Risk Assessment Analysis of Medical Information System Services using COBIT 5 Framework

Odjie Dwianto
Department of Information SystemUniversitas Ahmad Dahlan Yogyakarta of Indonesia

Imam Riadi
Department of Information System Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

PT. MandatechMataram Mukti is providers for application social service in theYogyakarta area. Risk management requires risk assessment analysis of ongoing business processes for business processes to run well. COBIT 5 is here to answer the challenges of this modern era, especially risk management. The need for a risk assessment analysis to measure the extent to which elements apply risk management to the enterprise. The purpose of this study is to determine the current Capability Level value (capability level) and expected value, calculate gap value, and provide recommendations following APO12 (Manage Risk) and EDM03 (Ensure Risk Optimization) domains. Risk management assessment analysis in this study uses the COBIT 5 framework using the APO12 (Manage Risk) and EDM03 (Ensure Risk Optimization) process domains including the stages of data collection, risk analysis, risk profile, risk articulation, risk tolerance values, ways to respond to risks, evaluate risk management and direct risk management. The research stages carried out have three stages of research analysis: determining the current capability, expected levels, conducting gap analysis, and providing recommendations and suggestions for improvement. Based on the results of calculations carried out in this study, the level of domain APO12 capabilities currently (Manage Risk) gets a score of 1.83 is at level 1 (Performed Process) meaning that the IT process in Medical Information System Services has carried out management and governance efforts properly. The APO12 (Manage Risk) domains gets a gap value of 1. Capability Level in EDM03(Ensuring Risk Optimization) domains gets a capability value of 1.62 (PerfomedProcess) for expected capability value at domain capability level APO12 and EDM03 is at level 2, for the result of calculation of gap value get a gap value of 1 in the EDM03(Ensuring Risk Optimization) domains, recommendations produced in this study are the following expected company objectives.

Keywords

Risk Management, Information Systems, COBIT 5,RACIChart,ProcessCapabilityLevel.

1. INTRODUCTION

Information Technology (IT) is useful in helping to complete work effectively and efficiently if managed properly. Poor management can increase negative risks for the organization in question. This is an impetus for services to best utilize IT in managing its services,social service companies are those who feel social demands to help and serve the community, especially during the pandemic.Thisprovidesinformation and there are three companies focus on, namely first, assisting and supporting in managing information technology operations, second, ensure that IT performance is good,third, streamline daily routines or managers can focus on the main activities of the business. Based on the company profile above, Information Technology supports the course of business in the company, so that risks to IT can occur at any time. Therefore, to overcome the above problems, in this study the author carried out risk management of information technology using the COBIT 5 framework. Then in this study, the author conducted an analysis of the services. The service has carried out risk management in its work culture but will be adjusted to the COBIT 5 standard in its application, by carrying out a capability value to risk at this time. The assessment consists of several stages which include analysis of capability level, gap, and risk assessment. The assessment stage will produce recommendations for mitigation measures that can be used by the service for technology development so that it strongly supports governance and minimizes the risk of information technology service systems.

2. STUDY LITERATURE

2.1 DefinitionRisk

A risk is an adverse event or other definitions; the risk is the possibility of an outcome that does not match expectations. Risk arises due to uncertain conditions [1], risk is an event that occurs in a company that affects the achievement of company goals. Risk management is the ability to deal with risks with a good effect in helping to realize the goals of a company[2].

2.2 IT Risk Management

Risk is a set of procedures and methodologies used to identify measure, monitor, and control risks arising from a bank's business activities. This is related to the general definition of risk, namely in every business/activity there is always the possibility of not achieving a goal or there is always uncertainty over every decision that has been taken. In some situations, this risk can destroy the organization. Therefore, it is important to manage risks. Risk management aims to manage these risks so that can get the most optimal results. The main objective of risk management is to ensure that all risks and business policies can be applied consistently [3].

2.3 Definition of IT Risk Management

IT Risk Management is a combination of a process used to identify, review,risk is a comprehensive risk management system that an organization faces for the progress of the enterprise [4].

2.4 COBIT 5

COBIT 5 is the framework for the latest generation of ISACA guidance that addresses IT governance and management.COBIT 5 provides a framework that helps companies achieve their goals with information technology governance and managementso that the company can finally achieve its vision and mission.This, companies can create optimal value from information technology by maintaining a balance between realizing benefits, optimizing the level of risk, and using resources. COBIT 5 enables information technology to be holistically organized and managed for the entire company and provides a clear picture of stakeholder engagement in governance [5].

2.4.1 COBIT 5 Basic Principles

COBIT 5 framework consists of 5 (five) main principles and is equipped with 7 (seven) enablers. COBIT 5 adapts 5 (five) principles that seem to companies can create a successful governance and management framework with a holistic approach of 7 (seven) enablers provided to optimize technology and information while providing benefits to stakeholders [6].

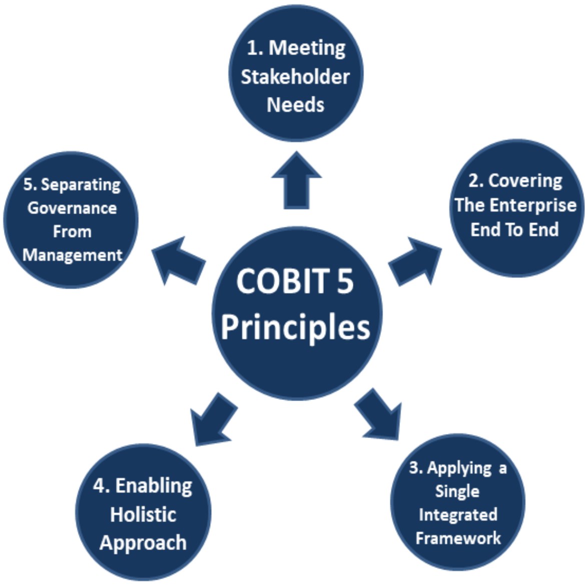
1. Meeting Stakeholder Needs
2. Covering The Enterprise End To End
3. Applying a Single Integrated Framework
4. Enabling Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Figure1. COBIT5BasicPrinciples

Based on Figure 1, Control Objectives for Information and Related Technology (COBIT) in general has five basic principles [7]:

a. Meeting Stakeholder Needs Where the company can provide value for its stakeholders. For example, by maintaining a balance between the realization of profits and possible risks.
b. Covering the entire company (Covering the End-to-End) is a system that can provide a view of IT governance and management in one company based on the number of enablers around the company.
c. Implementing a single integrated work framework (Applying a Single Integrated Framework) COBIT 5 is an integrated framework that can be aligned with other standards related to IT in providing direction to IT activities in one company.
d. Using an approach holistic (Enabling a Holistic Approach) supports defining enablers in one company's effective and efficient IT governance and management.
e. Separation of governance from management (Separating Governance from Management) describes the difference between governance and management. Two important disciplines in which there are different structures, activities, responsibilities, and goals from each other.

2.4.2 COBIT 5 Implementation

Based on ISACA [3]there are 7 (seven) stages in implementing COBIT 5:

a. Stage1(Initiate Program)
Identifies who will be the controller to support change and creates a desire to achieve goals in the executive label which is then made into a new form of process, the controller can be sourced from both internal or external parties, and the existence of problems allows to be a driver of change.
b. Stage2(Define Problems and Opportunities)
Ensure that IT goals with strategies and risks of change are commensurate and prioritize company goals, IT goals, and key IT processes.
c. Stage3(Define Road Map)
setting targets to make improvements, which is then followed by gap analysis (difference).
d. Stage4(Plan Program)
Plan the right solution for immediate execution, monitor, and ensure sustainable business risks.
e. Stage5(Execute Plan)
Calculates and monitors the system to ensure the business does not change the direction of the goal which is then carried out with daily activities.
f. Stage6(Related Benefits)
Focusing on revolutionizing continuous change from better management and management practices to business and monitoring the achievement of improvements using work schemes.
g. Stage7(Review Effectiveness)
Evaluating the achievement of objectives to identify governance needs,identifies governance or other management needs and improve needs on an ongoing basis.

2.5 Capability Level

Capability Level Process in the COBIT 5 framework there are 6 (six) levels of process capability [8].

1. Level 0 (Incomplete Process).
The process is not implemented or fails to achieve the process goal.

2. Level 1 (Performed Process).
The implementation of the process of achieving its goals. PA 1.1 Process performance, is a process implemented to achieve the objectives of its process.

3. Level 2 (Managed Process).
Processes at level 1 are implemented into process settings (planned, monitored, and evaluated) and the work products of the processes are defined, controlled, and maintained appropriately. PA 2.1 Performance Management, measures the extent to which process performance is managed. PA

2.2 Work Product Management, measures the extent to which the work products produced by the process are appropriately managed.

4. Level 3 (Established Process).
Processes defined and implemented according to existing standards, PA 3.1 Process Definitions, measure the extent to which processes are maintained to improve the deployment of specified processes. PA 3.2 Process Deployment, measures the extent to which a process is still implemented as a defined process to achieve process results.

5. Level 4 (Predictable Process).
The process operates according to the specified limits to

achieve the results of a process. PA 4.1 Process Measurement, measuring the extent to which measurement results can ensure that the performance of relevant process performance objectives is achieved in support of specified business objectives. PA 4.2 process control, measuring the extent to which processes are quantitatively managed to produce stable, capable, and predictable processes within defined limits.

6. Level 5 (Optimizing Process).
This process is constantly developed to complement the relevant current conditions and lead to business goals, PA 5.1 Process Innovation, Process innovation, measuring the extent to which process changes are identified from process implementation and from innovation approaches to process implementation. PA 5.2 Process Optimization, measuring the extent to which changes are defined, effectively manages process execution to support the achievement of process improvement goals.

2.6 COBIT 5 Goals Cascade

Based on ISACA [6], Goals Cascade COBIT 5, at this stage identifying Enterprise Goals through interviews following the needs of stakeholder needs, researchers mapping to IT-Related Goals which then establish the process on COBIT 5, the purpose of the COBIT 5 cascade is to translate specific stakeholder needs, organizational goals, IT-Related Goals, enabler goals that are implemented and adjusted to effectively support the needs of the company and IT service solutions. From the results of mapping on services in the company, it can be seen that IT-Related Goals IT agility produces six primary COBIT processes, namely APO12 (Manage Risk), and EDM03 (Ensure Risk Optimization) while for the BAI, DSS, and MEA domains there is no important relationship with existing IT-Related Goals. Of the four processes, only two processes were selected according to the level of urgency and interviews that have been carried out by the company [9].

2.7 RACI Chart

RACI Chart has a function at the level of the process of responsibility for roles in the organizational structure of the enterprise. RACI Chart defines a person's authority in an IT-based company. The RACI Chart to be used is guided by the APO12 and EDM03 processes, which will then be used to determine respondents.

2.4.3 RACI Chart APO12

The results ofthe RACI Chart are used for the APO12 domain so that researchers can map potential respondents who will fill out a questionnaire which will later be used as data processing material. RACI identification is taken based on people who are directly involved in business processes individually have been involved as actors of the RACI Chart both actors of task implementation, decision making, giving directions, and roles that must understand the decisions taken, so that it can be concluded that the elements in the PT. MandatechMataramMukti took part in the RACI Chart actors based on the person carrying out the process tasks. Effort (responsible) that is used as a reference in choosing respondents. There are 6 (six) key management practices of COBIT 5 as follows:

1. APO12.01 (Collect Data)
   Identifies and collects data that is useful for identifying, analyzing, and reporting risks related to effective information technology.
2. APO12.02 (Analyze Risk)
   Disseminates useful information to support decision-making that is useful in business processes and risk factors that occur.
3. APO12.03 (Maintaining a Risk Profile)
   Maintains a list containing known risks and risk attributes and control resources, capabilities, and activities
4. APO12.04 (Articulating Risks)
   Provides all stakeholders with the necessary information technology explanations and opportunities for the latest information technology to get an appropriate response.
5. APO12.05 (Define a Risk Management Action Portfolio)
   Managing existing opportunities to minimize all risks to a level acceptable as a portfolio
6. APO12.06 (Respond to Risk)
   Respond quickly in a short time with effective measures to reduce the amount of loss due to events related to information technology.

2.4.4 RACI Chart EDM03

RACI is for the EDM03 domain, so that questionnaire questions can be used for prospective respondents to be filled out which will later be used as data processing materials. RACI Chart Identification is taken based on people directly involved in business processes in PT. MandatechMataramMukti. RACI Chart above is taken based on the duties of each individual who is in the company the parties in the company have been individually involved as actors from the RACI Chart, both acting actors, decision making, direction givers, and roles who must understand the decisions taken so that it can be concluded that the elements in the company contribute to the RACI Chart actors based on the person who carries out the task of participating in the business process (person in charge) which is used as a reference in the selection of respondents. There are 2 (two) key governance practices of COBIT 5 as follows:

1. EDM03.01 (Evaluate Risk Management), this process reviews and assesses the effect of risk on the use of the latest information technology in the company. Taking into account the appropriate risk appetite of the company and the risks to the value of the company associated with the use of information technology are identified and managed.
2. EDM03.02 (Direct Risk Management), this process establishes risk management measures to provide adequate confidence regarding information technology risk management following ensuring that information technology risks do not exceed the risk appetite of directors.

2.8 ProcessAssessmentModel

According to ISACA [6], The Process Assessment Modelis used for process-based COBIT assessment to improve theaccuracy and reliability of IT process assessment. Indicatorsare used to assess whether a process attribute can be achievedornot.Thereare2(two)types of assessment indicators:

1. Process Capability Indicator, with ability levels 1 to 5.This indicator is general to each attribute of processcapabilities.Theindicatorsusedtoassessprocesscapabilityare GenericPractice(GP)andGenericWorkProducts (GWP).
2. ProcessPerformanceIndicator,whichappliesexclusivelyto thelevelofability1.Processperformanceindicators(basicpracticesandworkproducts)aredeterminedforeachprocessan dareused to determine whether the process capabilities areat level.

3. METHODOLOGY

3.1 Research of Stage

This section will explain the methodology for carrying out research work so that the work steps are planned and become more systematic and orderly. This chapter will explain the methodology of the research to be carried out. The stages of this research are carried out so that the work steps become more systematic and directed. This section will explain the methodology for carrying out research work so that the work steps become more systematic and organized. The stages of research include 6 steps which are broad as follows:

1. In the first stage, the researcher will start research by conducting literature studies as an initial stage, literaturestudies are carried out by collecting references from both journals and books. There are 6 journals quoted of course, the journals used in research in the last 3 years, and 1 book about COBIT 5.
2. The second stage is identifying the problem, in this stage, the researcher makes direct observations in Human Resources in Higher Education to get results from these problems. Synchronizing the problem with the method taken, namely COBIT 5 and position mapping using the RACI Chart method.
3. The third stage is collecting data. data collection techniques using the media questionnaire, observation, and interview.
4. The fourth stage performs data analysis, the researcher will assess the capability value of the Current Capability Level by processing the questionnaire data, then the researcher will assess the desired capability level, capability level value, and the last time the researcher conducts a gap assessment.
5. In the fifth stage, researchers will make recommendations following each domain that has a gap value, in the follow-up if the recommendations are implemented the organization will have the advantage of being able to reach the desired level. Recommendations will then be reported to human resources in universities as input to increase the desired level.
6. In the sixth stage, researchers will share suggestions and conclusions in conducting research based on known results. The following are the stages of the research work that will be carried out [10].

The stages of the research work that will be carried out as shown in Figure 2. This research was conducted using COBIT 5 framework for the APO12 (Manage Risk) and EDM03 (Ensure Risk Optimization). The scenario that will be passed explains the stages of working on this research so that the steps are more focused and clear [11].

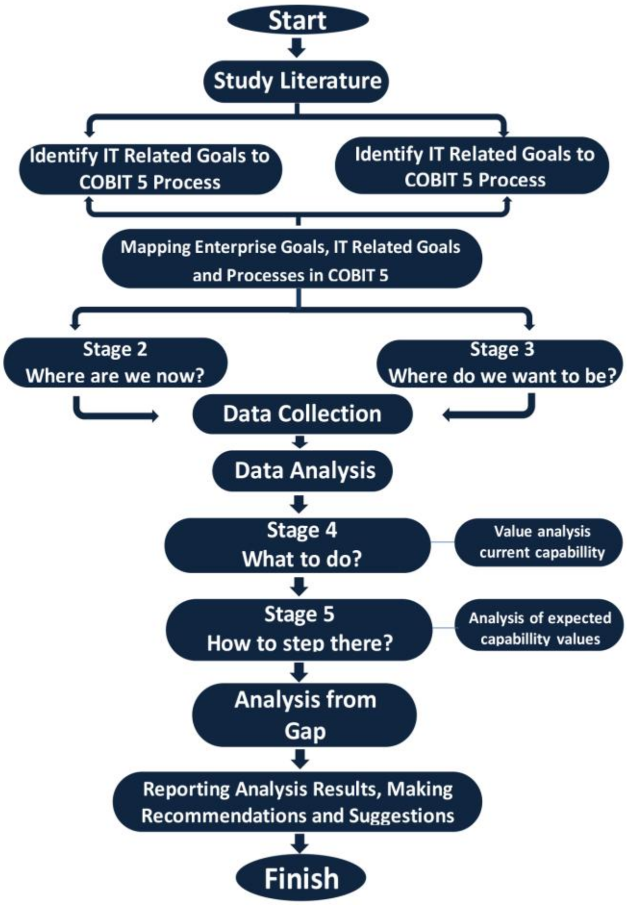
Start
Study Literature
Identify IT Related Goals to COBIT 5 Process
Identify IT Related Goals to COBIT 5 Process
Mapping Enterprise Goals, IT Related Goals and Processes in COBIT 5
Stage 2 Where are we now?
Stage 3 Where do we want to be?
Data Collection
Data Analysis
Stage 4 What to do?
Value analysis current capability
Stage 5 How to step there?
Analysis of expected capabillity values
Analysis from Gap
Reporting Analysis Results, Making Recommendations and Suggestions
Finish

Figure2. Risk Assessment Analysis Research Stage of Medical Information System Services

Based on Figure 2,the stages of the research carried out are as below:

1. Literature studies are carried out by collecting various information and references regarding research topics. This is done to support knowledge in managing risks in the company. The literature used is academic books, papers, theses, and journals related to risk management, as well as the COBIT 5 standard framework guidebook.
2. Defining the problem by specifying the process domains usedAPO12 and EDM03 to define the RACI Chart.
3. Collect the necessary data for the evaluation of information technology by disseminating questionnaires, observations, and interviews.
4. The fourth stage is to analyze the data, it takes the role of the researcher to process the data, and then makes its information and then the information will be used to make decisions. 5. Researchers will find out how much capability levellevel a company has (PT. MandatechMataramMukti), after knowing the current level of capability level, the next stage will be giving authority to the implementing party to determine the expected capability. the level then the final process is to analyze the degree of capability resulting in gaps.
5. The fifth stage is the stage of reporting research results, after knowing the results of research in the previous stage, will then be reported to stakeholders and at the same time provide suggestions and recommendations based on research results to the organization.
6. Make conclusions and suggestions from research that contains a summary of the results of the research

process that has been carried out, to answer the formulation of the problem and research objectives.

2.9 Data Collection

1. Observational
   Observation is carried out by observing directly an objectin detail and reviewing and understanding a situation oreventthataimstoaswellasseekinformationandproblemstobestudiedinthisstudy.Inthisstudy,observations were made by studying and understandingMedical Information System Services.
2. Interviews
   Interviews are conducted between two or more people bymeetingface-to-facebetweentheinformantandtheinterviewer.Thisinterviewwasconductedtoobtainaccurateinformation fromthe interviewes.
3. Questionnaire,
   The questionnaire uses the RACI Chart method to determine research respondents, this method aims to more easily map and distinguish the main tasks that are following the responsibilities of each work unit or existing employee to help carry out the company's business processes.

2.10 Implementation

3.3.1 Questionnaire Preparation

Assessment of risk by measuring the Capability Level in the APO12 (Manage Risk) and EDM03 (Ensure Risk Optimization) domains, researchers used a questionnaire survey method based on the Capability Model COBIT 5, namely by looking at activity points in the process domain APO12.01 to APO12.06 and processing the domain EDM03.01 to EDM03.02 Determine the level of capability. Questionnaires will be conducted to determine the level of capabilityin the company. The results of this method of making questionnaires will be used as a guideline for solving research problems and the extent of the level of risk in the company.

3.3.2 Determination of Respondents

The RACI Chart method to identify potential respondents, this study is a method used to map potential respondents so that it can facilitate decision-making and help management determines the roles and responsibilities of each respondent. Research respondents are required for data collection. The stage of determining respondents is carried out by identifying respondents who are believed to understand the medical information system service. Respondents are also taken according to the duties and responsibilities of each staff member.

Table1.ChartResultRespondents RACIAPO12

No	Unit COBIT5	ID
1	BusinessProcessOwner	R1
2	ProjectManagementOffice	R2
3	ChiefRiskOfficer	R2
4	ChiefInformationSecurityOfficer	R2
5	HeadArchitect	R2
6	HeadDevelopment	R3
7	HeadIT Operations	R3
8	HeadITAdministration	R4
9	ServiceManager	R5
10	InformationSecurityManager	R3
11	BusinessContinuityManager	R5
12	PrivacyOfficer	R4
13	Compliance	R5
14	Audit	R4
15	ChiefInformationOfficer	R3

Based on Table 1, the results of the domain mapping RACI Chart APO12 (Manage Risk) on Medical Information System Services PT. MandatechMataramMukti has 5 work units that have been matched with work units in the company and produced five respondents who will fill out the research questionnaire. Because there are several units of work done by the same person.

Table2.ChartResultRespondentsRACIEDM03

No	Unit COBIT5	ID
1	ChiefExecutive Officer	R1
2	BusinessExecutives	R5
3	StrategyExecutiveCommittee	R2
4	ChiefRiskOfficer	R2
5	ChiefInformationOfficer	R3

Based on Table 2, the results of the RACI Chart EDM03 domain mapping (Ensuring Risk Optimization) on PT. MandatechMataramMukti 5 work units have been matched with work units in medical information system services and produced five respondents who will fill out a questionnaire. Research because there are several units of work carried out by the same person.

3.3.3 Observation and Interview

At the observation stage and interviews are conducted to obtain relevant data related to the research topic. The interview aims to obtain valid data so that the results of the study can be maintained until it is completed. Here are the results of interviews conducted by researchers:

1. Overview of PT.MandatechMataramMukti.
2. Overview of Medical Information System Services at PT. MandatechMataramMukti.
3. The organizational structure of the Medical Information System Services of PT. MandatechMataramMukti.
4. Business processes on Medical Information System Services.
5. Duties and responsibilities of staff in the Medical Information System Services of PT. MandatechMataramMukti.
6. Problems that exist in Medical Information System Services today.
7. Find a way out of the problem of the Medical Information System Service together.
8. Capability Level value that the company expects on Medical Information System Services.
9. Management risks that may occur in medical information system services are expected to be overcome by risk assessment analysis using the COBIT 5 framework and APO12 (Manage Risk) and EDM03 (Ensure Risk Optimization) process domains.

3.3.4 DataAnalysis

The value expected by the company is at level 2. At this level, the company already has a standardization of IT processes within the scope of thecompany as a whole. This means that they already have a standard of process that applies throughout the company.

3.3.4.1 CurrentLevelCapability

At this stage, the researchers used the calculation of the GuttmannScale and the COBIT5 Toolkit Version Scale to calculate the Current Level Capability value. The results of the calculations can be seen in Table 3.

Table3.CurrentCapabilityAPO12

Domain	Process	Current Level
APO12.01	Collectingdata	1,86
APO12.02	Analyzingrisk	1,63
APO12.03	Maintainingriskprofile	1,89
APO12.04	Articulationofrisk	1.96
APO12.05	Determining riskmanagementportfolio	1.59
APO12.06	Respondingtorisk	1.65

Based on Table 3 the calculation of the APO12 domain questionnaire (Manage Risk) using Guttmann scale calculations obtained a value of 1.76 (Performed Process). This value is obtained from the calculation of the average Current Level divided by the number of process domains. the implementation of business processes in the Medical Information System Services has carried out planning, monitoring, and adjustments and the results of their work have been determined, supervised, and maintained properly. The following is a table of calculation results using the EDM03 domain. The table of calculation results can be seen in Table 4.

Table4.CurrentCapabilityEDM03

Domain	Process	Current Level
EDM03.01	Evaluating riskmanagement	1.67
EDM03.02	Directingrisk management	1.60

Based on Table 4 above, the value is 1.64 in the calculation of the current level. At this level, it can be said that the company has not achieved standardization of IT processes within the scope of the company as a whole and has been implemented throughout the company.

3.3.4.2 Expected Level Capability

The expected value of Medical Information System Services is at level 2. At this level, the company does not yet have a standardized IT process for the company as a whole. This means that they do not have a standard process that applies throughout the company.

3.3.4.3 Analysis GAP Value GAP

The value obtained in the APO12 (Manage Risk) domains is 1.00 while in the EDMO3 (Ensure Risk Optimization) domains it is 1.00, which means that the Medical Information System service has not reached the desired level, so it requires recommendations and suggestions to achieve the desired level.

Table5.GAPDomainValueAPO12

Domain	Process	Current	Expected	Max	Gap
APO12.01	Collectingdata	1.86	2.00	5.00	1
APO12.02	Analyzingdata	1.63	2.00	5.00	1
APO12.03	Maintaining riskprofile	1.89	2.00	5.00	1
APO12.04	Articulaterisk	1.96	2.00	5.00	1
APO12.05	Determine riskmanagementportfolio	1.59	2.00	5.00	1
APO12.06	Respondtorisk	1.65	2.00	5.00	1
Average CurrentLevel		1,76	2.00	5.00	1

Based on Table 5 above, it can be concluded that Medical Information System Services reach level 1.76 which means that the company in implementing the IT process has achieved its goals, and has been managed well, so there is more assessment because the implementation and achievements are carried out with good management. The Capability Level results show the known EDM03 (Ensuring Risk Optimization) domains. The table of gap values can be seen in Table 6.

Table 6. Domain Value GAP EDM03 Domain Current Value

Domain	Process	Current	Expected	Max	Gap
EDM03.01	Evaluatingrisk	1.67	2.00	5.00	1
EDM03.02	Directing riskmanagement	1.60	2.00	5.00	1
AverageCurrentLevel		1.64	2.00	5.00	1

Based on Table 6 above, it can be concluded that the medical information system has reached the expected level and received a GAP value of 1.00 for all existing domains.

Table 7. Process APO12 PA 1.1 Process Performance

PA1.1(ProcessPerformed)			
Domain	**Goal**	**Description**	**Comment**
APO12.01 (CollectData)	Collectingdata toanalyzerisk	✔	Have made effortsto implement,plan, identify andimprovemaintenance-related methodsof collecting,classifying andanalyzing datarelated toITrisks.
APO12.02 (Analyze Risk)	Analyzing risk data.	✔	Have made efforts to implement, plan,identify and improve the understanding and consideration of risk analysis, IT risk factors and

			asset criticism as well as the ability to detect IT risk scenarios.
APO12.03 (Maintain aRiskProfile)	Maintaining riskattributes.	✔	Have made efforts to implement, plan, identify and improve business process support personnel including applications, facilities and suppliers, as well as plan, utilize and improve IT service requirements and approvals to maintain business processes.
APO12.04 (ArticulateRisk)	ProvidesinformationonIT riskopportunities.	✔	Have made efforts to implement, plan, identify and improve reporting the results of IT risk analysis to stakeholders in a format that is useful for supporting organizationaldecisions.
APO12.05 (DefineRisk ManagementPortofolio)	Managingopportunitiestominimizerisks	✔	Have made efforts to implement, plan, identify and improve activities to maintain an inventory of risk management controls in accordance with IT risks tolerance.
APO12.06 (RespondtoRisks)	Responding appropriatelyto IT risks.	✔	Have made efforts to implement, plan, identify, and improve the implementation of appropriate response plans to minimize the impact of IT risks incidents.
EDM03.01 (EvaluateRisk Management)	Evaluatingand assessing the useof IT	✔	Have made efforts to implement and improve the evaluation of the risk tolerance limits that used to be accepted by the company.
EDM03.02 (DirectRiskManagement)	Directing theimplementation of IT risk management	✔	Have made efforts to directly implement appropriate mechanisms to respond quickly to changes in risk and report immediately to the leadership supported by agreed principles.
Average Score			100%

Based on Table 7 above, can be seen that the completeness of data requirements at level 1 in each process domain has been met and can be interpreted on a PA (Process Attribute) scale with attribute values > 85% - 100% F (Full Achieved). To be able to reach level 1 Medical Information System Services must meet the requirements at level 1. The following is the completeness of the data requirements owned by customer service by APO12. A full list of data needs can be found in Table 7. The objectives of process performance are identified in the risk management of the services inthe company has made efforts to improve the achievement of the goal of implementing IT risk tolerance which requires an appropriate response. Employee SOP and Process Performance will be planned and monitored in risk management have made efforts to increase the rapid level of indicators for the identification and monitoring of IT risk profiles the responsibility and authority to carry out the processes are determined, assigned, and the company has made efforts to implement and improve employee SOP it is then communicated in the understanding of risk management IT risk analysis, IT risk factors and critical assets. The values and capability level values in the APO12 and EDM03 domains. The graph on the gap and capability level values can be seen in Figure 3.

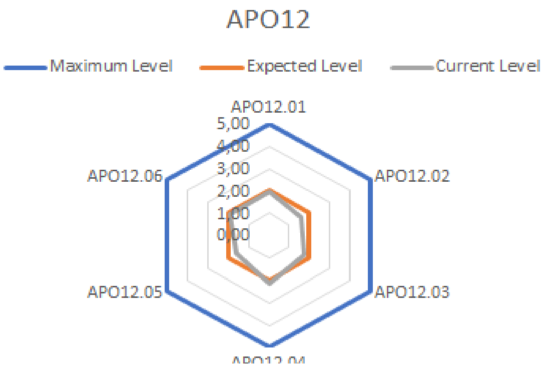

Figure 3. Graphic Gap Value Domain APO12

Figure 3 is a graph of the expected value and domain alignment value APO12 which will be a guideline for a technological solution whose value is prepared from a questionnaire with the COBIT 5 domain standard that has been studied, based on picture of the gap value and the EDM03 domain capability value.

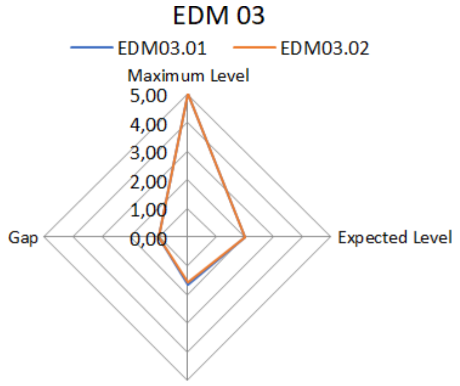

Figure 4. Grafic Gap Value Domain EDM03

Based on Figure 4.it is known that the EDM03 process (Ensuring Risk Optimization) is at level 1 seen from the value of capability level 1. At this level, the Medical Information System Services has implemented the Performed Process.

3.3.4.1 APO12andEDM03 Recommendation

Table 8.The results of the recommendations and suggestions obtained from the analysis of the gap values obtained will be carried out by the service department in the company can be seen in Table 8.

Table 8. Recommendation and Suggestion Report

Domain	Recommendation
APO12.01 (Collect Data)	a. Should plan to report data related to IT risks that may occur in the future, and conduct meetings or find solutions or evaluations to overcome these possible risks. b. Staff in Medical Information System Services must monitor and conduct meetings related to planning and evaluation in managing data records both in the internal and external environment in managing IT risks. c. Must have a plan for managing IT risks, one of which is having backups and data that contains databases and MOU processes for further investigations. d. Must plan to record or document the results of meetings or deliberations that discuss follow-up investigations and evaluations related to IT. e. Must have staff who specifically plan in monitoring and managing the data that has been collected as well as evaluate the main causal factors related to IT.
APO12.02 (Analyze Risk)	a. Should include planning, monitoring, and evaluating materials that specifically address the deepening of risk factors in employee SOP documents. b. Should carry out risk mapping planning to assist in making subsequent decisions regarding the estimated

	magnitude of losses and profits related to IT risk scenarios. c. Must evaluate, and determine mutually agreed benchmarks in identifying IT risks. d. Must have records or databases related to the costs of various actions taken by the company to deal with risks that may occur in the future.
APO12.03 (Maintain aRiskProfile)	a. Must make planning efforts related to the addition of auxiliary staff in working to maintain the course of business processes. b. Must have monitoring and evaluation planning guidelines in place to maintain their course. c. Must monitor the data input related to the company's database to be safe for the use of information about IT risk events recorded in the company's risk profile.
APO12.04 (ArticulateRisk)	a. Must conduct joint evaluations of stakeholders to support business processes, and company decisions. b. Must have monitoring and evaluation of the implementation of SOPs in managing IT-related business processes, so as not to cause greater losses and face the worst possibilities. c. Must create SOPs or documents that regulate the company's business processes so as not to pose greater risks.
APO12.05 (DefineaRiskManagementActionPortofolio)	a. Must have a thorough preparation in testing the agreed plan so that when a risk occurs, the plan can overcome the risks that are occurring. b. Must have a planning document that sets a reasonable limit of tolerable risks so that these risks do not hinder the course of the company's business processes.

	c. Must have project planning, and monitoring designed to reduce the risks that enable the company's strategic opportunities.
APO12.06(Respond to Risk)	a. Should plan preparations and test plans that document the specific steps to be taken when a risk event occurs. b. Should carry out incident category planning, and comparison of actual exposures with risk tolerance thresholds. c. Must carry out appropriate response planning to minimize the impact when risk incidents occur.
EDM03.01 (Evaluate RiskManagement)	a. Should periodically evaluate the management activities factoring the level of its risk to the company and ensuring that the company's decisions have been made correctly. b. Must carry out planning for the creation of standards for the level of risk that the company uses to meet the company's objectives.
EDM03.02 (Direct RiskManagement)	a. Must plan, monitor and evaluate the promotions that have currently been carried out and expand the promotion to each reach. b. Must maintain and improve in terms of directing the risks that arise to be properly resolved.

Based onTable 8, recommendations from the APO12 and EDM03 domains are made to be applied to Medical Information System Services to have an impact on reducing IT risks.

4. CONCLUSION

Based on the calculation of the Current Level in the APO12 (Manage Risk) and EDM03 (Ensure Risk Optimization) domains, the Capability Level value is 1.83 (Performed Process) for the APO12 (Manage Risk) domains. For the EDM03 (Ensuring Risk Optimization), the Capability Level value is 1.62 (Performed Process). Value of gaps (differences) in the APO12 (Manage Risk) and EDM03 (Ensure Risk Optimization), domains have been known using concrete calculations and obtained gap values in each domain. For the APO12 (Manage Risk) domain, the gap value of 1 level is obtained from the calculation of the Current Level in the APO12 (Manage Risk) domains. As for the EDM03 (Ensuring Risk Optimization)domains, it produces a gap value of 1 level. The result of the recommendations given is to improve risk management in Medical Information System Services that have not reached the desired level require recommendations and mitigation measures that must be carried out, namely by having a regular schedule, making IT risk management SOPs, backing up data to company databases, adding staff who are experts in analyzing risks so that improvements can be made so that risks arise that can be identified and resolved properly. Technology that has not reached the desired level requires recommendation and mitigation steps that must be carried out, namely by having a routine schedule, making SOPs on IT risk management, backing up data to the company database, adding staff who are experts in analyzing risks so that new investigations can be carried outthat may arise can be identified and resolved properly.

5. REFERENCES

[1] ISACA. 2012. COBIT 5: A Business Framework For The Governance and Management Of Enterprise IT. 2012.

[2] Putri, I. Y., Suprapto., & Herlambang, D. A. (2018). ‘Assessment of the Capability of Implementing Information Technology Risk Management using the

COBIT 5 Framework (Study on PDAM Malang City, East Java)', Journal of Information Technology and Computer Science Development, e-ISSN: 2548-964X, Vol. 2, No. 11, November 2018, hlm. 4855-4862.

[3] Astuti, R. (2018). Implementation of Information System Risk Management using COBIT 5. Media Informatics (Vol.17No.1).https://jurnal.likmi.ac.id/Jurnal/3_2018/0318_04_Rini.pdf.

[4] ISACA. 2012. COBIT 5: Enabling Processes, Rolling Meadows. ISACA. 2012. COBIT 5 Implementation.USA: IT Governance Institute.

[5] Elly., & Halim, F. (2021). 'IT Infrastructure Governance Evaluation With COBIT 5 Framework', Journal of Information Systems, SMIK Mikroskil.

[6] YP Andriani and I. Riadi. (2021). “Risk Assessment of Monitoring Services using COBIT 5 Framework,” Int. J. Comput. Appl., vol. 183, no. 37, pp. 8-16.

[7] ISACA. 2012. COBIT 5: Process Assessment Model, USA: IT Governance Institute.

[8] Jung, Ho-Won, & Hunter, R. (nd). The Relationship Between ISO/IEC 15504 Process Capability Levels, ISO 9001 Certification, and Organization Size. An Empirical Study. Elsevier.

[9] Alfia Miranti. 2019. Evaluation of Information Technology Governance using COBIT 5 Framework (Case Study: PT. Praweda Ciptakarsa Informatics). Thesis. Jakarta: Information Systems UIN Syarif Hidayatullah.

[10] Tamara. (2021). Analysis ofRisk Management Assessment on Student Credit Services using COBIT 5 Method.

[11] Rival Dwi Anggriyan P., Eman S., Awalludiyah and Ambarwati. 2019. Evaluation of IT Risk Management using Framework COBIT 5 for PT.BTM. Journal Information Systems (E-Journal). VOL.11, NO.2, October 2019.

[12] Fitriani, W., & et al. (January 2019). Information Technology Governance Audit using COBIT 5. Journal of Engineering and Informatics Vol. 6, No. 1, Pg. 42 - 45.

[13] Khairuna, D., Wibowo, S., & Gamayanto, I. (2020). 'Evaluation of Information Technology Risk Management using COBIT 5 Framework Based on Domain APO12 (Manage Risk) at Head Office of BPR Agung Sejahtera', Journal of Information A system, Vol. 5, No. 1, Mei 2020:18-26 DOI:10.33633/joinsv5i1.3088.

[14] Setyaningrum, ND (2018). Evaluation of Information Technology Risk Management using COBIT 5 Framework (Case Study: PT. Kimia Farma (Persero) Tbk- Plant Watudakon). Journal of Information Technology Development and Computer Science. (Vol. 2 No. 1) http://jptiik.ub.ac.id/index.php/jptiik/article/download/731/286.

[15] Sugiyono. (September 2019). Quantitative, Qualitative, and R&D Research Methods. Bandung: ALFABETA.

[16] Astuti, R. (2018). Implementation of Information System Risk Management using COBIT 5. Media Informatics, 17(1), 18–28.

[17] Khairuna, D., Wibowo, S., & Gamayanto, I. (2020). ‘Evaluation of Information Technology Risk Management using COBIT 5 Framework Based on

[18] Nurfitri Zukhrufatul Firdaus., Suprapto. 2018. Evalution IT Risk Management using COBIT 5 IT Risk (Case Study: PT. Petrokimia Gresik). Journal IT Development and Computer Science, Vol.2, No. 1, January 2018, Pg. 91-100

[19] Nurfadiun. 2017. Creating a Risk Management Model for Information Technology Infrastructure Management using COBIT 5 Framework Biskom UAD. Thesis. Yogyakarta: Informatics Engineering UAD.

[20] Dimas Adi P., Awalludiyah A. and Eman S. 2020. Risk Management Analysis Dealer Management System Service using COBIT 5. JOURNAL MATRIX, VOL. 10, NO. 2.

[21] Riyan Abdul A., Kusrini and Sudarmawan. 2018. Evaluation of Information Technology Risk Management in STATE-OWNED Companies using Cobit 5 Standard (Case Study: PT TASPEN PERSERO). Journal IT CIDA Vol. 4 No. 2 December 2018.

[22] Prilly Peshaulia Thenu, Agustinus Fritz Wijaya and Christ Rudianto. 2020. Information Technology Risk Management Analysis using COBIT 5 (Case Study: PT GLOBAL INFOTECH). Journal Bina Computer JBK, Vol. 2, No. 1, 1-13.

[23] Riki N. and Handayaningsih, S.2019. Risk Management Analysis of Student Resignation Services using COBIT 5 Framework Focuses on Managing Risk (APO12).

[24] M. Habibullah A., Suprapto. 2018. Evaluation of Information Technology Risk Management Using the COBIT 5 Framework (Case Study for Perum Jasa Tirta 1 Malang). Journal of Information Technology Development and Computer Science, Vol.2, No. 1, January 2018, hlm. 101-110.

[25] Yani Iriana Putri, Suprapto and Admaja Dwi Herlambang. 2018. Assessment of Capability Implementing Information Technology Risk Management sings the COBIT 5 Framework (Case Study: PDAM Malang East Java). Journal Development of Information Technology and Computer Science Vol. 2, No. 11 November 2018, hlm 4855-4862.

[26] Dimas Adi P., Awalludiyah A. and Eman S. 2020. Analysisof Risk Management in Systems Management Dealer Service using COBIT 5 Framework. JOURNAL MATRIX, VOL. 10, NO. 2.

[27] Indriyanto. (2020). Analysis of Risk Assessment in Canasoft Information Systems using COBIT 5 Framework.

[28] Nanda Noveryal and Imam Riadi. (2022). Analysis a Maturity of Case Search Information Systems using Cobit 5Framework. International Journal of Computer Applications. Vol.184, No.12, May 2022, hlm. 29-35.