**semanTIK**, Vol.6, No.2, Jul-Des 2020, pp. 1-8
ISSN: 2502-8928 (Online)
DOI : 10.5281/zenodo.4394146
**Terakreditasi "Peringkat 4 (Sinta 4)" oleh Kemenristekdikti**
Website : http://ojs.uho.ac.id/index.php/semantik



# INFORMATION TECHNOLOGY AUDIT USING COBIT 5 ON DELIVER DOMAIN, SERVICE AND SUPPORT (DSS) IN PT. XYZ, A MINING COMPANY

**Joe Yuan Mambu[*1], Valentshea Doringin[2], Sintya Hamise[3], Erienika M. Lompoliu[4]**
[1,2,3]Fakultas Ilmu Komputer, Universitas Klabat, Airmadidi
[4]Fakultas Ekonomi dan Bisnis, Universitas Klabat, Airmadidi
e-mail: [*1]**joeyuan.mambu@unklab.ac.id**, [2]vhayrin@gmail.com, [3]sintyahamise023@gmail.com, [4]erienika.lompoliu@unklab.ac.id

**Abstract**

Information Technology (IT) is crucial for companies. With technology, all jobs can be made easily by humans and can advance business processes more quickly and effectively. To find out the extent of the company's development in IT processing, an audit is needed. Without an efficient use of IT, companies will only waste IT-related investment that has been made. The purpose of this study is to audit IT governance implemented in a mining company XYZ. The IT governance audit that we use is based on the COBIT 5. framework. In this study, we use one Deliver, Service, Support (DSS) domain that includes six subdomains: DSS01 (Manage Operations), DSS02 (Manage Service requests and Incidents), DSS03 (Manage Problems), DSS04 (Manage Continuity), DSS05 (Manage Security Service), and DSS06 (Manage Business Process Control). For data collection in this study, researchers used interviews and questionnaire methods for related parties. The results of the IT Maturity Level for DSS domains reached an average level 2 or Managed Process, which shows that the company was able to operate the IT process yet with unclear definition and standard operating procedure nor evaluation or planned improvement.

**Keywords**; COBIT 5, DSS, Capability Level, IT Auditing

## 1. INTRODUCTION

It is a common thing that Information Technology has become essential in organizations or companies because it simplifies the business process. The advancement of Information Technology in this era can be seen in many kinds of devices of every hardware, software, and telecommunication. Information technology was created to support humans in doing any type of activities more effectively and efficiently. Companies make use of information technology in reaching their strategic plan along with the vision and mission [1]. Companies and organizations rely on the use of information technology that is well designed to manage the company data more effectively and useful in managing the management and decision making [2].

Information technology needs to be well organized so it can be used properly. Thus, an audit is necessary to measure and evaluate an information technology adopted by the company and determine the company standard [3]. Seeing the advantages of Information Technology, XYZ Company, an undisclosed name due to privacy rights, decided to implement Information Technology into their business process. Information Technology added significant value to the company and can make their activities more effective and efficient. Therefore, the use of technology in supporting a company's business individually to compete in the globalization era is essential. However, most companies only focus on the

procurement of hardware and software, neglecting the importance of the employees' training to increase their performance and prevent future problems in the work system because of poor information management [4].

Information Technology Audit is really important for a company because it aims to create a good IT Governance, which is an activity of using IT management in order to generate a maximum expense, decision making, and problem-solving process [5]. The audit was first started only for a financial report. However, with the rapid changes in technology, IT's role was budgeted into the company investment. Accordingly, a professional audit for IT functionality is existed [6].

The object of this research is a company named XYZ. This company engaged in gold mining, which is located at an undisclosed location. The government has approved this mining since 1968. The 400.000 square kilometers of the gold mining area was operated from 2010 until 2011. The shareholders play an essential role in making this company successful. They enabled the company project production to work on time according to their schedule. XYZ Company was well managed using the right information technology to return the company investment. They adopted Information Technology to lead the company as the assurance for investment to answer without fail. To prevent any risk in spoiling the company investment, an Information Technology audit is needed to know the standard of Information Technology usage in the company. COBIT (Control Objectives for Information and Related Technologies) and ITIL (Information Technology Infrastructure Library) are good alternatives to measure the company standard.

In auditing, COBIT 5 was chosen as the primary tool, which is the best practice of a framework. COBIT is used to measure an organization's maturity, and the framework was often used for auditing. COBIT focused more on controlling instead of executing. This practice will always maximize the IT role in business investment, ensuring an excellent service deliverance and providing measurement to evaluate when there are errors. [7]. In 1992, ISACA created COBIT and became a standard focusing on business target and process, and was made as an IT technical tool and managerial [5].

There are five domains in 5th version COBIT, such as APO (Align, Plan, and Organize), EDM (Evaluate, Direct, and Monitor), BAI (Build, Acquire and Implement), MEA (Monitor, Evaluate and Assess), and DSS (Deliver, Service, and Support). This research is only focused on one of the domains, which is DSS (Deliver, Support, and Service) [8].

DSS summarized the service delivery, which is corresponding with the user service, data management, security management, and continuity. Parts of DSS are managed service requests, manage operations, and incident, manage continuity, manage business process control, manage problems, manage security services [6]. Manage operations in a company aim to achieve the transformation from input to output like products or services, manage service request, and incident in a company strive to be responsible for any incident. Manage problems in a company aim to manage the cycle of any issues that are already happened and were predicted to occur, manage continuity aim to return the company performance on the right track after experiencing an incident. Manage security services for a company aim to protect the data and information from future threats, and manage business process control aim to optimized and monitoring the business activities and to create the business progress. The researcher decided to use the DSS domain according to the XYZ company situation where technology is adopted, the need for delivery, service, and information technology support service [9]. DSS also focused on the implementation of an information technology system that is more effective and efficient [10].

A measurement using the Process Capability Model (PCM) is executed on an excellent realization of IT management in XYZ Company. PCM is defined as having six levels start from 0 to 5, which is representing the incremental capability of the applied process [3].

Therefore, the purpose of this research is to measure the maturity level of information technology using the COBIT 5 framework in the Deliver, Service and Support (DSS) Domain for XYZ Company.

## 2. RESEARCH METHOD

The research aims to perform an Information Technology audit by measuring the maturity level using COBIT 5 framework in Deliver, Service and Support (DSS) domain for XYZ Company. DSS domain is an object which is an influential factor of this research. There are six subdomains in the DSS domain as the references for this research. There are Manage Operations, Manage Service Requests and Incidents, Manage Problem, Manage Continuity, Manage Security Service, Manage Business Process Control.

### 2.1 Research Time and Location

The research location is where the research is drawing the data from responders. The research location is situated at an undisclosed, due to privacy issues, remote areas from November 2019 until March 2020.

### 2.2 Research Responders

Any information or data from a trustable source is required to work on this research. Data and information were gained based on the RACI (Responsible, Accountable, Consulted, Informed) mapping [11]. The chosen responder for this research is one person who was selected according to the RACI chart mapping along with the Responsible (R) and Accountable (A), which is the Helpdesk Coordinator. The chart form of RACI mapping can be seen in Table 1.

Since the Helpdesk Coordinator is accountable (fully responsible) for all the DSS domain, he would best choice to answer and provide documents as necessary evidence such as SOP documentation or activities log. All the answer is backed up by documentation, thus having one source can be sufficient.

Table 1 Mapping Of Respondents To RACI Chart

| DSS | *Helpdesk Coordinator* | *Programmer* | *Telco Coordinator* | *IT Engineer* | *Software Development Specialist* | *IT Manager* |
|---|---|---|---|---|---|---|
| DSS01 | RA | C | C | C | C | I |
| DSS02 | A | R | C | C | C | I |
| DSS03 | A | C | C | R | C | I |
| DSS04 | R | C | A | R | R | CI |
| DSS05 | RC | R | R | RC | AC | I |
| DSS06 | A | C | R | R | RC | I |

### 2.3 Research Method

The research method for this research is descriptive and qualitative. The qualitative data was obtained from the documentation of every event, recording, and documentation related to the condition. By using this method, this research could reach the non-linear step, to prove that this research can be done based on the clear rule and an accurate explanation of a situation [12].

### 2.4 Data

The obtained is obtained directly from the research object, which was collected from the questionnaire forms shared with the IT Staff in XYZ Company.

### 2.5 Data Collection Technique

In collecting the data, the researcher is doing a direct interview with the company and collecting the data with an open ended questionnaire and interview to the IT Staff of the company.

### 2.6 Research Design

Research Design is designed for procedures in performing the research. The research design is practical for researchers to conduct the investigation effectively. The design of this research is about collecting data and analyzing data procedures.

On Figure 1 can be seen the flow diagram of the research.

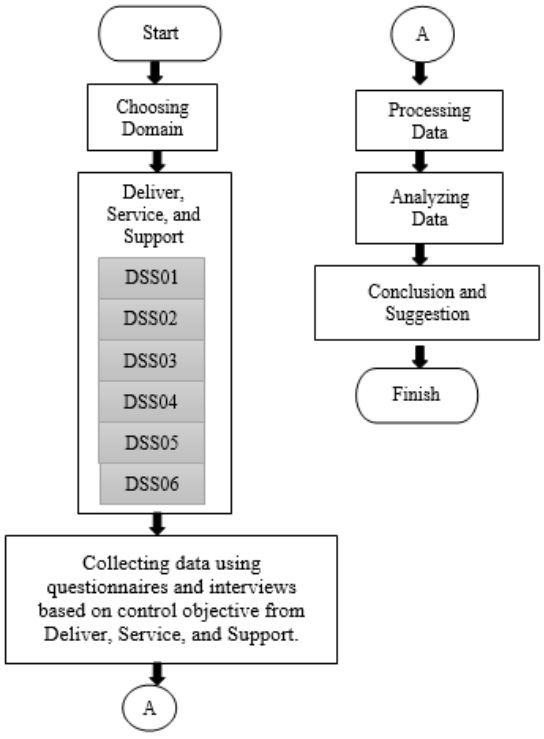


Figure 1 Research Flow Diagram

These are the explanations of the steps above:

1. The researcher starts to determine the designated research domains. The chosen domain is DSS with its six control objectives (Manage Operations), (Manage Service Requests and Incidents), (Manage Problems), (Manage continuity), (Manage Security Service), and (Manage Business Process Controls).
2. The researcher then gathers data through questionnaires and interviews with the related person of interest. Due to the nature of the question, all questions are open-ended and mostly asked directly through several interviews
3. From the recorded interview the researcher process and analyze the answers and map it to the maturity level of each domain
4. From the mapped maturity level the researcher then come up with result, suggestion, and conclusion for the company DSS domain audit

2.7 Description of Each DSS Sub Domains

There is a total of six DSS sub-domains, and here is the description of each domain [13]:

1. DSS01: Co-ordinate and enforce the tasks and organizational processes necessary to provide IT facilities internally and externally, including the implementation of the predefined standard operating procedures and reporting activities required.
   Questions asks in this subdomain including: How IT operational procedures is handled (e.g. SOP of IT operational), Outsourced IT services (e.g. Service Level Agreement (SLA) on outsourced IT services, IT infrastructure monitoring (e.g. logs of incidents and ticketing), and other related issues that can be seen on ISACA COBIT 5 DSS01 guidelines [13, pp. 173-175]
2. DSS02: Provide timely and efficient response and resolution of customer requests for all forms of incidents. Recovery, inquiry, evaluation, escalation and settlement for regular service; documenting & meeting customer requests.
   Questions asks in this subdomain including: How incidents and service is classified (e.g. incidents' priority and categorization), record of the incident prioritation (e.g. systems that logs incidents description and prioritation), service request verification and approval process, and other issues can be seen on ISACA COBIT 5 DSS02 guidelines [13, pp. 178-180]
3. DSS03: Identify and categorize issues and root causes and address repeated accidents promptly. Provide change guidelines.
   Questions asks in this subdomain including: How problems, not incident, is identified and classified (e.g. problem, is identified and classified by its priority or impacts), how investigation and diagnose been done (e.g. procedures in problem handling), how issue is raised (e.g. log issue in the system), and other issues can be seen on ISACA COBIT 5 DSS03 [13, pp. 181-183]
4. DSS04: Create and retain a strategy to allow business and IT to adapt to events and disturbances in order to continue the activity of essential business processes and IT resources needed and to retain the supply of information at a degree appropriate to the organization.
   Questions asks in this subdomain including: How business continuity is defined in policies (e.g. Business continuity scope and objectives ), have an exercise on the business continuity (e.g. Have the Business Continuity Plan (BCP) tested regularly), review and improve the BCP (e.g. Have a regular meeting to review the BCP), and other issues can be seen on ISACA COBIT 5 DSS04 [13, pp. 185-189]
5. DSS05: To ensure the degree of information protection risk appropriate to the organization in compliance with the security policies, protect enterprise information. Establishing and maintaining information control roles and access privileges and controlling protection.
   Questions asks in this subdomain including: How the system is protected against malware (e.g. Antivirus implementation), how the network and connectivity is secured (e.g. How the firewall and Intrusion Detection System

(IDS) is implemented), how the endpoint security is implemented (e.g. End user security policy and regulation), how the physical security of the IT assets (e.g. door and cabinet access to IT rooms) and other issues can be seen on ISACA COBIT 5 DSS04 [13, pp. 191-195]

6. DSS06: Establish and maintain adequate business process controls to ensure that all applicable information processing criteria are fulfilled by information related to and processed by in-house or outsourced business processes. Identify the appropriate criteria for information management and maintain and operate sufficient controls to ensure that these requirements are met by information and information processing.

   Questions asks in this subdomain including: How the business activities is aligned with the business objectives (e.g. IT policies and plan is based on the company strategic plan), how the information control within and outside the company (e.g. using encrypted messaging services), access control of company digital assets (e.g. access control management on companies files), and other issues can be seen on ISACA COBIT 5 DSS06 [13, pp. 197-200]

## 3. RESULT AND DISCUSSION

### 3.1 Domain DSS Result

Through the interview and data gathering, the result of the auditing process is shown in Table 2

Table 2 Maturity Calculation of Every DSS Domain

| DSS | Maturity Level |
|---|---|
| DSS01 | 3 |
| DSS02 | 2 |
| DSS03 | 2 |
| DSS04 | 2 |
| DSS05 | 1 |
| DSS06 | 2 |

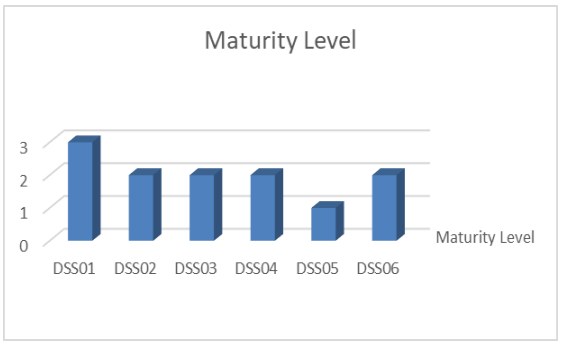


Figure 2 Maturity Level of IT DSS Domain Chart for PT. XYZ

### 3.2 Improvement Recommendation

1. DSS01 Recommendation

According to the Maturity Level's analysed result on the DSS01 interview, which is occurred on the third level or (Established Process). These are the recommendations for XYZ Company.

a) There is a set schedule of every operational procedure in XYZ Company activities. To improve the performance, it is recommended to evaluate and update every available SOP.
b) Conducting updates every time an error is found in performing the procedures.

2. DSS02 Recommendation

According to the analysed result of the DSS02 Maturity Level Interview, which is on the second level or (Managed Process), these are the XYZ Company's recommendations.

a) Divide tasks or responsibilities in handling every incident or problem.
b) Conduct a regular meeting to evaluate every occurred incident.
c) Own an SOP to support every incident handling activity.

3. DSS03 Recommendation

According to the analysed result of the DSS03 Maturity Level Interview, which is on the second level or (Managed Process), these are the XYZ Company's recommendations.

a) Conduct a performance in handling a pending incident or undone tasks and assign them back into a prioritized order that has to be done.
b) Conduct proper documentation of every problem that happened to prevent any repetition problem in the future.

c) Own a clear SOP and always evaluate it to have an excellent performance in handling data access or ticketing problems. IT asset handling can be adequately evaluated.

4. DSS04 Recommendation

According to the analysed result of the DSS04 Maturity Level Interview, which is on the second level or (Managed Process), these are the XYZ Company's recommendations.

a) Own an SOP for every conducted strategy in handling every incident.
b) Own a designated plan to be implemented outside the company (for hardware) if a disaster occurs.
c) Conduct training for every internal and external IT party regularly towards their responsibilities of every incident that happened.

5. DSS05 Recommendation

According to the analyzed result of DSS05 Maturity Level Interview, which is on the first level or (Performed Process), then these are the recommendations for the XYZ Company.

a) Own an SOP to conduct every security step for the company data.
b) Create a policy of every entry access to the company's IT office and provide the physical security of every document inside the office or the IT assets.

6. DSS06 Recommendation

According to the analyzed result of DSS06 Maturity Level Interview, which is on the second level or (Managed Process, then these are the recommendations for the XYZ Company.

a) Have written documentation of data delivery and information validation procedure.
b) Conduct a regular check of the system and find out the update time.
c) Own a security asset in delivering information outside the company and have a good SOP.

## 4. CONCLUSION

According to the IT Maturity Level result from the research conducted in XYZ Company. These are the conclusions of the result:

1. Based on the Maturity Level Result, it is known that the IT Maturity Level for the DSS Domain has averagely reached the second level (Managed Process) which means there is still a manageable process. The IT process task has been well managed through the planning and evaluating steps, which become better. Meanwhile, DSS01 has the highest maturity level reached a third level (Established Process), that means it is on the implementation step where the process is already standardized and available to be implemented in every company scope in IT, so in other words, XYZ Company is standing on the stabilized step or Established Process. Aside from DSS01, there is also DSS05, which averagely reached the first level of maturity (Performed Process), which means every process has been arranged and all the staffs of the IT department are aware of it and assigned their responsibilities.
2. In every sub-domain process inside the DSS domain, recommendation and improvement are given to be used later to improve the maturity level progress in reaching the maturity level goal in the future for a better company,
3. According to the analysed result from Picture 4.1, where the whole DSS Domain chart is summarized, it can be seen that the highest level is DSS01, level 1. Every subdomain activity averagely has reached the second level, which means every running activity has its task and requires an SOP to sustain the subdomain in achieving a higher level.
4. Based on the audit result of XYZ Company, it is concluded that most of the IT activities have performed well. Each of the actions has its designated process and is executed according to the SOP. Some activities rely on the responsibilities, which has decreased the audit value because it was performed without the SOP.

## 5. RECOMMENDATION AND SUGGESTION

According to the Information Technology Maturity Level result using COBIT 5 in XYZ Company, there are four suggestions from the researcher to be used for

further research in the future that is related to COBIT 5 below:

1. It is recommended to arrange the right time to interview with the interviewees; it is suggested two weeks before the appointment. While interviewing, it is good to take notes and record to get a significant result.
2. This research only uses one domain; further research is recommended to have more than one domain.
3. It is recommended to specify the RACI mapping before choosing the interviewees so that the interview questionnaire can all be fulfilled.
4. It is recommended to use mapping in accordance with the company vision and mission for the chosen domain to get a more significant scope.

## DAFTAR PUSTAKA


[1] H. F. Kurniawan, "Analisis Penggunaan Teknologi Informasi dan Pengaruhnya Terhadap Semangat Kerja Pegawai Kantor Kementerian Agama Di Wilayah Yogyakarta," Universitas Islam Negeri Sunan Kalijaga, p. 79, 2014.

[2] J. Y. Mambu, J. Rewah, A. C. Iskak, and O. N. Sigarlaki, "Evaluasi Sistem Informasi Universitas Klabat Menggunakan Framework COBIT 5.0 Pada Domain MEA," Cogito Smart Journal, vol. 5, p. 10, Desember 2019.

[3] R. K. Candra, I. Atastina, and Y. Firdaus, "Audit Teknologi Informasi menggunakan Framework COBIT 5 Pada Domain DSS (Delivery, Service, and Support) (Studi Kasus : iGracias Telkom University)," e-Proceeding of Engineering, vol. 2, p. 16, Apr. 2015.

[4] Y. W. Cahyadi, "Pengukuruan Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Pada PRoses Align, Planning, And Organize Terkait Layanan Internet (Studi Kasus: PT. Lestari Mahaputra Buana)," Universitas Pasundan Bandung, p. 14, Desember 2017.

[5] W. Wella, "Audit Sistem Informasi Menggunakan Cobit 5.0 Domain DSS pada PT Erajaya Swasembada, Tbk," ULTIMA, InfoSys, vol. VII, p. 7, Jun. 2016.

[6] I. M. M. Matin, A. Arini, and L. K. Wardhani, "Analisis Keamanan Informasi Data Center Menggunakan Cobit 5," J. Teknik inform., vol. 10, no. 2, pp. 119–128, Jan. 2018, doi: 10.15408/jti.v10i2.7026.

[7] H. Agung and J. F. Andry, "Audit Sistem Informasi Akademik Pada Universitas XYZ Menggunakan COBIT 5 Pada Domain Deliver, Service & Support (DSS)," Seminar Nasional Teknologi Fakultas Teknik Universitas Krisnadwipayana, p. 9, Jul. 2019.

[8] M. A. Helmiawan, "COBIT 5 Untuk Manajemen Teknologi Informasi & Proses Bisnis Perusahaan," Informasi, vol. IX, p. 15.

[9] J. F. Andry, "Audit Tata Kelola TI Menggunakan Kerangka Kerja COBIT Pada Domain DS dan ME Di Perusahaan Kreavi Informatika Solusindo," Seminar Nasional Teknologi Informasi dan Komunikasi (SENTIKA), p. 8, Mar. 2016.

[10] R. G. Mufti, Suprapto, and Y. T. Mursityo, "Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT Martina Berto Tbk)," Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 1, pp. 1622–1631, Desember 2017.

[11] J. M. Jacka and P. J. Keller, *Business Process Mapping: Improving Customer Satisfaction.* New Jersey: John Wiley & Sons, Inc, 2009.

[12] E. Salamah, S. Purwaningsih, and R. Kurnia, "Kandungan Mineral Remis (Corbicula Javanica) Akibat Proses Pengolahan," Jurnal Akuatika, vol. III No.1, p. 10, Mar. 2012.

[13] ISACA, *COBIT 5: Enabling Processes*. New York: ISACA, 2012