Maturity Evaluation of Information Technology Governance in PT DEF Using Cobit 5 Framework

Mayang Anglingsari Putri[1], Ismiarta Aknuranda[2], Wayan Firdaus Mahmudy[3]

[123] Faculty of Computer Science, Brawijaya University

{mayang3110@gmail.com, i.aknuranda@ub.ac.id, wayanfm@ub.ac.id}

Abstract. Information technology governance is used to guide and control an organization in achieving the goals that had been planned in advance. PT DEF is a company which utilizes information technology to support its business processes. Nevertheless, it indeed requires an IT governance that can be beneficial as a reference for IT activities in order to run properly. This research intends to conduct an audit of information technology governance based on the COBIT 5 framework domain, which is DSS (Deliver, Service and Support) domain in the process of DSS03 (Manage Problems). According to the research results, the values that have been obtained from the process of DSS03 capability level was 64.66%, that is regarded as Partially Achieved. Capability level will be used as a reference in seeking gap contained in the domain of DSS03 process. Furthermore, these would be able to make recommendations aimed at increasing the value of the expected maturity. This research contributes to the evaluation results and recommendations to improve the capability level on DSS03 domain, hence PT DEF can upgrade its IT governance by using DSS03 process.

1   Introduction

Governance is helpful to guide and control an organization in achieving the goals that had been planned in advance. 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 [1][2]. In obtaining these purposes requires a control mechanism or information technology audit to assume the extent of IT governance [3].

One of the companies that have been performed information technology to support its operating system is PT DEF. PT DEF is one of the companies which engaged in the field of electricity and utilizes IT to gain its operational activities. However, upon on observations that have been done, PT. DEF does not have a certain rule yet in the governance of IT and tend to perform activities on the circumstance of sudden and unfocused in the handling of IT. This probably cause IT performances in the organisasion become deficient. Therefore, PT DEF needs an audit of technology governance. Audit information technology system is an activity that enables to measure

how proper a system of information that has been running in the organization. Audit information system emphasizes on some vital aspects which are checking whether the computerized organization system can support asset security, whether it can support the achievement of the organization, whether it is already utilizing resources efficiently, and whether consistency is guranteed and whether the data is accurate.

When conducting the audit of information technology governance, there is a standard that can be engaged and recognized globally. One of these standards that may be useful is Control Objectives for Information and related Technology 5 (COBIT 5) released by IT Governance Institute (ITGI), which is part of ISACA [4][5][6].

Based on the mapping of COBIT 5 Enterprise Goals to IT related Goals has been obtained a single process in the domain that is DSS domain (Deliver, Service and Support) on DSS03 process (Managing Problems). The description of DSS03 process is to determine problems in a company along with its causes, and then presents the resolution for certain period to prevent the recurrence of incidents and provide recommendations for improvement [7].

On early research, the standard of COBIT 4.1 framework in auditing information technology governance took place in PT PLN Kediri. The research was conducted to determine the extent of information technology governance that have been run on the domain to all domain of COBIT 4.1 which are domain Plan Organize (PO), Deliver Support (DS), Monitor Evaluate (MO), and Acquire Implement (AI). This study had results in the evaluation and recommendations for improvement that can be applied to PT. PLN Kediri, in which company would be able to arrange planning of IT infrastructure development procedures asociates with domain of COBIT 4.1 [8].

The implementation of the COBIT framework is also engaged in   another research. This current research was presented about the tools for client-vendor to communicate is capable of supporting multiple functions of IT controls which are regulated by the COBIT framework. In addition, domain of COBIT framework is worthwhile to coordinate both communication and control for project development (Gantman & Fedorowicz 2016). COBIT and ISO 27001 is applied to evaluate the information technology security in the insurance companies. The subjective of this research is to indicate how vital the role of data security evaluation in the insurance companies, because the customers' data is something that is confidential and important [9].

Based on the issues mentioned above, this research is conducted using the COBIT 5 framework standards in auditing information technology governance at PT DEF. This research is conducted to determine the extent of IT governance in the DSS domain of DSS03 process that has been run by PT DEF. Due to the exixtence of information technology audit governance, there is expected to provide a reference for improving the information technology governance in order to run business objectives properly as planned.

2   Methodology

2.1   COBIT 5

COBIT 5 is a framework used to measure and improve IT governance [10][11]. COBIT was selected because it has ability both of IT control and   provides IT measurement framework for analysis of objects that needs to be repaired [12]. There are five main principles in COBIT 5 as follows [13]:
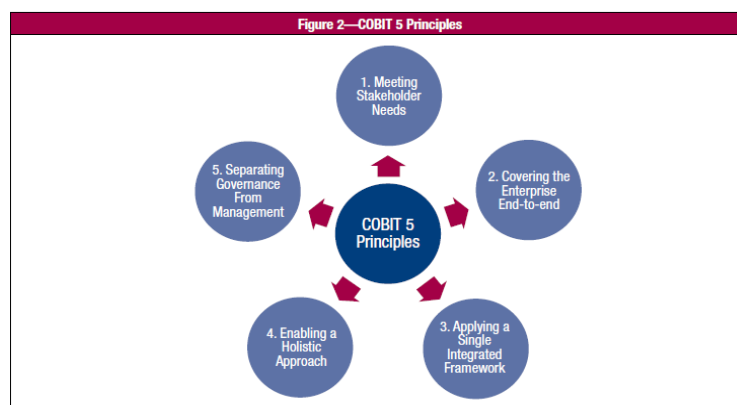

Figure 1. COBIT 5 Principles

1.   Meeting Stakeholders Needs

It is necessary for companies to consider all stakeholders who involved, when making decisions related to advantages, resources and risk assessment decisions.

2.   Covering the Enterprose End to End

COBIT 5 does not only concern over the governance of IT functions but also considers information technology as an asset that must be protected as much as any other asset in the organization.

3.   Applying a Single Integrated Framework

COBIT 5 enables for being used by organizations as comprehensive governance and integrator governance framework.

4.   Enabling a Holistic Approach

COBIT 5 is defined as a group of enablers that supports to apply comprehensive governance.

5.   Separating Governance and Management

This principle explains that within the framework COBIT 5 makes a solid differentiation between management and governance. COBIT 5 defines the information technology activities into five domains, as follows:

Table 1. COBIT 5 Domain

Domain	Descriptions
EDM (*Evaluate, Direct and Monitor*)	This governance process deals with the aims of stakeholders, including assesment, risk optimization and companies resources.
APO (*Align, Plan and Organise*)	Scouting to solutions delivery (BAI) and availability of service and support (DSS)
BAI (*Build, Acquire and Implement*)	Providing solutions and through it, so that it will turn out to be a service
DSS (*Deliver, Service and Support*)	Accepting solutions and beneficial to the final users.
MEA(*Monitor,Evaluate,and Assess*)	Monitoring within processes so that the rules are followed correctly.

The method used in this research at PT DEF based on COBIT 5 framework is as follows:
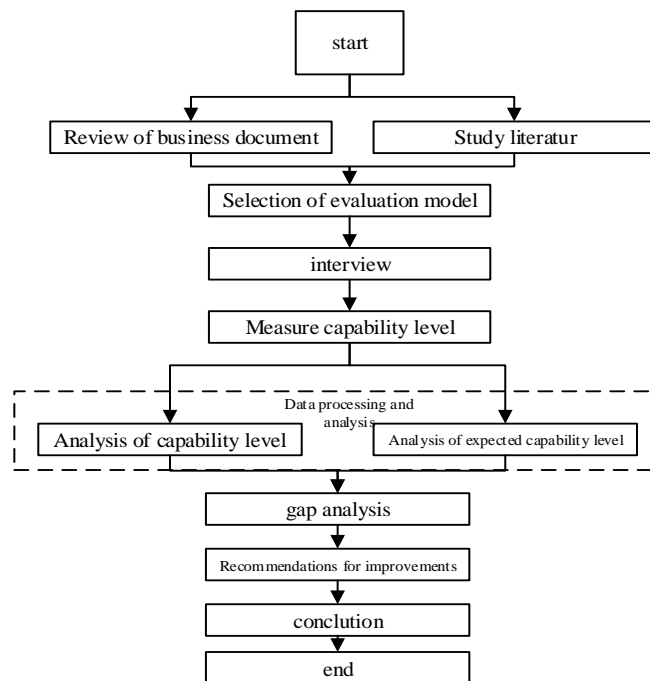
Figure 2. The stages of research methodology

On this research, respondents who participated in determining the value of DSS domain in the DSS03 process were five employees of IT department. According to the COBIT 5 of ISACA states that respondents determination based on RACI (Responsible, Accountable, Consulted, Informed) table is used to determine the respondents.

Based on interviews conducted with employees at PT DEF had been obtained mapped enterprise goals in IT related field for mapping process and evaluation. Mapping results can be seen in the following table:

Table 2. Mapping Results

Enterprise Goal	IT Related Goal	IT Process
Optimisation of business process functionality	Integrating technology into a business process to support and empower business processes.	DSS03- *Manage Problems*

The next stage, data was developed to guide the capability level of COBIT 5. Below is the translation of recapitulation calculation formula in order to obtain the stage of Capability Level:

$$A = \frac{\sum BPr + \sum input + \sum output}{BPr} \qquad (1)$$

$$CL = \frac{A1 + A2 + A3 + \cdots An}{Total\ A} \qquad (2)$$

Details

A = Average konversion, bp, input and ouput

BPr = Best Practice

$\sum BP$ = Best Practice Total in %

$\sum input$ = Input total in %

$\sum output$ = Output total in %

CL = Total amount of Capacity Level

Assessing the capability levels [14] are divided into stages as follows:

Table 3. Mapping the Value Range Capability

Range Capability Level
0 – Incomplete Process
1 – Performed Process
2 – Managed Process
3 – Established Process
4 – Predictable Process
5 – Optimizing Process

By rating level [14] as follows:

Table 4. Rating Levels

Abreviation	Description %	Achieved
N	Not achieved	0 to 15% achievement
P	Partially achieved	>15% to 50% achievement
L	Largely achieved	>50% to 85% achievement
V	Fully achieved	>85% to 100% achievement

3   Results

3.1   Capability Level Measurement

DSS03 process is a 'Manage Problems', according to ISACA (2012), Manage Problem is a description of DSS03 process to identify problems and then provides resolution for certain period to prevent the recurrence of incidents and presents recommendations for improvement. This research utilizes sub domain of DSS03 which are:

Table 5. Best Practices DSS03

Process	Base Practices (BPs)	Description
DSS03	DSS03-BP1	Classify problems
	DSS03-BP2	Diagnose problems
	DSS03-BP3	Lift the known error
	DSS03-BP4	Resolve and close the problem
	DSS03-BP5	Perform problem management proactively

Rate capability level was obtained with the calculation of interviews recapitulation, and then measure the rate of capability level on DSS03 process based on the level of response capability.

Table 6. Capability Level Measurement of DSS03

BASE PRACTIES	S	Outcomes DSS03-01
DSS03-BP1	1	1
DSS03-BP2	0	1
DSS03-BP3	1	1
DSS03-BP4	0	1
DSS03-BP5	1	1
$\sum BP$r		80%
Input Work Products (WPs)	**A**	
The Risk-related root causes	1	1
Criteria for registration issues	1	1
Problem about log	1	1
Incident resolution	0	1
Closed service and incident requests	0	1
$\sum i$nput		60%

Output Work Products (WPs)	A	
Problem classification scheme	1	1
Status report issues	1	1
About internal registers	0	1
Root cause of Internal problem	1	1
Problem resolution report	1	1
Records of known error	0	1
Proposed solution to find out the error	1	1
Closed problem records	0	1
Knowledge communication is learned	1	1
Problem resolution monitoring report	0	1
Identified ongoing solutions	1	1
$\sum Output$		54%
CL		64.67%

Based on recapitulation data above, the calculation results of capability level on DSS03 process had the results of 64.66% which means 'Partially Achieved'. While stands on level 1 the activity is called 'Manage Change Acceptance and Transitioning', the process is still at the stage of planned and monitored has not been implemented fully.

3.2   Maturity Rate Analysis

Current Capability is the average value of maturity level from the actual circumstance (As Is) of   DSS03 process, while Expected Capability is the average value of maturity target level expected (To be) to determine the average results. Capability Level can be seen as follows:

Table 8. Gap Analysis of Maturity Rate (Capability Level)

Domain	Current Capability	Expected Level	Gap
DSS03	1	2	1

Based on table data of Value Gap Capability Level as-is by to-be Domain DSS of DSS03 process above, could be obtained graphic as follows:
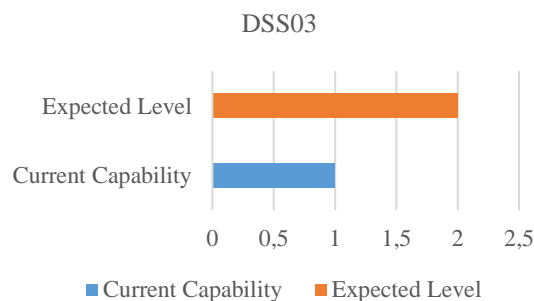

Figure 3. Capability Level Graphic

Below is gaps description or gap in every domain of DSS03 which have been found by the researchers:

According to the audit findings have been made in the research, hence recommendations have been made in order to support increasing value of maturity   IT governance at PT DEF. Recommendations can be given for improvement toward governance processes are as follows:

1) PT DEF needs to be aware of the need for risk management issues, yet there is still uncertain formal procedures and processes that do not well organized.

2) If there is a damage or issue on the system, PT DEF side could make improvements individually and carried out in conditions of a sudden which have no formal procedures and documents.

3) While addressing issues or interruptions on existing IT infrastructure, PT DEF will monitor the damage first, but the maintenance is done by suddenly without any standard procedures.

4   Fixing Recommendations

Once the results audit of bussiness processes have been determined. The results of the capability level also could be gained, those then may used to arrange a table of recommendations and improvements to achieve the target (To be).

This improvement recommendations derived from the calculation results analysis and the level capability gap analysis as a form of design solutions to provide a proposed improvement. Proposed improvements are arranged directly so companies would be able to increase its level of maturity as expected. Determining recommendation is done by providing repair solutions for every process that has not fullest to the 100%. It begins from the whole process which contained on maturity rate at levels that must be completed. Recommendations can be given to repair IT governance processes as follows:

1) Perform the analysis and evaluation of errors that have occurred in each steps in the workability of IT projects on a regular basis.

2) Arrage a risk analysis that may occur in the future, for example, the risk when the network or server is down or one of the tools is damaged. Thus, design solutions asosiates with potencial issues.

3) Arrange cost analysis for mistakes should have been made.

4) Display the potencial risk analysis with proper format.

5) Perform documentation towards repairment issues, thus if there is unexpected issue takes place could be handle easily.

5   Conclusions

The evaluation results of information technology governance audit in PT. DEF according to the calculation value of capability level of DSS03 process was 64.66% which regarded as Partially Achieved and stood ini level 1 of capability. Value gap between present value (as-is) and expected value (to-be) on DSS domain in the DSS03

process in PT DEF was based on capability level calculation which has a plenty gap. Purposes recomendations that may be used to increase the rate of every domain of COBIT 5 process, so it can be useful as fixing recommendation for companies. This research presents such prosedures to evaluate the process of IT governance in certain company asosiates with COBIT 5 framework. For upcoming study, researchers would compare results of IT governance audit between COBIT 4.1 and COBIT 5 which would apply in the companies.

References

[1] R. Fauzan, R. Latifah, P. S. Informasi, F. Teknik, and U. K. Indonesia, "Audit Tata Kelola Teknologi Informasi Untuk Mengontrol Manajemen Kualitas Menggunakan (Studi Kasus : PT Nikkatsu Electric Works)," *J. Tek. Inform. dan Sist. Inf.*, vol. 1, pp. 235–244, 2015.

[2] D. S. Kerr and U. S. Murthy, "Information & Management The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations : An international survey," *Inf. Manag.*, vol. 50, no. 7, pp. 590–597, 2013.

[3] M. A. Putri, I. Aknuranda, and W. F. Mahmudy, "Development of a Conceptual Framework to Determine Improvement of IT Governance using COBIT 5 and AHP-GA," *Adv. Res. Circuits Syst. Int. Conf. Malaysia*, pp. 1–6.

[4] R. Gomes, "The Main Benefits Of Cobit In A High Public Educational Institution - A Case Study," *Pacific Asia Conf. Inf. Syst.*, 2009.

[5] A. Syamsudin and E. T. Lutfi, "Evaluasi Tingkat Kematangan Tata Kelola Teknologi Informasi Stain Kediri Menggunakan Framework COBIT 5," *Semin. Nas. Teknol. Inf. dan Multimed. 2014 STMIK AMIKOM Yogyakarta*, pp. 1–5, 2014.

[6] S. M. Mutu, T. Kapabilitas, and S. Guttman, "Evaluasi dan Perbaikan Kualitas Pelayanan Menggunakan COBIT 5 Domain APO (APO11)," vol. 3, 2008.

[7] ISACA, *COBIT 5 : The Framework*. USA: IT Governance Institute, 2012.

[8] M. A. Putri, V. A. Lestari, and I. Aknuranda, "Audit of Information Technology Governance Using COBIT 4.1: Case Study in PT. XY," *Int. Conf. Ind. Internet Things (ICIIOT), Bandung,Indonesia*, pp. 1–7.

[9] T. Mataracioglu and S. Ozkan, "Governing Information Security in Conjunction With COBIT and ISO 27001," *Int. J. Netw. Secur. Its Appl.*, pp. 1–5.

[10] H. Purba, "Study of IT Governance Development Use Cobit 4 . 1 and AHP at Education Institution (Case Study : Adventist University of Indonesia)," *J. Teknol. Inf. Dan Komun.*, vol. 2, 2009.

[11] ISACA, *COBIT 4.1*. IT Governance Institute, 2007.

[12] E. W. N. Bernroider and M. Ivanov, "IT project management control and the Control Objectives for IT and related Technology (CobiT) framework," *Int. J. Proj. Manag.*, vol. 29, pp. 325–336, 2011.

[13] Isaca, "COBIT 5 : The Framework - Exposure Draft," *USA IT Gov. Inst.*, p. 86, 2011.

[14] ISACA, *Process Assessment Model (PAM): Using COBIT 5*. USA: IT Governance Institute, 2012.