JOIN (Jurnal Online Informatika)
Volume 3 No. 2 | December 2018: 68-73
DOI: 10.15575/join.v3i2.226

Data Center Risks Analysis Through The COBIT Framework 4.1

Arini[1], Luh Kesuma Wardhani[2], Iik Muhamad Malik Matin[3]
[1,2,3]Informatics Engineering, Faculty of Science and Technology
UIN Syarif Hidayatullah, Jakarta, Indonesia
[1]arini@uinjkt.ac.id, [2]luhkesuma@uinjkt.ac.id, [3]iikmuhamadmalikmatin@mhs.uinjkt.ac.id

***Abstract*- Information Technology Governance in UIN Jakarta is the responsibility of the Pusat Teknologi Informasi dan Pangkalan Data (Pustipanda). Some troubles have occurred in the data center Pustipanda, among others the loss of courses and its values that have been inputted in the application of Academic Information System (AIS), loss of data that has been inputted on the application Beban Kinerja Dosen (BKD), damage data content on the portal in the environment UIN Jakarta. Risk analysis is needed to identify and anticipate and minimize risks which may occur. In this research, the risk analysis is using the COBIT 4.1 framework that is in the PO9 process (Manage and Assess IT Risk) as input towards PO9 is the domain of PO1, PO10, DS2, DS4, DS5, ME1, and ME4. Questionnaires which were distributed to respondents were developed from input variables. Respondents were chosen by purposive sampling method. The results of the questionnaire were recapitulated and calculated the value and degree of capability. The result of this research is the level of domain capability in data center Pustipanda is at level 2 (managed) with value 1.91. A fairly low value is obtained on DS4, DS5 and ME1 domains, which are 1.67, 1.88 and 0.67. Arosen risks from the majority of data center risk assessment were the absence of documented policies and procedure and lack of training for risk management measures at Pustipanda data center.**

***Keyword* : COBIT 4.1, data center, risk, IT Governance**

I. INTRODUCTION

Information Technology (IT) has an important role for every company which uses information technology in its business activities, and categorised as one of the factors in achieving company goals. IT will be optimal if only the IT management is maximized. Proper management of IT in a company will certainly identify all forms of risk from the application of IT and the handling of the risks which will be faced. Hence, the company requires an application which is needed to be carried out by the company, namely implementing IT Governance.

IT Governance is intended as a pattern of authority/policy towards the act of IT. This pattern includes building policies and management of IT Infrastructure, using IT by end-users efficiently, effectively and safely, as well as effective IT Project Management processes[1].

The COBIT standard of the ISACA institution in United States defines IT Governance as "*a structure of processes and processes to direct and enterprise control in order to achieve the return of goals and value while balancing risk versus return over IT and its processes*"[2]. Whereas according to Oltsik, IT Governance is defined as a collection of policies, processes/activities and procedures to support IT operations so that the results are in line with business strategy (organizational strategy). The scope of IT Governance in large-scale companies usually includes the occasions related to *Change Management, Problem Management, Release Management, Availability Management* and even *Service-Level Management*[3].

In realization of IT Governance in a company, it is impossible for IT management in medium and medium scale companies comes from the computer department (IT Function) only. All parties (stakeholders) must be involved in accordance with their proportions as end-users.

UIN Syarif Hidayatullah Jakarta as a fairly large organization also utilizes and relies on IT in all fields of work. UIN Syarif Hidayatullah Jakarta has a special unit which handles IT matters on campus, namely PUSTIPANDA (*Pusat Teknologi Informasi dan Pangkalan Data*). The vision of Pustipanda UIN Syarif Hidayatullah Jakarta focuses on becoming a world-class digital university to support scientific, Islamic, and Indonesianness integration, with the scope of tasks in developing systems and networks and data centers[4].

The data center which is managed by Pustipanda supports all functions. The functions allow various models of university business activities to run on Internet services, intranets, and both. Some disruptions have occurred in the data center of Pustipanda which resulted in disruption of IT services to users in the UIN campus environment. These disruptions include loss of grades in the Academic Information System (AIS) application, loss of courses which have been inputted in AIS, loss of data inputted to the application of Lecturer Performance Load (BKD) that has been inputted, and damage to content on the portal in the environment UIN Jakarta. Therefore, it is necessary to analyze the existing risks.

This risk analysis is a process in risk management within an organization. Therefore, the problems of IT risk management are also important things which can

Received: Augus 14, 2018: Revised: December 3, 2018; Received: January 9, 2019; Published: January 31, 2019

affect university business activities. Risk management plays an important role as an action to protect IT assets at a university. The data center of Pustipanda risk management process needs a framework which can map the risks that might occur and how universities, in this case Pustipanda, apply strategies so that the risks that might arise can be overcome. One of the frameworks which will be used to carry out risk management is the *Control Objective for Information and related Technology* (COBIT).

COBIT is a standard guide to information technology management practices which is one of the frameworks that can be used to analyze information technology risk management. The COBIT standard is issued by the IT Governance Institute which is part of ISACA. The COBIT Framework implies a framework which can evaluate IT services through the domain of Deliver and Support domain which concerns the actual delivery of services needed. The domain concerns on compiling traditional operations on security and continuity aspects until training, this domain includes the actual data processing through the application system which often classified in application control[5]. Given the importance of the Pustipanda data center as a backbone of business processes at UIN Jakarta, this study focuses on the risk analysis of the Pustipanda data center at UIN Syarif Hidayatullah Jakarta using the COBIT framework 4.1.

II. METHOD

A. DATA COLLECTION METHOD

1. Observation

The researcher observed the Pustipanda on the first floor of the Sharia and Law Faculty building UIN Syarif Hidayatullah Jakarta. Observations were conducted to observe the Pustipanda data center condition, the technology infrastructure which is used, and the required documents collection.

2. Questionnaire

Questionnaires were distributed to Pustipanda related parties to clarify the risks identified in the data center. This questionnaire contains questions concerning risks which might arise in managing the data center. This questionnaire was developed from COBIT 4 PO9 (Manage and Asses Risk). The weight of the selected answer represents the value and level of capability of the maturity level of related domain.

The Purposive Sampling method is used in determining respondents, namely determining respondents with special considerations so that it is appropriate to be used as respondents. The chosen respondents are respondents who have roles and responsibilities which are in accordance with the object under study.

B. RESEARCH PROCEDURES

Cobit 4.1 framework is used in carrying out the Pustipanda data center risk analysis. The COBIT 4.1 Framework was chosen to be used as an analysis method as COBIT 4.1 provides the Plan and Organize (PO) phases where one sub-section of the PO is PO9 which discusses information technology risk assessment and management. PO9 is conducted by creating and maintaining a risk management framework. In general, the stages used for PO9 are risk identification, risk assessment, risk management and risk monitoring[6]. In accordance with the problem, the research procedure is limited to the risk assessment stage.

At the procedure of research object identification will be conducted towards the research object related to research subject identity, namely vision, mission, core business, quality objectives.

Risk identification will be the main concern at the business process in the Pustipanda data center in the procedure of risk identification. Identification was done by looking at various factors which influence business processes, such as business profiles, applications, infrastructure, operations, and human resources. Therefore, the procedure results the list of risks which may be shown in the data center process.

After the risk is identified, an assessment of the risk will be carried out. Emerging risks will be confirmed to the informant in the form of a questionnaire to see the relationship between risk and business processes. Questionnaire questions refer to objective controls on the domains PO1, PO10, DS2, DS4, DS5, ME1 and ME4. The results of this assessment stage are a description of the risks that might arise in the Pustipanda data center. The results of this assessment will be the basis for deciding on the handling actions that will be given to those risks. The research procedure can be seen in Figure 1 below:

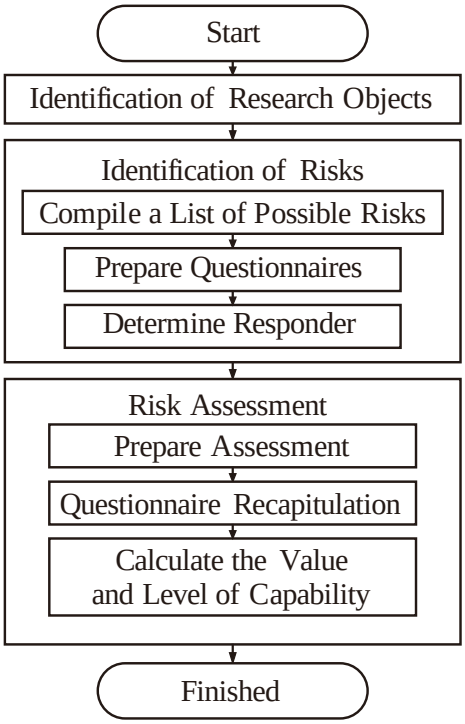

Figure 1. Research Framework

ISSN 2527-1682 (Print)
ISSN 2527-9165 (Online)

III. RESULT AND DISCUSSION

A. THE IDENTIFICATION OF RESEARCH OBJECT

1. Vision and Mision of Pustipanda

The vision of Pustipanda in UIN Syarif Hidayatullah Jakarta is focused to be a World-Class Digital University to support the Integration of Science, Islam, and Indonesianness. The missions of Pustipanda are 1). Improving the performance of information systems for innovative, creative, high availability, high reliability, secure, fast, informed, documented, and integrated universities in order to improve the performance and quality of education, teaching, research, scientific publications, community service and the organization of UIN Syarif Hidayatullah Jakarta, 2). Improving the quality of university governance by utilizing Information and Communications Technology (ICT) technology, 3). Improving research in the ICT field in order to maintain the business continuity and knowledge share of the development of Information and Communications Technology (ICT)

2. Core Business

Core Business of Pustipanda are 1). Implementing information system development and maintenance, 2). Implementing network development and maintenance, 3). Implementing information systems and network services, 4). Implementing cooperation between computer centers and information systems at universities and/or other agencies at home and abroad, 5). Central computer administration.

3. Quality Target

Pustipanda Quality goals are 1). Making Information and Communications Technology (ICT) systems which are oriented to the needs of stakeholders and shareholders of UIN Syarif Hidayatullah Jakarta, 2). Improving the quality of infrastructure, human resources, and services of Information and Communications Technology (ICT) within UIN Syarif Hidayatullah UIN, 3). Developing and implementing IT governance in accordance with national and international standards.

B. THE IDENTIFICATION OF RISKS

1. Arranging the List of Possible Risks

In the case of the Pustipanda data center, risks may arise from various aspects, such as application, infrastructure, human resources, and operations. Each aspects are very important to be taken into account as it is possible that one of the risk factors from one aspect will cause the business process or Pustipanda activity not to work as it should and ultimately not reach the planned goals. Hence, every aspect which influences the business process of Pustipanda needs to be reviewed properly.

The stages of analysis were carried out starting from the risk identification stage. The following stage will allow the identification of the possible risks which will appear in the business process or Pustipanda activities. The risks may arise from the side of application, infrastructure, human resources, and operations as the object of this research is the Pustipanda data center. Therefore, the risks were identified. The results of identification can be seen in Table 1.

Table 1. The result of risk identification

Risk Factors	Risks
Human Resource	Misapplication of access right
	Misapplication of position
	Unfavorable staff
	Unable to prevent risks
	Uncomprehensive acknowledgement of the work field
	Unable to prevent possible risks
	Lacks of training towards work field
	Lack of data or information from internal business/institution
	Unmatch data or information within the fact
	Former user/staff still gain access
	Physical access which is unauthorized
	Data Lose
	Human error
	Damage risk due to human resource (cybercrime, terrorism, hijacking)
Nature	Storm
	Flood
	Dust
	Dew
	Earthquake
	Fire
	Humid
	Heat Radiation
	Temperature
Application and Technology	Backup failure
	Damaged Data
	Failure/ hardware damaged
	Terminated signal connection
	Low signal quality
	Overheat
	Overload
	Stolen Ware
	Full Storage
	Full Storage
	System Crash
	Unstable Electrical Voltage
	Technology Used
	Virus
Infrastructure Security	Room Access Key
	Room Key
	Access control list
	Firewall
	Idss

Risk Factors	Risks
	Host idss
	Layer 2 security feature (*data link layer*)
	Layer 3 security feature
	Password
	CCTV (physical security)
	Monitoring
	Policy (monitoring)
	Center of generator and center of cooler security
	Location

2. Preparing the Questionnaire

The questionnaire in this study was designed with reference from COBIT 4.1 capability model in PO9. PO9 must also pay attention to the objective controls as inputs for the PO9 process, namely PO1, PO10, DS2, DS4, DS5, ME1 and ME4. The weight of the selected answer represents the value and level of capability of the maturity level of the related domain.

3. Determining Respondent

In determining the right respondent to fill out the questionnaire, Purposive Sampling method is used. In order for the data obtained to be representative, the respondents who could answer the questionnaire were those who are responsible and know the processes and activities in the data center. There are 3 (three) respondents who were considered to have responsibility and knowledge related to data center activities, namely:

1. Head of Puspipanda,
2. Field Coordinator of Data Center and Security,
3. Field Staf Data Center and Security.

C. THE ASSESSMENT OF RISK

1. Arranging Assessment

Questionnaire assessment was conducted after gaining the data from respondent answer. Questionnaire assessment was based on the value and level of capability which was published by COBIT.

Table 2. The Result of Risk Identification

Value Range	Answer	Value of Capability	Level of Capability
0,00-0,50	0	0.00	0 *Incomplete Process*
0,51-1,50	1	1.00	1 *Performed Process*
1,51-2,50	2	2.00	2. *Managed Process*
2,51-3,50	3	3.00	3. *Established Process*
3,51-4,50	4	4.00	4 *Predictable Process*
4,51-5,0	5	5.00	5 *Optimizing Process*

2. The Recapitulation of Questionnaire

The questionnaire was addressed to respondents who understood the object of the research, namely the Pustipanda data center, in this case, the head of the Pustipanda, data center coordinator and data center staff. There were questions in the questionnaire which was divided based on several aspects, namely business profiles, applications, infrastructure, human resources, and operations.

In conducting the questionnaire recapitulation, the questions were grouped according to domain variables, where in the assessment of the PO9, PO1, PO10, DS2, DS4, DS5, ME1 and ME4 domain variables were process inputs.

3. The Determination of Capability Value and Level

The calculation of questionnaire recapitulation in determining capability value and level could be formulated as:

a. Value and level of capability PO1

$$\mathrm{CL} = \frac{33}{12} = 2.75$$

According to the calculation, PO1 placed in the third level of capability with a value of 2.75.

b. Value and level of capability PO10

$$\mathrm{CL} = \frac{5}{3} = 1.7$$

According to the calculation, PO10 placed in the second level of capability with value of 1.7.

c. Value and level of capability DS2

$$\mathrm{CL} = \frac{21}{10} = 2.1$$

According to the calculation, DS2 placed in the second level of capability with value of 2.1.

d. Value and level of capability DS4

$$\mathrm{CL} = \frac{87}{52} = 1.67$$

According to the calculation, DS4 placed in the second level of capability with value of 1.67.

e. Value and level of capability DS5

$$\mathrm{CL} = \frac{130}{69} = 1.88$$

According to the calculation, DS5 placed in the second level of capability with value of 1.88.

f. Value and level of capability ME1

$$\mathrm{CL} = \frac{2}{3} = 0{,}67$$

According to the calculation, ME1 placed in the first level of capability with value of 0.67.

g. Value and level of capability ME4

$$\mathrm{CL} = \frac{2}{1} = 2$$

According to the calculation, ME4 placed in the second level of capability with value of 2.

According to the calculation of value and level of capability, it could be concluded that the value and level of capability which could be seen in Table 3 and Picture 2.

ISSN 2527-1682 (Print)
ISSN 2527-9165 (Online)

Table 3. The result of questionnaire value

Input	Maturity		
	Value	Level	The Meaning of Level
PO1	2.75	3	Established
PO10	2.3	2	Managed
DS2	2.10	2	Managed
DS4	1.67	2	Managed
DS5	1.88	2	Managed
ME1	0.67	1	Performed
ME4	2.00	2	Managed
Average	1,91	2	Managed

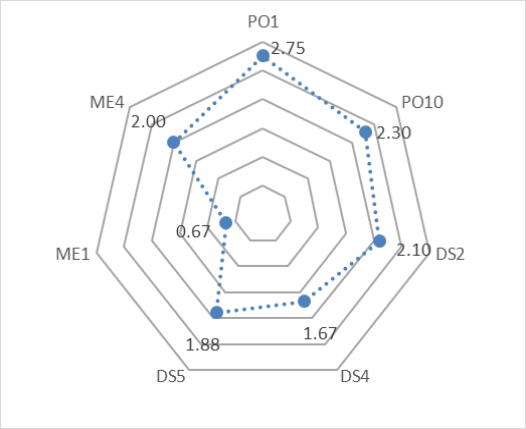

Figure 2. The capability result from value and level measurement of UIN Jakarta P09 data center

Based on the value and level of capability in table 3, the result shows that respondents rated the maturity level of PO9 domain (manage and assess IT risk) in the data center Pustipanda at level 2 (managed) with a value of 1.91. The level of capability at level 2 shows that the Pustipanda data center of UIN Jakarta has carried out business process activities according to the stated objectives. Everyone in Pustipanda data center accesses sufficient resources to carry out their respective tasks. Planning and monitoring activities for activities in the data center have been carried out, but not all activities have been documented.

Table 4. The act of data center Pustipanda documentation

No.	Activity	Documentation	
		Available	Unavailable
1.	Failure handling/ Hardware failure	√	
2.	Failure handling/ Software failure	√	
3.	Overheat handling		√
4.	Full storage handling		√
5.	Low signal quality handling	√	
6.	Unauthorized accessed information		√
7.	Misapplication of access right handling		√
8.	Corrupted data handling	√	
9.	Terminated network handling	√	
10.	System crash handling	√	
11.	Server down handling	√	

Some risks which would hinder the Pustipanda business process was also identified by questionnaire. The following results may be seen in Table 4. These risks come from the DS5 domain (Ensure Security System), DS4 (Ensure Continuity Service) and ME1 (Monitor and Evaluate IT Performance).

The crucial risk is shown through DS5 as Pustipanda does not have procedures to overcome security vulnerabilities, report security or incident problems yet, and has not carried out security training for staff. Therefore, the DS5 maturity value which was assessed by respondents was quite low, 1.88, and at level 2.

Table 5. Some risks at data center Pustipanda

Variable of Domain	Risk
DS5	Pustipanda has not had the rightful procedure to handle low-security issue.
	Pustipanda has not had the policy and procedure to submit problems or incident.
	Pustipanda has not had a security training as development and testing.
DS4	Pustipanda has not had a periodical testing towards disaster recovery plan and business resumption plan.
	Pustipanda already has the guidelines to manage the protocol and allowed services in the network but still has not documented.
	Pustipanda has not had formal process which was documented to eliminate data either physically or electronically.
	Pustipanda has the documentation regarding supplementary configuration for infrastructure but it was updated.
	Pustipanda has the documentation regarding diagram of application architecture and diagram of *data flow* diagram but it was not updated.
	Pustipanda has not had a rightful policy and procedure as a handling of media backup and restore.
	The staffs of Pustipanda have not had a detailed knowledge as an act of risk handling.
	Pustipanda has not had the handling documentation towards overheat, full storage, backup failure, unauthorized

Variable of Domain	Risk
	accessed information, misapplication access right / user ID, overload handling.
ME1	Pustipanda has conducted system revire but was not documented.

Whereas in DS4, the respondent gives a capability value of 1.67 and the capability level is in level 2 (managed). Arose risks are due to the lack of documentation of several processes. The absence of documentation means that the Pustipanda has not implemented measures for the continuity of service yet. Aside from documentation problems, arose risks in DS4 is an implementation of risk prevention training for staff. This is very necessary for a proper service in UIN Jakarta academic community.

While the ME1 domain (Monitor and Evaluate IT Performance) has a capability value of 0.67 and is at the capability of level 1 (performed). Being at level 1 means that your library has run the process to achieve the objectives for monitoring and evaluation. This process has not been planned, it has not been conducted periodically and has not been documented.

The questionnaire also obtained PO1 domain results (Define Strategic IT Plan) which have a pretty good value of 2.75 and are at the capability level 3 (Established). Pustipanda has defined a strategic plan for developing information technology at UIN Jakarta. This is stated in the Pustipanda planning, strategy, and *Indikator Kinerja Utama (IKU)*

IV. CONCLUSIONS

The conclusion of this study is:

1. In general, the data center of Pustipanda is in the level of 2 (managed) with a value of 1.91. The level of capability at level 2 shows that the Pustipanda data center of UIN Jakarta has carried out business process activities according to the stated objectives. Everyone in the field of Pustipanda data center accesses sufficient resources to carry out their respective tasks. Planning and monitoring activities for activities in the data center have been carried out, but not all activities have been documented.
2. The data center of Pustipanda has a low value for the DS5 domain (Ensure System Security), DS4 (Ensure Continuity Service) and ME1 (Monitor and Evaluate IT performance). In order not to obstruct the data center in achieving its objectives, the risks outlined in table 5 must be handled.

Suggestions regarding the research are:

1. Continue the analysis of risks to the handling and monitoring risks.
2. Conduct the analysis of risks through different method.

V. REFERENCES

[1] V. Sambamurthy and R. W. Zmud, "Arrangements for Information Technology Governance: A Theory of Multiple Contingencies," *MIS Q.*, vol. 23, no. 2, p. 261, Jun. 1999.

[2] K. Brand, H. Boonen, and IT Service Management Forum., *IT Governance based on COBIT® 4.1 : A Management Guide*. Van Haren Publishing, 2007.

[3] J. Oltsik, "IT Governance: Is IT Governance the Answer?," *Tech Republic*, 2003. .

[4] Pustipanda, "About Us | Pustipanda UIN Syarif Hidayatullah Jakarta." [Online]. Available: https://pustipanda.uinjkt.ac.id/about-us/. [Accessed: 01-Oct-2016].

[5] B. Supradono, "Tingkat Kematangan Tata Kelola Teknologi Informasi (IT Governance) pada Layanan dan Dukungan Teknologi Informasi (Kasus: Perguruan Tinggi Swasta di Kota Semarang)," in *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2011 (Semantik 2011)*, 2011.

[6] Information Systems Audit and Control Association., *COBIT Process Assessment Model (PAM) : using COBIT 4.1*. ISACA, 2011.