RISK MANAGEMENT EVALUATION IN LIBRARIES BASED ON COBIT 5

Adi Nugraha Setiadi,
Master of Electrical Engineering Student
Department of Electrical Engineering and Information Technology
Universitas Gadjah Mada
Yogyakarta, Indonesia.
E-mail: adi.cio15@mail.ugm.ac.id

Widyawan,
Department of Electrical Engineering and Information Technology
Universitas Gadjah Mada
Yogyakarta, Indonesia.
E-mail: widyawan@ugm.ac.id

Selo,
Department of Electrical Engineering and Information Technology
Universitas Gadjah Mada
Yogyakarta, Indonesia.
E-mail: selo@ugm.ac.id

ABSTRACT

Along with the increasing role of information technology (IT), the need of IT governance in organizations also increases. Therefore, an evaluation needs to be performed to discover the actual condition of IT management in the organization aforementioned. The importance of IT in an organization is to aid business activities. Universitas Ahmad Dahlan (UAD) has four campuses supported with library and therefore implements integrated libraries system that connects the library of all four campuses. However, the IT service provided for users is yet to be improved. The questions in the IT library service include policy, procedure, activities and documentation related to risk management. UAD library has to ensure that risk management available is appropriate for its necessities and business activities. UAD library also hopes that every problems meets its solution. This research aims to understand the condition of risk management applied in UAD library related to IT using COBIT 5 framework in process domain EDM03 (Ensure Risk Optimisation). In order to obtain data accuracy, raw data was collected through questionnaire, direct observation and interview with the people involved in the field. Results show that EDM03 was at level 2. This research also provides process practice recommendation and its activities that aid UAD library in its IT service.

Key Words: *risk management, capability level, IT governance, COBIT 5, EDM03*
JEL Classification: *O32*

1. INTRODUCTION

IT governance is highly needed as a result of the rapid development of technology. This factor encourages many organizations to utilize IT in its own governance. The increasing role of IT is proportional to the increasing investment made by the organization in the IT field. Therefore, a fine IT governance that is suitable for the organization's necessities is urgently needed (Diharja, 2013).

Utilization of IT in education system is required to support its productivity, effectivity, and efficiency. University, as one of the institutions involved in higher educational system, experiences the high social demand following globalization. One of the demands proposed to universities is IT development (Effendi, 2008).

Risks involved in IT development in university are damage, loss, or dysfunction of IT infrastructure. In spite of its applicable features, IT system frequently causes problems and risks to the university (Innike et al., 2014). The risks of implementing IT system are latent, therefore, detection and understanding of the problems by the university becomes a necessity because damage and loss, either financial or operational, can be anticipated (ISACA, 2013). A fine risk management will provide institutional competitive advantage. The purpose of risk management is to ensure that every possible risk can be identified and managed so that business activities can run adequately (Indah et al., 2014).

Risk management in libraries is a comprehensive study which needs analysis of potential threats. Those threats may become risks if not properly treated by the parties involved (Ali, 2016). UAD libraries need to take accurate actions to address those risks.

Ahmad Dahlan University currently has been utilizing technology quite well. UAD maximizes the use of technology for planning, management, operations, and evaluation. With the good governance and planning, technology implementation will run efficiently and effectively. The information system at UAD will continue to be developed in accordance with the needs and existing business processes.

In UAD library there are two information system, i.e. digital library and SIMPus UAD. Digital library ia a service that can be accessed through www.digilib.uad.ac.id. Library member are able to download the collection on this website. SIMPus UAD is a dedicated service for UAD librarian. This information system is used to manage the book collection database, manage visitor data, manage library members, manage borrowing, and create various types of reports that can be useful as an evaluation material.

After observation on risk management, some analysis of current condition is as follows:

1. There has been no research on the application of IT, especially in the UAD library, with the aim to be in line with business processes.
2. The absence of SOPs and documentation on handling when there is a risk. Until now the process of handling risk is only based on experience and habits.
3. The making of information system in UAD library is developed by programmer from BISKOM UAD, so that when problems occur on the system can be handled immediately.

One of the framework that can be applied to evaluate risk management related to IT in UAD libraries is COBIT 5, process domain EDM03 in particular (Ensure Risk Optimisation). Process domain EDM03 was chosen in this research because this domain discusses specific details in risk identification related to IT. This research conducted a measurement of the UAD libraries readiness in risk management in term of IT service.

2. LITERATURE REVIEW

2.1 PREVIOUS RESEARCHES

Previous researches relevant to this research are mentioned below:

1) Research done by Amirul Iqbal titled "Evaluasi Business Continuity Plan Menggunakan COBIT 5 (Studi Kasus: DSSDI Universitas Gadjah Mada). This research employs COBIT 5 in order to identify and evaluate Business Continuity Plan (BCP) in Direktorat Sistem dan Sumber Daya Informasi (DSSDI) UGM. The author compared some of the IT governance frameworks available and chose COBIT 5 as the framework employed in the research. Consideration in regards to COBIT 5 includes utilization rate, completeness, IT governance measurement, best practice support, simplicity in utilization, manual, framework creation availability, and document template. Results showed that IT governance, particularly in BCP has been implemented. However, the implementation needs to be improved because most of the capability processes are at level 1 (performed) and 2 (managed).

2) Research done by Khairul Sani titled "Evaluasi Governance Pada Layanan Akademik Perguruan Tinggi Menggunakan COBIT 5 (Studi Kasus BISKOM UAD)". This research focused on capability measurement of IT governance employed by BISKOM UAD. Generally, this research resulted in two types of recommendations. First recommendation is for the IT governance to be consistent with the strategy and business processes in UAD, particularly improving student academic service. Second recommendation is for the change of SOP with the involvement of IT consistent with the business processes in UAD.

2.2 RISK MANAGEMENT

Risk management is a set of complete policy and procedure owned by an organization to manage, monitor, and control the exposure of risks (Setia, 2015). Risk management functions to overcome risks which comprises management process, measurement, and risk assessment. The main purposes of risk management is to reduce negative impact and to avoid risks, to accommodate some or all of the risk consequences, or to divert risks to other parties.

2.3 COBIT 5

COBIT (Control Objective for Information and Related Technology) is a framework and IT governance standard. It is also a set of measurement that is generally acknowledged for management processes and IT governance. This framework was first arranged by Information Systems and Audit and Control Association (ISACA) and now is managed by IT Governance Institute (ITGI). In 2012, ITGI issued IT governance COBIT 5. COBIT 5 is the newest version of COBIT framework which provides end-to-end business description from IT governance. COBIT 5 was developed from COBIT 4, integrated with Val IT 2 and Risk IT from ISACA, BMIS, ITIL, and relevant standard from ISO (ISACA, 2012).

ISACA (2012) explains that there are 7 phases which have to be performed according to COBIT 5 implementation life cycle:

1. Initiate Program, identification process which triggers changes such as trend condition, performance, software implementation, current issues and organization's objectives that encourage changes.

2. Define Problems and Opportunities, an alignment process between the objectives of IT application and risk, and or organization's strategies.
3. Define Road Map, a target determination program to enhance improvement and followed by gap analysis to determine potential solutions.
4. Plan Program, plans feasible and practical solutions by defining projects supported by justifiable business cases and developing a change plan for implementation.
5. Execute Plan, provides for the implementation of the proposed solutions into day-to-day practices and the establishment of measures and monitoring systems to ensure that business alignment is achieved and performance can be measured.
6. Realized Benefits, focuses on sustainable transition of the improved governance and management practices into normal business operations and monitoring achievement of the improvements using the performance metrics and expected benefits.
7. Review Effectiveness, reviews the overall success of the initiative, identifies further governance or management requirements and reinforces the need for continual improvement. It also prioritizes further opportunities to improve COBIT.

2.4 MANAGEMENT RISK FOCUS DOMAIN

According to COBIT 5 framework, there are 2 processes interrelated to risk management identification and communication. One of the processes is EDM03 whose objective is to ensure that the risk level and tolerance exposed to the organization is acceptable, understood, articulated and communicated. Another objective of EDM03 is to ensure that IT-related risks are identified and monitored. EDM03 process is classified into three attributes:

1. EDM03.01 Evaluate Risk Management
2. EDM03.02 Direct Risk Management
3. EDM03.03 Monitor Risk Management

3. METHODOLOGY

This research was conducted in accordance with the Figure 1 below.

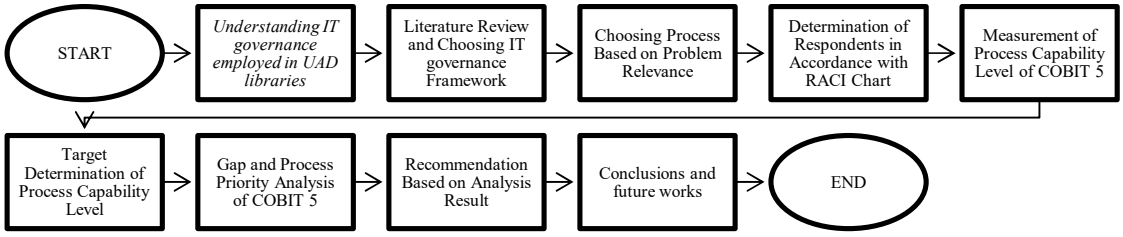

Figure 1 Research methodology

The measures taken in this research are mentioned below:

1. Understanding IT governance employed in UAD libraries

This measure was taken by conducting interview with the Head of the Library of UAD to determine the scope of risk management evaluation and current IT governance employed by UAD library.

2. Literature Review and Choosing IT governance Framework

This measure was performed by reading and studying papers related to this research. The objective of this measure was to seek for references and also understanding the stages in risk management evaluation and implementation of COBIT 5.

3. Choosing Process Based on Problem Relevance

General description of organization, vision and mission, general description of IT systems that are employed in the processes involved in COBIT 5. Based on the discussions with the UAD library, a decision was made to conduct an evaluation based on Enterprise Goals COBIT 5 relating to the continuity and availability of the organization's business services. From the mapping using the Goals Cascade in COBIT 5, we obtained some COBIT 5 process that suits the needs of the UAD library, as can be seen at Table I below.

Table I Mapping of Enterprise Goals, IT-related Goals and relevant primary processes

Enterprise Goals	**IT-related Goals**	**COBIT 5 Process**
07. Business service continuity and availability	04. Managed IT-related business risk	EDM03 Ensure Risk Optimisation
		APO10 Manage Suppliers
		APO12 Manage Risk
		APO13 Manage Security
		BAI01 Manage Programmes and Projects
		BAI06 Manage Changes
		DSS01 Manage Operations
		DSS02 Manage Service Requests and Incidents
		DSS03 Manage Problems
		DSS04 Manage Continuity
		DSS05 Manage Security Services
		DSS06 Manage Business Process Controls
		MEA01 Monitor, Evaluate and Assess Performance and Conformance
		MEA02 Monitor, Evaluate and Assess the System of Internal Control
		MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

4. Determination of Respondents in Accordance with RACI Chart

This stage consist of respondent determination based on role and authority in RACI Chart. A RACI chart is a matrix of all the activities or decision-making authorities undertaken in an organisation set against all the people or roles. Based on this, we can determine the proper

respondent. Total respondents in this study are 6 people, consisting of the head librarian, technical coordinator of the library, and other employees.

5. Measurement of Process Capability Level

   Assessment of process capability level using COBIT 5, EDM03 process domain in particular. Capability level in COBIT 5 are categorized into six levels: Level 0 (Incomplete), Level 1 (Performed), Level 2 (Managed), Level 3 (Established), Level 4 (Predictable), and Level 5 (Optimizing). Assessment starts from level 0, in accordance with the criteria of Process Assessment (PA) in COBIT 5. If assessment level 1 gets percentage 85% (Fully Achieved), then the assessment will continue to the next level.

6. Target Determination of Process Capability Level

   This stage consist of target determination of process capability level that desired to be accomplished. Interview was used as a method to obtain data from the people in the institution involved in the IT governance. Results from this stage is target capability level.

7. Gap and Process Priority Analysis of COBIT 5

   Analysis of gap and process priority was conducted at this stage.

8. Recommendation Based on Analysis Result

   By knowing the capability level from result of identification and data analysis, we will be able to know the activity that required but not yet fulfilled by organization. Therefore, this recommendations is based on best practice according to COBIT 5.

9. Conclusions and Future Works

   After analysis, we will get a conclusion that should be in align with the purpose of this research. The conclusions to be generated are the level of capability and activity recommendations. Future works are more directed to the next researcher to consider the scope of the study.

4. RESULTS AND DISCUSSION

In this study we used questionnaire method based on COBIT 5 Process Assessment Model by following the guideline at activity to determine the capability level. The survey was used to determine the level of risk management capability level with the form of questions.

Based on the results of the questionnaires that we distributed, we can calculate the level of capability for each process based on governance/management practice and the resulting output.

The EDM03 process has a focus on risk management and risk tolerance associated with information systems services in organizations. This information system deals with the business processes that run in the library. A summary of achievement of capability level for EDM03 process can be seen in Table II.

At first we calculate the level of capability level 1, it was found that EDM03 gets score 88,9% or Fully Achieved. Therefore, the assessment proceeds to level 2 and EDM03 gets score 84,5% at PA 2.1 and 58% at PA 2.2. Based on those score, assessment does not advance to level 3 because PA 21 and PA 2.2 did not fullfill the criteria.

Table II Summary of EDM03 process capability assessment

Objectives	Ensure that IT risk in the organization does not exceed the company's capability and tolerance to accept risks, identify and manage the impact of IT risks on corporate values, and reduce the occurrence of failures									
EDM03 Ensure Risk Optimisation	**Level 0**	**Level 1**	**Level 2**		**Level 3**		**Level 4**		**Level 5**	
		PA 1.1	**PA 2.1**	**PA 2.2**	**PA 3.1**	**PA 3.2**	**PA 4.1**	**PA 4.2**	**PA 5.1**	**PA 5.2**
Percentage		88,9%	84.5%	58%						
Criteria		*Fully Achieved*	*Fully Achieved*	*Largely Achieved*						

Table III Detailed assessment of EDM03 prcess Level 1

EDM03			
Governance Practice	***Outputs***	***Exist***	***Score***
EDM03.01 Evaluate risk management	Risk appetite guidance	Y	100%
	Approved risk tolerance levels	Y	
	Evaluation of risk management activities	Y	
EDM03.02 Direct risk management	Risk management policies	Y	66,6%
	Key objectives to be monitored for risk management	N	
	Approved process for measuring risk management	Y	
EDM03.03 Monitor risk management	Remedial actions to address risk management deviations	Y	100%
	Risk management issues for the board	Y	
Average			88,9%

Based on the results of the assessment, it was found that EDM03 process in UAD library has reached level 2 with Fully Achieved (F) in Process Assessment (PA) 2.1 Performance Management and Largely Achieved (L) in PA 2.2 Work Product Management.

Detailed measurements of the level capability level of the Level 1 EDM03 process can be seen in Table II. Then the details of the level capability level of EDM03 process level 2 - PA 2.1 Performance Management and PA 2.2 Work Product Management can be seen in Table IV and Table V.

Table IV Detailed assessment of EDM03 process Level 2 – PA 2.1 Performance Management

2.1 Performance Management		
Generic Practices	***Exist***	***Score***
GP 2.1.1 Identify the objectives	Y	75%

GP 2.1.2 Plan and monitor the performance	Y	83%
GP 2.1.3 Adjust the performance	Y	100%
GP 2.1.4 Define responsibilities and authorities	Y	66%
GP 2.1.5 Identify and make available	Y	83%
GP 2.1.6 Manage the interfaces	Y	100%
Rata-rata		**84.5%**

Table V Detailed assessment of EDM03 process Level 2 – PA 2.2 Work Product Management

2.2 Work Product Management		
Generic Practices	***Exist***	***Score***
GP 2.2.1 Define the requirements for the work products	Y	66%
GP 2.2.2 Define the requirements for documentation and control	Y	66%
GP 2.2.3 Identify, document and control	Y	50%
GP 2.2.4 Review and adjust work products	Y	50%
Rata-rata		**58%**

Based on the results of the assessment, it was found that EDM03 process in UAD library has reached level 2 with Fully Achieved (F) in Process Assessment (PA) 2.1 Performance Management and Largely Achieved (L) in PA 2.2 Work Product Management.

Detailed measurements of the level capability level of the Level 1 EDM03 process can be seen in Table II. Then the details of the level capability level of EDM03 process level 2 - PA 2.1 Performance Management and PA 2.2 Work Product Management can be seen in Table III and Table IV.

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 CONCLUSIONS

In this paper, we have evaluated the risk management in the library of Universitas Ahmad Dahlan using the COBIT 5 frameworks, it can be summarize as follows:

1. In this risk management evaluation using COBIT 5 framework process, especially EDM03 (Ensure risk optimization), the capability process of this domain is level 2 (managed process), which means identification, planning, and communication activity about risk management has been managed and its work has been determined, monitored, and managed appropriately.

2. The gap between the current level of capability and the target level to be achieved is 1 level, from level 2 to level 3.

3. A recommendation has been made based on COBIT 5 framework with a summary:

    a. there are 7 activity and 6 output to comply with Process Assessment 2.1 Performance Management

    b. there are 4 activity and 4 output to comply with Process Assessment 2.2 Work Product Management

5.2 RECOMMENDATION FOR PROCESS EDM03 PA 2.1

To reach capability level 3 from level 2 on EDM03 process, UAD library should reach 85-100% percentage point on generic practices (GPs) and generic work products (GWPs). In the Process Assessment 2.1 Performance Management UAD library is recommended to perform generic practices as follows:

1. Identify the objective when making risk appetite guidance. The objective should be well understood, defined, and communicated. The identification of this objectives is suggested to include the evidence of targets such as milestones, required activities, and schedules.

2. Knows clearly when communicating information activities related to risks IT begin and when the activity is considered complete.

3. Plan, monitor, and record the performance of risk profiles. It aims to see how far the performance of risk management in achieving the purpose of the library.

4. Adjust the performance of the process of identification and communicating information about IT risks. When the activity is not in achieved with the plan, it is necessary to identify the problem and make adjustment of plans and schedules as appropriate.

5. Define responsibilities and authorities for performing the risk identification. The key responsibilities and authorities for performing the key activities of the process are defined, assigned and communicated. The need for process performance experience, knowledge and skills is defined.

6. Identify and make available resources to perform the risk identification according to plan. Resources and information necessary for performing the key activities of the process are identified, made available, allocated and used

7. Manage the interfaces between involved parties for risk identification. The individuals and groups involved with the risk identification are identified, responsibilities are defined and effective communication mechanisms are in place.

Besides doing the generic practices, UAD libraries must have generic work products:

1. Documentation about risk definition and communication process risks that occur.

2. Details of the risk identification performance.

3. Record risk identification and communication process performance

4. Details of action taken when identification risk is not achieved.

5. Documentation about risk identification should provide details of the process owner and who is responsible, accountable, consulted and/or informed (RACI).

6. Documentation should provide details of the process communication plan.

5.3 RECOMMENDATION FOR PROCESS EDM03 PA 2.2

In the Process Assessment 2.2 Work Product Management UAD library is recommended to perform generic practices as follows:

1. Define the requirement and criteria for the risk identification process, and then these requirement are reviewed and approved.

2. Define the requirement for documentation and control of the risk identification process. These needs include identification, approval from relevant parties, and trace ability of the process.

3. Identifying, documenting, and controlling the record of reviews that has been made on the risk identification and risk communication process. These activities are need to be done including when problem occur and has been resolved, also the record must be exist.

4. Review and adjust risk profile to meet the defined requirements. Risk profile are subject to review against requirements in accordance with planned arrangements and any issues arising are resolved.

Besides doing the generic practices, UAD libraries must have generic work products:

1. Documentation that provide details of identification and communication about risk management, including the organizational structure and level of satisfaction that is expected.

2. Documentation of internal control matrix that identifies the risk that exist within the business process.

3. Quality plan for the identification and communication about risk management and should present the outline procedure. This plan is supposed to help version controls and change controls that applied to risk appetite guidance.

4. Quality records of risk identification and communication should provide a trace of an audit review undertaken.

References

A. Iqbal, “Evaluasi Business Continuity Plan Menggunakan COBIT 5 (Studi Kasus: DSSDI Universitas Gadjah Mada)”, Universitas Gadjah Mada, Yogyakarta, 2016.

D. Innike, B. C. Hidayanto and H. M. Astuti, “Penilaian Risiko Keamanan Informasi Menggunakan Metode Failure Mode and Effect Analysis di Divisi TI Bank XYZ Surabaya,” Seminar Nasional Sistem Informasi Indonesia, Surabaya, 2014.

D. R. Indah, Harlili and A. Firdaus, “Risk Management for Enterprise Resource Planning Post Implementation Using COBIT 5 for Risk,” in International Conference on Computer Science and Engineering, Bandung, 2014.

Diharja, Anas A., “Audit Tata Kelola Sistem Kepegawaian Dinas Tenaga Kerja dan Transmigrasi Provinsi Sumatera Selatan dengan Kerangka Kerja COBIT Versi 5”. Universitas Bina Darma. Palembang, 2013.

Effendi, Dian., “Perancangan IT Governance Pada Layanan Akademik di UNIKOM (Universitas Komputer Indonesia) Menggunakan COBIT (Control Objectives For Information and Related Technology) Versi 4.0.” Institut Teknologi Bandung, Bandung, 2008

Glasgow Caledonian University, “Risk Management Strategy,” Risk Management Strategy, Juni 2015.

I. Ali, “Pengamanan Koleksi Digital dengan Pendekatan Manajemen Risiko”, Media Pustakawan, vol 23, no 2. 2016

ISACA, COBIT 5. Rolling Meadows, IL, USA: ISACA, 2012

ISACA, COBIT 5 for Risk, Illionis: ISACA, 2013

K. Sani, “Evaluasi IT Governance pada Layanan Akademik Perguruan Tinggi Menggunakan COBIT 5 (Studi Kasus BISKOM UAD),” Universitas Gadjah Mada, Yogyakarta, 2017.

M. Setia, “Manajemen Risiko”, Cetakan ke-1, Bandung: Pustaka Setia. 2015