corporate information protection and service delivery, then the company has not yet undertaken any training to anticipate in case of natural or human-error, health and safety training, as well as no facilities to assist in the event of a power outage. Then the capability level in DSS01 domain is 1.6 which means only achieve performed process.

Recommendations for DSS01 domains are proposed by companies to backup data every week to be more effective and efficient, then implement more specific SOPs for IT not only in general and in monitoring event logs and routinely review existing event logs to monitor event logs running in accordance with the desired company related to the IT infrastructure, using IT outsourced and ensuring that company requirements for enterprise information security are complied with in accordance with the contract, ensuring that IT priority for service delivery is adhered and integrating internal IT management with outsourced service providers, the next is training how to use tools to anticipate in the event of a natural disaster or human-error result so that every employee knows what to do, and adds tools that can protect IT facilities from power differences and power outages, so if that a power outage happen in company, the company can still continue its business process. In Table 1 below is the capability level for each sub domain in the DSS01 domain.

Table 1. Capability Level Domain DSS01

Sub Domain	Current	Expected
DSS01-01	2	3
DSS01-02	1	3
DSS01-03	2	3
DSS01-04	2	3
DSS01-05	1	3
Average	1,6	

3.2 DSS02 Manage Service Requests and Incidents

This process discuss about responding to appropriate and effective user requests and resolutions of all types of incidents. Restore normal services, record and meet user requests, and investigate, diagnose, upgrade and resolve incidents. The goal of this process is to achieve increased productivity and minimize disruption through quick settlement of user inquiries and incidents.

In the DSS02 domain the company has not applied standard procedures in case of incidents, especially in the maintenance process and also the service request procedure, in addition, there are no regulations / policies in recording new issues and at the closing of service and incident requests, then not filing incident resolution and not using helpdesk to help companies solve existing problems. Then the capability level in DSS02 domain is 1.3 which means only achieving the performed process.

Recommendation for domain DSS02 is proposed the company determine and apply standard procedure if problem / constraint occurs at the time of maintenance so that can know action of beginning which must be done, besides, company not apply procedure in request service as desired by company and also procedure in problem closing and service requests, then the

company proposes using helpdesk so that all issues can be reported to the helpdesk and helpdesk can help companies to solving the problems and provide the best solution, then archive event resolution, so as to allow for future knowledge resources, and implement temporary solutions if problems which has not been completely resolved so that the business process can still run and not loss. In Table 2 below is the capability level for each sub domain in the DSS02 domain.

Table 2. Capability Level Domain DSS02

Sub Domain	Current	Expected
DSS02-01	1	3
DSS02-02	1	3
DSS02-03	1	3
DSS02-04	2	3
DSS02-05	1	3
DSS02-06	1	3
DSS02-07	2	3
Average	1,3	

3.3 DSS03 Manage Problems

Identify and classify problems and root causes and provide timely resolution to prevent recurring events, then provide recommendations for improvement. The goal of this process is to increase availability, improve service levels, reduce costs, and improve customer satisfaction and convenience by reducing the number of operational issues.

In the company's DSS03 domain it does not categorize and prioritize existing problems by prioritizing problems that have a greater impact to solve and not classifying problems by distinguishing known and unknown issues making it easier to handle, then companies have not processed solutions on a benefit-based problem to be obtained and the costs to be incurred by the impacts that will occur and a very important thing, in addition, there are no procedures in closing the problem and request changes and do not apply the policy in reporting problems and not meeting regularly to discuss problems and plan changes . Then the capability level in the domain DSS03 is 1.2 which means only achieving the performed process.

Recommendations for DSS03 domains are that companies should categorize and prioritize existing problems by prioritizing problems that have the greatest impact first to solve to minimize the losses encountered, otherwise classifying the problem by distinguishing known and unknown errors making it easier to handle problems, then process solutions on issues based on benefits to be gained and costs to be incurred, as well as impacts that will occur and what matters most and apply procedures that can regulate in closing issues and change requests so as to be more organized and in line with the steps has been determined and desirable, and also companies apply policies in reporting problems in accordance with the desired company and meeting regularly to discuss problems and plan changes. In Table 3 below is the capability level for each sub domain in the DSS03 domain.

Table 3. Capability Level Domain DSS03

Sub Domain	Current	Expected
DSS03-01	1	3
DSS03-02	1	3
DSS03-03	2	3
DSS03-04	1	3
DSS03-05	1	3
Average	1,2	

3.4 DSS06 Manage Business Process Controls

Determine and maintain appropriate business process controls to ensure that related information is processed by business processes in the company or outsourced has met all relevant information control requirements then identified, and manages and operates adequate controls to ensure that information processing complies with these requirements. The purpose of this process is to maintain information integrity and security of information assets handled in business processes within the company or outside the company [9] [10].

In the DSS06 domain the company is not documenting activities during business process control activities and does not maintain data integrity during unexpected interruptions in business processes, furthermore the company does not periodically review access controls, logs and reports to ensure that all access rights are correct and aligned, then the company has not yet implemented procedures on errors and security procedures to protect the information assets and does not document and maintain evidence of error correction actions, and the company has not yet determined the retention requirements (storage) made based on business needs. Then the capability level in the domain DSS06 is 1.2 which means only achieving the performed process.

Recommendations for DSS06 domains are that companies may documenting activities when controlling business process activities so as to be easier to identify and maintain data integrity during unexpected interruptions in business processes, in addition to the company's regular review of access controls, logs, and reports to ensure that all permissions are right and aligned, then apply procedures on errors ranging from fixing errors, resolving errors and handling unbalanced conditions and security procedures to protect information assets, and specifying retention (storage) requirements made based on business needs ranging from operational needs, financial reporting, and compliance. In Table 4 below is the capability level for each sub domain in the DSS06 domain.

Table 4. Capability Level Domain DSS06

Sub Domain	Current	Expected
DSS06-01	1	3
DSS06-02	1	3
DSS06-03	1	3
DSS06-04	1	3
DSS06-05	2	3
DSS06-06	1	3
Average	1,2	

3.5 Gap Analysis

Gap analysis is the distance between the capability level and the expected level, to compare the capability level obtained with the expected level of each process contained in Table 5. Gap analysis.

Table 5. Gap Analysis

Domain	Capability Level	Expected Level	Gap
DSS01	1,6	3	1,4
DSS02	1,3	3	1,7
DSS03	1,2	3	1,8
DSS06	1,2	3	1,8

Based on Table 5, it can be concluded that the gap between the capability level and the expected level in the DSS01 domain is 1.4 to reach the expected level, then in DSS02 is 1.7 to achieve the expected level, and in DSS03 is 1.8 to reach expected level, and also in DSS06 that is 1.8 needed improvement to reach expected level.

Overall the recommendation for this company is create and apply the procedures and policies that are determined by the company so that the process can run better in accordance with the desired company, in addition, data backup should be done once a week to be more effective and to minimize the occurrence of important data loss, and conduct training regularly for every employee to know what to do when something happens without having to wait for a leader decision.

In Figure 2 is the capability level for the DSS domain (Deliver, Service, and Support). Current is the average capability level of each domain, Expected is the capability level expected by the company, and Optimized is the highest level capability in COBIT 5.

In Figure 2 it can be concluded that the capability level that has been obtained has not reached the capability level expected by the company because most of the level that got stopped at level 1 that is performed process. Then the information technology that has been applied and

running in the company should be improved so it can achieve the expected capability level. Based on the results in the researchers can find that the lack of documentation, procedures, policies and maintenance that make the process at the DSS domain stop at level 1.

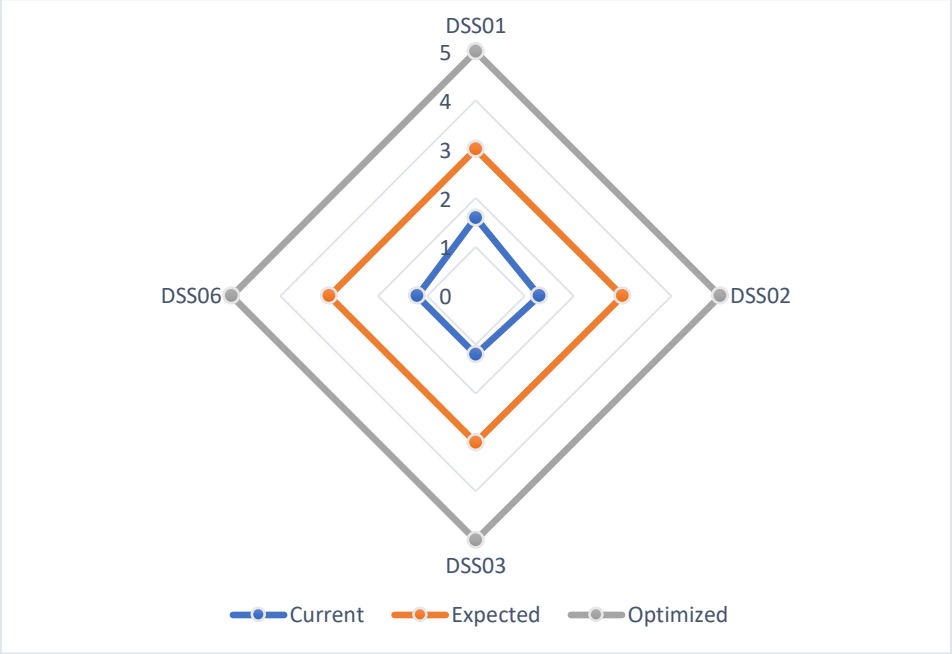

Figure 2. Index Capability Level domain DSS

4. Conclusion

Based on the audit of information technology governance conducted by researchers using COBIT 5, then the conclusion of this study is the average capability level of the overall process obtained most of the process has reached level 1 performed process, which means the activity in the domain DSS is already in line with the objectives of each process but the lack of procedures, policies, and documentation applied by the company that makes most of the processes in the DSS domain stop at level 1. Recommendations proposed by researchers to improve the capability level in accordance with the expected capability level is create and apply the procedures and policies that are determined by the company so that the process can run better in accordance with the desired company, in addition, data backup should be done once a week to be more effective and to minimize the occurrence of important data loss, and conduct training regularly for every employee to know what to do when something happens without having to wait for a leader decision.

References

[1] N. Aulia and S. Handayaningsih, *"Pembuatan Model Tata Kelola It Untuk Proses Akademik Menggunakan Cobit 4 . 1 (Studi Kasus : Universitas XYZ),"* Jurnal Sarjana Teknik Informatiika, Vol. 1, No. 1, Pp. 287–296, 2013.

[2] Wella, *"Audit Sistem Informasi Menggunakan Cobit 5 . 0 Domain DSS pada PT Erajaya Swasembada, Tbk," ULTIMA InfoSys*, Vol. VII, No. 1, Pp. 38–44, 2016.

[3] F. Ajismanto, *"Analisis Domain Proses COBIT Framework 5 Pada Sistem Informasi Worksheet (Studi Kasus : Perguruan Tinggi STMIK , Politeknik Palcomtech) Domain Analysis of COBIT Process Framework 5 In Worksheet Information System (Case Study : STMIK College , Palcomtec,"* Cogito Smart, Vol. 3, No. 2, 2017.

[4] E. Ekowansyah, Y. H. Chrisnanto, Puspita, and N. Sabrina, *"Audit Sistem Informasi Akademik Menggunakan COBIT 5 di Universitas Jenderal Achmad Yani,"* Seminar Nasional Komputer dan Informatika, Vol. 2017, Pp. 201–206, 2017.

[5] R. E. Putri, *"Model Penilaian Kapabilitas Proses Optimasi Resiko Ti Berdasarkan Cobit 5,"* Seminar Nasional Informatika 2015, Vol. 2015, No. November, Pp. 252–258, 2015.

[6] J. F. Andry, *"Audit of IT Governance Based on COBIT 5 Assessments: A Case Study,"* Jurnal Teknologi dan Sistem Informasi, Vol. 2, No. 2, Pp. 27–34, 2016.

[7] T. S. Agoan, H. F. Wowor, and S. Karouw, *"Analisa Tingkat Kematangan Teknologi Informasi Pada Dinas Komunikasi Dan Informatika Kota Manado Menggunakan Framework COBIT 5 Domain Evaluate, Deirect, Monitor (EDM) dan Deliver, Service, and Support (DSS),"* Jurnal Teknik Informatika, Vol. 10, No. 1, Pp. 1–9, 2017.

[8] J. F. Andry, *"Process Capability Model Based on COBIT 5 Assessments (Case Study),"* Jurnal Teknik Informatika dan Informasi (JATISI), Vol. 3, No. 1, 2016.

[9] Isaca, *"COBIT 5: Process Assessment Model (PAM): Using COBIT 5."* 2013.

[10] J. F. Andry and K. Christianto, *"Audit Menggunakan COBIT 4.1 dan COBIT 5 dengan Case Study."* Yogyakarta: TEKNOSAIN, 2018.