Risk Management Evaluation in Hospital Management Information Systems Using Framework COBIT 2019 - Case Study: Ernaldi Bahar South Sumatera Hospital

Hilditia Cici Triska Amirta [a,1,*], Muhammad Ihsan Jambak [a,2], Pacu Putra Suarli [a,3], Yadi Utama [a,4], Ari Wedhasmara [a,5], Putri Eka Sevtiyuni [a,6]

[a] Faculty of Computer Science, Universitsa Sriwijaya, Palembang, Indonesia
[1] hilditiacici66@gmail.com*; [2] jambak@unsri.ac.id; [3] pacuputra@unsri.ac.id*; [4] yadiutama@unsri.ac.id;
[5] a_wedhasmara@unsri.ac.id; [6] putrieka@unsri.ac.id

ARTICLE INFO

ABSTRACT

Hospital Management Information System (SIMRS) is a system to assist service performance, reporting and data retrieval at hospitals that have been required by the government to be implemented in all hospitals in Indonesia. The existence of SIMRS is certainly an inseparable part of the service process and hospital data management, but it can also cause various IT risks to arise. Therefore, a good risk management is needed to minimize any possible IT risks that have not or have occurred. The performance of an IT risk management can be indicated from its capability levels. This study aims to determine how high the capability levels and the gap value from each process of the IT risk management at Ernaldi Bahar Hospital. The framework used as a reference in the assessment of the risk management process is COBIT 2019 which has 3 stages, namely the mapping process, capability level assessment, and conclusions. This study resulted in the value of capabilities in each process in IT risk management, the gap value, and recommendations for improvement that can be applied to SIMRS Ernaldi Bahar. The results of the measurement of the IT risk management capability of SIMRS Ernaldi Bahar in the EDM03 and DSS03 processes are at level 3, while the APO12 and DSS05 processes are at level 1. The gap values for the EDM03 and DSS03 processes is 1 level, while the gap values for the APO12 and DSS05 processes are 3 levels. Process improvement recommendations refer to COBIT 2019 best practices.

1. Introduction

With the development of the world of information technology, the use of information systems has become an obligation for companies to be able to compete. Simultaneously, new threats related to information technology emerged. Companies must recognize threats or risks to be able to deal with them with the right method. So we need an appropriate standard to analyze in order to minimize the risks that arise.

COBIT (Control Objective of Information and Related Technology) is a framework for governance and management of organizational information and technology. Enterprise IT refers to all information processing and technology that an organization implements to achieve its goals, wherever this occurs within the organization. In another sense, IT organizations are not limited to just the IT department of the organization [1].

According to [2], in addition to governance and the main purpose of management objectives in general, the new, flexible and open COBIT architecture helps to create and integrate more detailed guidelines, using the governance and management objective structure as described in the COBIT 2019 Governance and Management Objectives publication.

Knowing from the Head of Information and Communication Technology Installation at Erba (Ernaldi Bahar) Hospital that there has never been an evaluation of IT risk management in the company, creates a new urgency to immediately carry out these activities so that SIMRS can continue to be developed and improved.

A good SIMRS is an information system which processes run effectively and efficiently, especially in managing the company's IT risks. To find out whether a company's processes have been carried out properly, it is necessary to carry out capability level measurement activities. Capability levels are a measure of how well a process being implemented. The importance of knowing the capability levels of a company can help determine whether the company has reached the expected level or whether there is still a large gap between the expected level and actual achievement [3]. Thus, the objectives of this study are evaluate the IT risk management capabilities in SIMRS Erba using framework COBIT 2019 and discover the gap between the expected level and actual achievement.

2. Literature Study

This section will discuss the basic theory used in research to evaluate the capability levels of IT Risk Management in SIMRS Erba and discover the gap on each process as well as a review of previous literature relevant to capability levels measurement using framework COBIT 2019.

1. COBIT 2019

COBIT framework draws a clear line between governance and management. The two disciplines cover different activities, require different organizational structures and serve different purposes. The board and executive management are usually responsible for the governance process, whereas the management process is the domain of senior and middle management [4].

COBIT 2019 is based on COBIT 5 and other authoritative sources. COBIT 2019 builds on previous versions of COBIT in the following areas:

1. Flexibility and openness

2. Currency and relevance

3. Prescriptive application

4. Performance management of IT

2. Capability Levels

According to [5] COBIT 2019 supports process capability scenarios based on Capability Maturity Model Integration (CMMI). The processes in each governance and management goal can operate at various capability levels, ranging from 0 to 5. Capability level is a measure of how well a process is implemented and performed.

[5] explains the enterprise's logic for adjusting target capability levels, as follows:

Given the high importance of a number of processes, the target capability level has been set at a higher value (3 or 4). The logic applied by the enterprise was that:

- Any governance/management objective that scored 75 or higher—meaning that its importance was at least 75% higher compared to a benchmark situation—would require a capability level 4.

- Any governance/management objective that scored 50 or higher would require a capability level 3. Any governance/management objective that scored 25 or higher would require a capability level 2.

- It is reasonable to consider that the remaining processes should reach capability level 1.

[6] Activities of the processes can be rated according to a simple binary pass/fail rating, or in a more detailed—and fully differentiated—way, using achievement ratings similar to those defined in International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standard ISO/IEC 33004, as follows:

- Fully (F)—The capability level is achieved for more than 85 percent.
- Largely (L)—The capability level is achieved between 50 percent and 85 percent.
- Partially (P)—The capability level is achieved between 15 percent and 50 percent.
- Not (N)—The capability level is achieved less than 15 percent.

3. Gap Analysis

Capability expectation analysis explains the level to be achieved from governance and management objectives. Gap analysis is derived from the capability expectation level value reduced by the current capability level value [7]. Gap analysis is conducted to identify gaps that arise between the actual conditions and the expected conditions.

3. Methodology

a. Research Unit

In making this research the authors conducted research at the Ernaldi Bahar South Sumatera Hospital, located on Jalan Gubernur H. Muhammad Ali Amin No. 002, Palembang, South Sumatera 30961.

b. Data

1. Data Type

The types of data used in this study are divided into 2 types; namely the type of data based on the source and the type of data based on its nature. Types of data based on sources are primary and secondary data types. Primary data is data obtained directly from the source of the object of research, while secondary data is data obtained through previous research, books, articles, and other references that are closely related to the research topic.

The type of data based on the nature used in this study is qualitative data. Qualitative data is data that does not have a definite size, this data can be in the form of sentences, pictures, videos, and sound recordings.

2. Data Source

The primary data used for this study was sourced from the Head of IT Department of Ernaldi Bahar Hospital through questionnaire and interview. While secondary data obtained from references to several journals and books that have a relationship with the topic

3. Research Stage

The following are the stages of the final project methodology based on the COBIT 2019 framework as shown in Figure 1.

Figure 1. Capability Level Measurement Stage

From the three stages above, recommendations and suggestions will be generated to prioritize governance and management objectives. However, before the research begins, it is very important to determine which unit of analysis will be carried out. For example, is the purpose of this research for the business unit, or the company as a whole. In this study, researchers have determined the unit to be studied, namely IT risk management in the company.

4. Result and Discussion

This section describes the results of the analysis of the assessment of capability levels for IT risk management in the Ernaldi Bahar Hospital Management Information System (SIMRS) of South Sumatra Province. The main objective of this study is to measure capability levels in the governance of SIMRS Erba using the COBIT 2019 framework.

a. Mapping

[8] The mapping process in COBIT 2019 is a process to determine which domains and processes will be selected for analysis. The first step is to review the enterprise's goal(s) which is then mapped using a value chain diagram as shown in Figure 2 below.
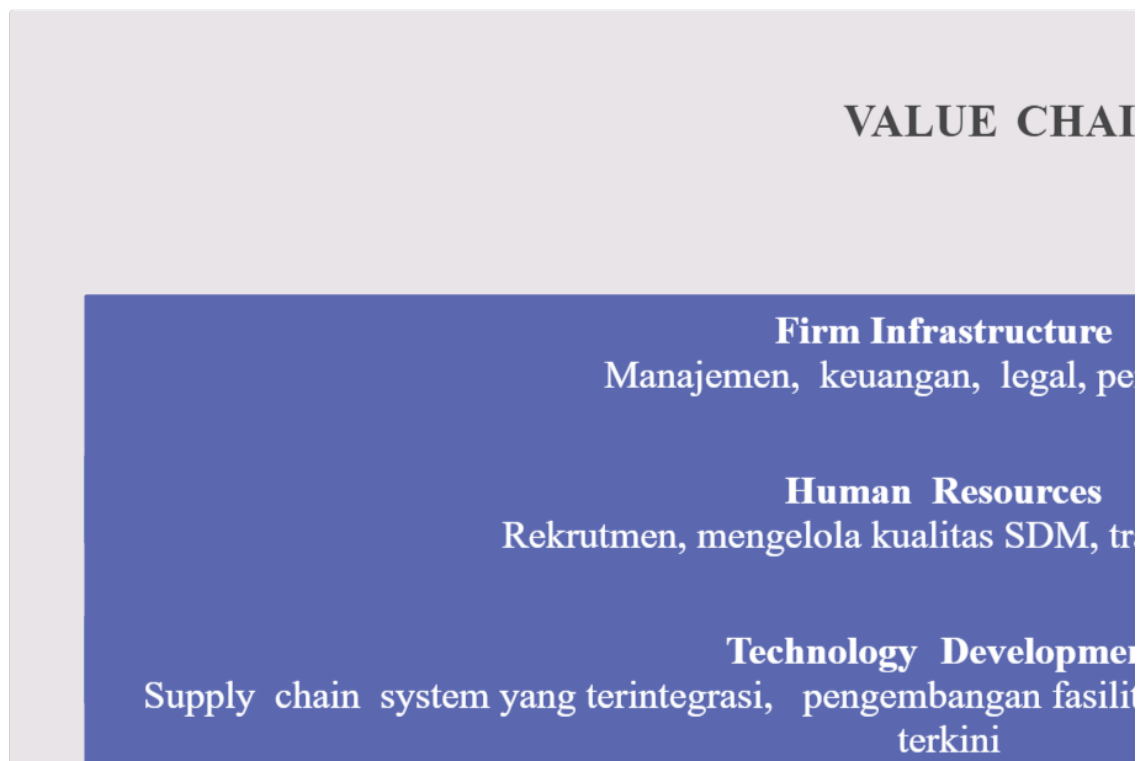

Figure 2. Value Chain Analysis

The next step is mapping the Main Tasks and Functions of the Information and Communication Technology Installation Department at Ernaldi Bahar Hospital, Sumatra Province. Based on [3] following Alignment Goals number 02 (AG02) Managed I&T-related risk, there are 3 processes that must be carried out; EDM03, APO12, and DSS05. After discussing again with Ernaldi Bahar Hospital, a secondary process was obtained, namely DSS03. The description of the process is described in Table 1 below.

Table 1. Description of COBIT 2019 Selected Process

No.	Process	Description
1.	EDM03 Ensured Risk Optimization	Ensure that the enterprise's risk tolerance and appetite is understood, communicated and informed; identify and manage risks to enterprise value related to the implementation of I&T.

2.	APO12 Managed Risk	IT-related risks are identified, assessed, and mitigated within tolerance levels that have been determined by the company's executive management on a continuous basis.
3.	DSS03 Managed Problems	Identify and classify problems and their root causes. Provide timely resolution to prevent recurring incidents, provide recommendations for improvement.
4.	DSS05 Managed Security Services	Protect enterprise information to maintain an acceptable level of information security risk by the enterprise in accordance with the security policy. Establish and maintain information security roles and access rights. Carry out security surveillance.

b. Capability Levels Measurement

Measurement of capability levels is done by distributing questionnaires. The contents of the questionnaire itself are questions that have been provided in the COBIT 2019 framework along with the level of each question. [8] Respondent identification was obtained by referring to the RACI Chart defined by COBIT 2019.

Table 2. Respondent Identification

RACI Respondent	Actual Respondent	Total
Chief Information Officer	PMKP Committee	1
Chief Technology Officer	Head of IT Department	1
Head Development	Development Staff	1
Head IT Operation	IT Staff (Programmer)	1
Head IT Administration	IT Staff (Administrasi)	1
Service Manager	Service Staff	1
Total		6

The processing of the answer data that has been obtained is carried out in the following equation.

$$Level\ achievement = \frac{total}{} \tag{1}$$

A process can be said to reach a certain level of capability and can go up to the next level if the category achieved is F (Fully achievement).

c. Discussion on the Results of the 2019 COBIT Process Capability Level Assessment

From the results of the analysis that has been carried out, it can be concluded that the process of implementing activities at Erba Hospital is still not managed properly as shown in the following Table 3.

Table 3. Capability Level Assessment Recapitulation

Objective	Capability Level Recapitulation					
Process	Lv. 0	Lv. 1	Lv. 2	Lv. 3	Lv. 4	Lv. 5
EDM03		100	88,89	100	50	
APO12		100	66,67	88,89	100	100
DSS03		100	100	100	80	100
DSS05		100	76,92	83,33	20	

Ernaldi Bahar Hospital has almost performed all activities in every process. In some processes the score at the highest level reaches 100%, but the score at the initial level has not yet touched the

minimum value that must be achieved which makes the results of their capability assessment low even though they have carried out activities to the highest capability.

d. Gap Analysis

The gap analysis of the capability level at Erba Hospital South Sumatra was obtained from the actual value of the COBIT 2019 process capability and the target capability value. The target expected by Erba Hospital based on the results of an interview with the Head of Information and Communication Technology Installation is at level 4 (Predictable). The following is a table and graph of the gap value.

Table 4. Gap Value

COBIT 2019 Processes	Actual (X)	Target (Y)	Gap (Y-X)
EDM03 Ensured Risk Optimization	3	4	1
APO12 Managed Risk	1	4	3
DSS03 Managed Problems	3	4	1
DSS05 Managed Security Services	1	4	3
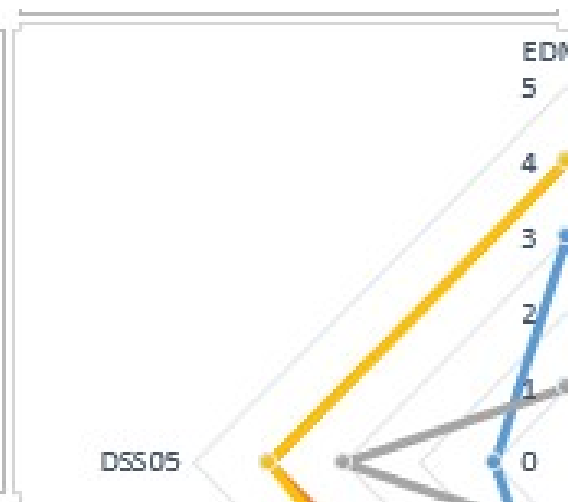
Figure 3. Gap Value Chart

5. Conclusion

Based on the results of this research regarding the evaluation of capability levels for risk management that has been carried out at SIMRS Erba using the COBIT 2019 framework, it is known that Erba Hospital has implemented several activities from all levels for each process studied but not all of them are in the Fully Achieved category, so it can be concluded that :

1. IT risk management governance at SIMRS Erba is not well structured so that when its capabilities are measured using a specific framework such as COBIT 2019 it produces relatively low scores.

2. Capability Levels for IT risk management SIMRS Erba in the EDM03 and DSS03 processes are at level 3, while the APO12 and DSS05 processes are at level 1.

3. The gap in the EDM03 and DSS03 process capability levels is 1 level between the target and actual achievements, while the gap in APO12 and DSS05 processes is 3 levels each.

Amirta, H.C.T et.al (Risk Management Evaluation…..)

References

[1] M. Adhisyanda Aditya, R. Dicky Mulyana, A. Mulyawan, S. LIKMI Bandung, and S. Mardira Indonesia, "PERBANDINGAN COBIT 2019 DAN ITIL V4 SEBAGAI PANDUAN TATA KELOLA DAN MANAGEMENT IT," *J. Comput. Bisnis*, vol. 13, no. 2, pp. 100–105, 2019.

[2] D. Steuperaert, "Cobit 2019: a Significant Update," *Edpacs*, vol. 59, no. 1, pp. 14–18, 2019, doi: 10.1080/07366981.2019.1578474.

[3] ISACA, *COBIT 2019 Governance and Management Objectives (ISACA)*. 2019.

[4] ISACA, *COBIT 2019 Framework Introduction and methodology*. 2019. [Online]. Available: https://community.mis.temple.edu/mis5203sec001sp2019/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

[5] ISACA, *Designing an Information and Technology Governance Solution*. 2018.

[6] ISACA, "Defining Target Capability Levels in COBIT 2019: A Proposal for Refinement," 2019, [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2019/defining-target-capability-levels-in-cobit-2019-a-proposal-for-refinement

[7] E. Nachrowi, Yani Nurhadryani, and Heru Sukoco, "Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, pp. 764–774, 2020, doi: 10.29207/resti.v4i4.2265.

[8] V. Kasma Septiyana, S. Sutikno, and K. Surendro, "Design of e-Government Security Governance System Using COBIT 2019," *IEEE Xplore*, vol. 2019, pp. 1–6, 2020, [Online]. Available: https://ieeexplore.ieee.org/document/8969808