4thICITB

AUDIT OF INFORMATION SYSTEM USING COBIT 5.0 AND ITIL V3 FOR INFORMATION SYSTEM OF ACADEMIC

Rini Nurlistiani[1)], R.Z Abdul Aziz[2)]

Informatics and Business Institute Darmajaya
[1]rininurlistiani@gmail.com, [2]rz.aziz@gmail.com

ABSTRACT

Information Technology (IT) is very important for sustainability and business growth. Dependence on IT requires special attention to governance which consists of leadership, organizational structure, and processes. it ensure that IT in the organization not only develops, but also sustains the company's strategy and goals. Informatics and Business Institute Darmajaya is one of the private universities in Bandar Lampung that utilizes IT in carrying out academic activities, one of which is by using the Information System of Academic (SISKA). In the implementation of good SISKA, an audit of information system needed to improve the performance of the system. In this study, audit for information system of academic used Control Objective for Information and related Technology (COBIT 5.0) on domains DSS01-DSS06, MEA-01, APO-12, and APO-13, as well as other references to determine improvement suggestions by adding the Information Processing Infrastructure Library (ITIL V3) on the domain process of Service Operation and Service Design processes as a framework. This study was used to evaluate the governance information systems of academic at Darmajaya to produce some recommendations for improvement. The results was used to provide recommendations for improvements to the information technology governance of SISKA IIB Darmajaya. For measure, this study using addition validity and reliability with SPSS tools to testing produce appropriate improvements for IT governance.

Keywords: Audit of Information System, COBIT 5.0, ITIL V3, IT Governance

INTRODUCTION

Information governance is the responsibility of the board of directors and management at the top level, this part of the management of the company and consists of leaders, all members of the organizational structure. These processes was used to ensure that existing information technology (IT) supports and assists the achievement of organizational strategies and

objectives (ITGI, 2003).

Information technology governance is also defined as a structured relationship and process to direct and control the organization to achieve its goals by balancing risks. IT governance is a process of directing and controlling IT that is currently in the organization and which is still planned; including monitoring and directing existing plans, and monitoring and evaluating the implementation, policies and strategies of IT so that the organization can achieve its goals. Although the definitions differ in several aspects, they all focus on the same issue, namely how IT can provide value by aligning the relationship between IT and business so that IT can reduce risk (COBIT Steering Committee and the ITGI, 2000).

Audit of Information System is the process of collecting and evaluating evidence to determine whether a computer system can secure assets, maintain data integrity, can drive the achievement of organizational goals effectively and use resources efficiently (Ron Weber, 1999). The audit stages according to (Gallegos, 2014) include several activities, that is Planning, Field Check, Reporting and Follow Up.

Control Objective for Information and Related Technology (COBIT) is a framework for IT management and management. This framework also helps create optimal value from the use of IT by balancing the benefits that exist with risk optimization and resource use. In this study COBIT version 5.0 is used for allows related IT to be regulated and managed holistically for all organizations related to end-to-end business processes in full and functional areas of responsibility, as well as considering IT in accordance with the interests of internal and external stakeholders (COBIT Steering Committee and the ITGI, 2012).

Information Technology Infrastructure Library (ITIL) is also the most recognized framework in the world. Since it was created twenty years ago, ITIL has evolved and changed so that it has deepened business and technological practices that have developed. The ISO / EIC 20000 standard provides formal and universal standards for organizations to obtain audit and certification of service management capabilities. While ISO / EIC 20000 is a standard that must be achieved and maintained, ITIL is a collection of useful knowledge to achieve these standards (Cabinet Office, ITIL Service Strategy, 2011). Through an audit of information system using COBIT 5.0 and ITIL V3, Putri Adella Elvina (2013) conduct study to evaluate staffing services at Diskominfo in Palembang city. Furthermore, Marrone Burgoa (2011) are adopted ITIL V3 and COBIT 4.1 to improve the company's operational processes. Similar research was also carried out by Dong Zhang

(2015) who conducted IT governance for small and medium enterprises (SMEs) in China. And Cherono-Winnie (2014) conduct research about the management of information & communication technology (ICT) at IT companies in Kenya using validity & reliability testing for IT governance measurement.

In this study, the researcher used DSS-01 to DSS-06, MEA-01, APO-12 and APO-13 domains. As well as the process at ITIL V3, namely Service Operation, Service Design, and Continual Service Improvement to conduct IT governance audits to improve the performance of existing information systems, and provide recommendations for good improvements to IT governance from information systems of academic.

Capability and Maturity Level Proses COBIT 5 and ITIL V3
Capability process level that is used to measure company IT maturity level (IT *Governance Mapping of COBIT 5 with ITIL V3 2011. ISACA. 2012)* on tabel 1.

Table 1. Capability dan Maturity Level COBIT 5 and ITIL V3

Index of Scale (ITIL V3)	Capability Level (COBIT 5)	Description
0,00 – 0,50	0 - Incomplete Process	The process is not implemented or fails to achieve its purpose
0,51 – 1,50	1 - Performed process	The process is implemented and achieves its process purpose
1,51 – 2,50	2 - Managed process	The process was implemented and managed with planning and adjustment
2,51 – 3,50	3 - Established Process	A defined process is used based on a standard process.
3,51 – 4,50	4 - Predictable Process	The process that had been applied before now operates within the limits determined to achieve the results of the process .
4,51 – 5,00	5 - Optimizing Process	The process is continuously improved to meet relevant current and projected business goals.

RESEARCH METHOD

In this study, The steps that was taken included the planning to determine the scope, subject, object to be audited, evaluation of audit results and communication with the ICT-Center bureau and Standard Operating Procedure (SOPs) related to the management of Standard Operating Procedure systems. Analyzing policies was done by collecting information through filling out questionnaires online through the Google Form as seen in Figures 1 and 2 with the number of respondents as many 100 people.

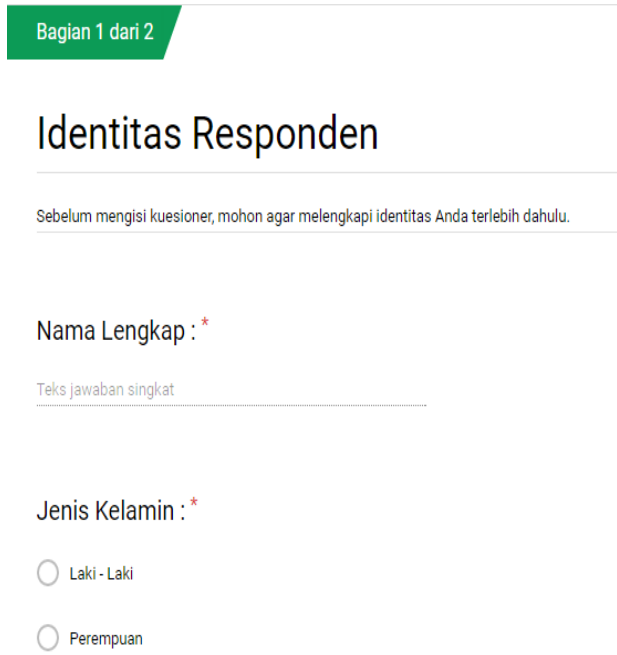

Figure 1. Identity of Respondent Layout

Figure 2. Quetioner Layout

In this stage ITIL V3 2011 mapping was carried out with COBIT 5. The aim was to obtain IT processes in COBIT 5 that were relevant in addressing IT problems in Darmajaya SISKA IIB and as a relevant framework for evaluating IT services. The following process mapping from the COBIT 5.0 framework and ITIL V3 can be seen in table 2-9 (Mapping of COBIT 5 with ITIL V3 2011. ISACA. 2012).

Table 2. Mapping COBIT 5.0 – ITIL V3 Domain DSS-01

SO – 4.1 Event Management	
DSS-01.1	Perform operational procedures
DSS-01.2	Manage outsourced IT services
DSS-01.3	Monitor IT infrastructure
DSS-01.4	Manage the environment
DSS-01.5	Manage facilities

Table 3. Mapping COBIT 5.0 – ITIL V3 Domain DSS-02

SO – 4.2 Incident Management and 4.3 Request Fulfilment	
DSS-02.1	Define incident and service request classification schemes
DSS-02.2	Record, classify and prioritise requests and incidents
DSS-02.3	Verify, approve and fulfil service requests
DSS-02.4	Investigate, diagnose andallocate incidents
DSS-02.5	Resolve and recover from incidents
DSS-02.6	Close service requests and incidents
DSS-02.7	Track status and produce reports

Table 4. Mapping COBIT 5.0 – ITIL V3 Domain DSS-03

SO – 4.4 Problem Management	
DSS-03.1	Identify and classify problems
DSS-03.2	Investigate and diagnose problems
DSS-03.3	Raise known errors
DSS-03.4	Resolve and close problems
DSS-03.5	Perform proactive problem management

Table 5. Mapping COBIT 5.0 – ITIL V3 Domain DSS-04

SD – 4.6 Service Continuity Management	
DSS-04.1	Define the business continuity policy, objectives and scope.
DSS-04.2	Maintain a continuity strategy
DSS-04.3	Develop and implement a business continuity response

DSS-04.4	Exercise, test and review
DSS-04.5	Review, maintain and improve the continuity plan
DSS-04.6	Conduct continuity plan training
DSS-04.7	Manage backup arrangements
DSS-04.8	Conduct post-resumption review

Table 6. Mapping COBIT 5.0 – ITIL V3 Domain DSS-05

SD – 4.7 Information Security Management	
DSS-05.1	Protect against malware
DSS-05.2	Manage network and connectivity security
DSS-05.3	Manage endpoint security
DSS-05.4	Manage user identity and logical access
DSS-05.5	Manage physical access to IT assets
DSS-05.6	Manage sensitive documents and output devices
DSS-05.7	Monitor the infrastructure for security-related events

Table 7. Mapping COBIT 5.0 – ITIL V3 Domain DSS-06

SO – 4.5 Assess Management	
DSS-06.1	Align control activities embedded in business processes with enterprise objectives
DSS-06.2	Control the processing of information
DSS-06.3	Manage roles, responsibilities, access privileges and levels of authority
DSS-06.4	Manage errors and exceptions
DSS-06.5	Ensure traceability of information events and accountabilities
DSS-06.6	Secure information assets

Table 8. Mapping COBIT 5.0 – ITIL V3 Domain MEA-01

CSI – 5.4 Service Measurement	
MEA-01.1	Establish a monitoring approach
MEA-01.2	Set performance and conformance targets
MEA-01.3	Collect and process performance and conformance data
MEA-01.4	Analyse and report performance
MEA-01.5	Ensure the implementation of corrective actions

Table 9. Mapping COBIT 5.0 – ITIL V3 Domain APO-12; APO-13

SD – 4.7 Information Security Management	
APO-12.1	Collect data
APO-12.2	Analyse risk
APO-12.3	Maintain a risk profile
APO-12.4	Articulate risk
APO-12.5	Define a risk management action portfolio
APO-12.6	Respond to risk
APO-13.1	Establish and maintain an ISMS
APO-13.2	Define and manage an information security risk treatment plan
APO-13.3	Monitor and review the ISMS

RESULT AND DICUSSION

Before calculating the maturity level, validity and reliability were tested using SPSS version 20.0. For the result significant or insignificant was conducted by comparing r_{count} values with r_{table} values with alpha **0,05**. From the results of the analysis carried out, obtained a minimum value of **0,481** to a maximum of **0,842**. This value was greater than r_{table}. That is explained that the condition was if r_{count} **>** $r_{table,}$ then the instrument was declared **Valid**. Whereas for testing reliability with Alpha Cronbach was carried out to build the construct of reliability of the study. The alpha coefficient ranged from a minimum of **0,714** to a maximum of **0,850** which indicated that the item question (instrument) was able to be **Reliable** (Aziz, R. A., & Morita, H. 2016).

Based on the recapitulation of the answers from the respondents, the highest capability score was found in the **APO-13** domain, namely the process of managing device security from the small/large risks that occur. The value in this domain was **2,55**. While the lowest value was found on **DSS-02** domain as the process of managing service requests and handling problems that were done for the continuity of the academic information system with a value of **2,43**. The average value of all domains was **2,48** as stated in table 10 at the Managed level.

Table 10. Capability Level of Current Conditions

Control Process of ITIL	Average	Capability
Service Operation (Event Management)	2,51	Established
Service Operation (Incident Management and Request Fulfilment)	2,43	Managed
Service Operation (Problem Management)	2,48	Managed

Service Design (Service Continuity Management)	2,46	Managed
Service Design (Information Security Management)	2,48	Managed
Service Operation (Access Management)	2,49	Managed
Continual Service Improvement (Service Measurement)	2,45	Managed
Service Design (Information Security Management)	2,50	Managed
Service Design (Information Security Management)	2,55	Established
Total Capability Level of Current Conditions	**2,48**	**Managed**

Meanwhile, the highest capability value for expected conditions was found in MEA-01, namely the existing monitoring, evaluation and SOP processes. The value obtained was **4,60**. While the lowest value was in the DSS01 domain, which was the process of managing operations from service operations to IT infrastructure. The value obtained was 4,41. The average value of all domains was **4,43** as stated in table 11 at the Predictable level.

Table 11. Capability Levels of Expected Conditions

Control Process of ITIL	Average	Capability
Service Operation (Event Management)	4,43	Predictable
Service Operation (Incident Management and Request Fulfilment)	4,43	Predictable
Service Operation (Problem Management)	4,43	Predictable
Service Design (Service Continuity Management)	4,44	Predictable
Service Design (Information Security Management)	4,46	Predictable
Service Operation (Access Management)	4,46	Predictable
Continual Service Improvement (Service Measurement)	4,44	Predictable
Service Design (Information Security Management)	4,44	Predictable
Service Design (Information Security Management)	4,38	Predictable
Total Capability Levels	**4,43**	**Predictable**

As a result of both the level capability assessment of the academic information system, a gap analysis assessment was carried out as shown in table 12. This analysis showed the gap between the current maturity level and the expected level of maturity.

Table 12. GAP Analysis

Domain		Process	Maturity Level		GAP
COBIT	ITIL		P	E	
DSS01	SO	Event Management	2.51	4.43	1.92
DSS02	SO	Incident Management & Request Fulfilment	2.43	4.43	2.00
DSS03	SO	Problem Management	2.48	4.43	1.95
DSS04	SD	Service Continuity Management	2.46	4.44	1.98
DSS05	SD	Information Security Management	2.48	4.46	1.98

DSS06	SO	Access Management	2.49	4.46	1.97
MEA-01	CSI	Service Measurement	2.45	4.44	1.99
APO-12	SD	Information Security Management	2.50	4.44	1.94
APO-13	SD	Information Security Management	2.55	4.38	1.83
Average			**1,95**		

The average of all GAP process domains is 1,95. Required adjustments to each domain process, because the value of 1,95 is the value of all the process domains, the writer will provide recommendations on each process under study so that the improvement recommendations are right on target. Different conditions of governance gap across the current process domain with expected governance.

After GAP analysis measurement, all process need to require recommendations to appropriate improvements for IT governance on COBIT 5 and ITIL V3. The measurement consists of :

1. **Critical Success Factors (CSF)** defining important things or activities that management can use to control IT processes in its organization.
2. **Key Performance Indicators (KPI)** define measures to determine the performance of IT processes carried out to achieve a predetermined goal. KPI is usually in the form of indicators of capability, implementation and capability of IT resources.
3. **Key Goal Indicators (KGI)** refers to a predetermined goal indicator that shows what must be achieved by a process. Measure-size that will give management an idea of whether existing IT processes have met the needs of existing business processes.

Based on the findings and GAP obtained, a recommendation was made to improve the ability of universities to reach the expected level of capability. Where the maturity level of the current condition was still at level 2 (Managed), the process described earlier was implemented and managed with planning and adjustment. To achieve the expected level 4 (Predictable), the process that had been applied before now operates within the limits determined to achieve the results of the process. The recommendations for governance improvements obtained from the results of the GAP analysis are Darmajaya's academic information system that needed to provide a good means of comparing optimal operating performance. It Provided the guarantees of service/security, reporting, and improved services. Perform monitoring and control of events that occured by found out the real situation. It occured in the application of information technology governance, regarded the performance and quality of the Academic Information System from the user side. This monitoring was carried out routinely in accordance with standard procedures and made reporting to management. Maintaining the quality of IT services was done by the elimination of repetitive problems / incidents, as well as providing overall quality to maintain business confidence in the IT field. Maintain user satisfaction was done by existing IT

services. Monitor and validate measurements was also done in previous business policies. It was took measurements and monitoring to identify further changes with corrective actions.

CONCLUSION

Based on the results and discussion, it was able to concluded that the Service Operation, Service Design, and Continual Service Improvement domains on the GAP was good enough as the average, with a GAP difference between the current conditions and expectations less than 2 (two). It meant that the smaller of gap analysis was in the current condition with the expected conditions, the IT governance process was getting better. In this process the gap analysis (GAP), it showed that it had been applied in the previous session within the limits specified to achieve the results of the process. For further research, it was able to be recommended to add a sub domain from COBIT 5 related to academic information system services and other process components in ITIL version 3 to improve governance success to be even better.

REFERENCE

Aziz, RZ Abdul., & Hiroshi Morita. 2016. National culture, organisational culture, total quality management implementation, and performance: an empirical investigation. International Journal of Productivity and Quality Management, 19(2), 139-159.

Britain, Great. "Cabinet Office, (2011a)."." *ITIL Service Design* (2011)

Burgoa, Mauricio Alberto Marrone. *Adoption and Benefits of Standardized IT Management Processes: IT Executives Perceptions of ITIL and COBIT*. Diss. Niedersächsische Staats-und Universitätsbibliothek Göttingen, 2011.

Cabinet Office. ITIL V3 2011. 2011. *www.cabinetoffice.gov.uk.*

COBIT Steering Committee and The ITGI. COBIT. 2003

Elvina, P. A. Evaluasi Layanan Teknologi Informasi di Kementerian Komunikasi dan Informatika Berdasarkan ITIL V3 2011 dan COBIT 5 *. Puti Adella Elvina, PPs-UI. 2013*

Gallegos F. 2014. Audit and Control of Information System. 716 p.

Lupiyoadi, Rambat, and Ridho Bramulya Ikhsan. "Praktikum Metode Riset Bisnis." *Salembaempat, Jakarta* (2015).

IT Governance Institute, *A Business Framework for the Governance and Management of Enterprise IT. COBIT 5 Framework. ISACA. 2012.*

IT Governance Institute, *Enabling Process COBIT 5 . ISACA. 2012*

IT Governance Institute, *Implementation COBIT 5 . ISACA. 2012.*

IT Governance Institute, *Mapping of COBIT 5 with ITIL V3 2011. ISACA. 2012.*

Nurlistiani, Rini. "Audit Sistem Infoemasi Menggunakan Pendekatan COBIT 5.0 dan ITIL V3 Pada Sistem Informasi Akademik (SISKA) IIB Darmajaya" (Bandar Lampung, 2018)

Wausi, Agnes, and Winnie CHERONO. "An Evaluation Framework for ICT Management Framework Selection in Kenyan Organisations." (2014).
Zhou, Chao, and Dong Zhang. "Adoption of COBIT5 and ITIL in Small and Medium Size Enterprises in China." (2014)