Risk Assessment Analysis of Digital Government Health Service using COBIT 5 Framework

Rayyan Hartawan
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
The health Digital Government Service (DGS) aims to improve services at Health Center Kasihan II Bantul by reducing patient waiting times. However, there are risks such as errors when accessing pages due to non-optimal servers and non-integration of SIMPUS data into health DGS, which can affect data accuracy. This study aims to assess risk using the Capability Level calculation on the health Digital Government Service (DGS). This research analyzes and evaluates risk management in the health Digital Government Service (DGS) using the COBIT 5 Framework domain APO12 (Manage Risk). The main objective is to determine the capability level, current capability, expected capability, and gap, and provide relevant recommendations. Data was collected through observations, interviews, and self-assessment questionnaires to conduct Capability Level assessments. Based on the findings of the Capability Level calculation that has been carried out, the current capability is at level 4, while the expected capability is at level 5, so there is a gap of 1. Recommendations from this research, which can be reviewed to improve performance in better IT risk management at the Digital Government Service (DGS) health, according to the problems faced by the organization.

Keywords
Digital Government Health Service, Risk Management, COBIT 5, Capability Level

1. INTRODUCTION
Local governments can benefit from information technology risk management by safeguarding their information technology assets, which serve as the center of information processing, storage, and distribution. One of the local government organizations that provide health services is Health Center Kasihan II Bantul [1]. To supervise daily operations (such as patient registration, diagnosis, prescription, and supervision of current data reporting), Health Center Kasihan II Bantul implemented a Health Center Information System called Digital Government Service (DGS) Health. Health Center Kasihan II Bantul previously implemented a Health Center management information system (SIMPUS), due to changes in government policies in Bantul Regency, it was transferred to the Health Center Information System using the Digital Government Service (DGS) Health.

Digital Government Service (DGS) Health, an application designed to streamline health services at Health Center and hospitals. The implementation of DGS Health also encounters several risks such as errors when accessing pages due to non-optimal servers and non-integration of SIMPUS data into health DGS.

Based on the above problems, this study aims to assess risk using the calculation of Capability Level on health DGS. Provide recommendations so that they can minimize risk. The COBIT 5 (Control Objective for Information and Associated Technology) framework is used in this research. By achieving a balance between obtaining benefits and maximizing risks and resource usage, the COBIT 5 framework can help businesses get the most out of their IT investments [2].

2. LITERATURE STUDY
2.1 Definition of Information System
According to [3], Hardware, software, and human devices that work together to manage data are the components of information systems.

According to [4], Information systems are systems that combine organized procedures, information technology, and people to provide information for management for decision making and business operations.

2.2 Characteristics of Information Systems
According to references from [5], identifies three general characteristics of information systems, which are as follows:

1. Communication networks, because they both provide information to different parties both inside and outside the company, information systems and communication networks are similar.
2. Having data stages and conversions, turning inputs into outputs is what information systems do. This modification or transition has three stages, namely the input stage, the processing stage, or the processing stage, and the power stage.
3. Data input and information output, The input stage involves entering various data for processing, and the output stage involves presenting information.

2.3 Definition of Information System Security
Information security involves protecting against various threats to ensure business continuity, reduce risk, and increase investment and business opportunities [6].

According to [6], Information security is an effort to protect information assets from potential threats. Information security indirectly ensures business continuity, reduces emerging risks, and allows you to optimize return on investment.

2.4 Aspects of Information System Security
In designing a good information security system, there are aspects of information security that need attention. As seen in Figure 1 [7].

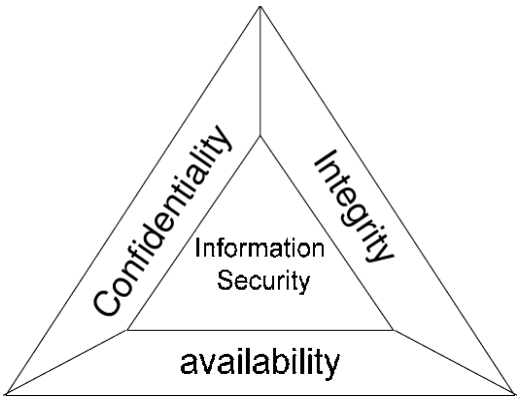


Figure 1. CIA TRIAD

The following is an explanation of Figure 1:

1. (Confidentiality) ensuring that information is kept confidential, only authorized individuals can access it, guaranteeing the confidentiality of data sent, received, and stored is kept confidential.
2. (Integrity) ensures that data is not modified without the permission of the (competent) authority, accuracy must be maintained and information needs.
3. (Availability) ensures that data will be available when necessary so that only authorized users can use information and equipment as needed.

2.5 Risk

[8], States that risk is a possibility, that a company cannot completely avoid risk even with a maximum control structure.

[9], Risk is loss or damage that can be caused by negligence, human or machine error, due to environmental disturbances, threats and even natural disasters in an environment.

According to [10], Risk is the possibility of an event that can harm the company. Risk is essentially an event that has a negative impact on the company's goals and strategies. The likelihood of a risk occurring and its effect on the business is fundamental to identify and measure.

2.6 Types of Risk

According to references from [11], risk is divided into two types, the following is an explanation of each type of risk:

1. Pure Risk
   Pure risks are risks where the possibility of loss exists and the possibility of making a profit does not exist. Examples of this type of risk are accident risk, fire risk, etc.
2. Speculative Risk
   Speculative risks are risks associated with the occurrence of two possibilities, namely the possibility of financial loss or receiving a subsidy.

According to [12], Whether risk is classified as speculative or pure risk will largely depend on the approach used.

2.7 Risk Assessment

The process of analyzing the dangers that were found during the earlier procedure is known as risk assessment. Risk assessment is done in order to prioritize the risks that need to be taken care of first and to decide which risk management technique will be used for each individual risk [13].

According to [14], Risk assessment is part of risk management, risk assessment is the process of assessing how often the risk occurs or how much impact the risk has.

2.8 Definition of Risk Management

Risk management is a process of identification, analysis, assessment, control, and efforts to avoid, minimize or even eliminate unacceptable risks [15].

According to [16], there are several stages of risk management, namely:

1. Risk Identification
   This step identifies the risks faced by the business by identifying risks by conducting a stakeholder analysis.
2. Risk Measurement
   Risk measurement refers to two factors, namely quantitative and qualitative. Quantitative risk is related to the amount or level of risk that may occur. Qualitative deals with the probability of the risk occurring, the higher the probability, the greater the risk.
3. Risk Mapping
   Risk mapping aims to prioritize risks according to their importance to the company.
4. Risk Management Model
   There are several types of risk management models, including conventional risk management models, defining risk capital, management organization structure, and others.
5. Monitor and Control
   Monitoring and control is important because:
   a. Management must ensure that the implementation of risk management is carried out as planned.
   b. Management must also ensure that the implementation of risk management is effective enough.
   c. Risk itself evolves, monitor and control aims to monitor developments against changing trends in the risk profile.

2.9 Risk Management Process

According to [17], risk management analysis methods can improve decision-making and increase the effectiveness of IT risks. There are three stages that comprise the risk management process, which are as follows:

1. Risk identification is the process of identifying risks in the organization by looking at the source of risk, its characteristics, impact, and determining the level and priority of risk.
2. Risk assessment is the stage to better understand risks by using appropriate measurement techniques.
3. Risk treatment is the next step after risk analysis, which involves risk management to avoid serious consequences.

2.10 COBIT 5

COBIT 5 can be understood as a framework that balances risks, optimizes resources, and helps businesses create the most value possible when managing information technology [18].

2.11 COBIT 5 Principles

According to [19], states that Recommendations for the administration of information technology in business are referenced in the COBIT 5 principles. The following Figure 2 lists the five COBIT 5 principles.

Figure 2. Principle COBIT 5

1. Meeting Stakeholder Needs, meeting stakeholder needs by creating value and efficiency.
2. Convering the Enterprise End to End, COBIT 5 involves human resources and governance as a whole.
3. Appliying a Single Integrated Framework, using an integrated framework with IT standards and best practices.
4. Enabling a Holistic Approach, Supports a holistic approach to IT management.
5. Separating Governance from management, separating governance from management in structure and purpose.

2.12 Enabler COBIT 5

COBIT 5 uses enablers to implement IT governance and management, helping companies achieve their goals. There are seven categories of enablers in COBIT 5 [19], as shown in Figure 3.

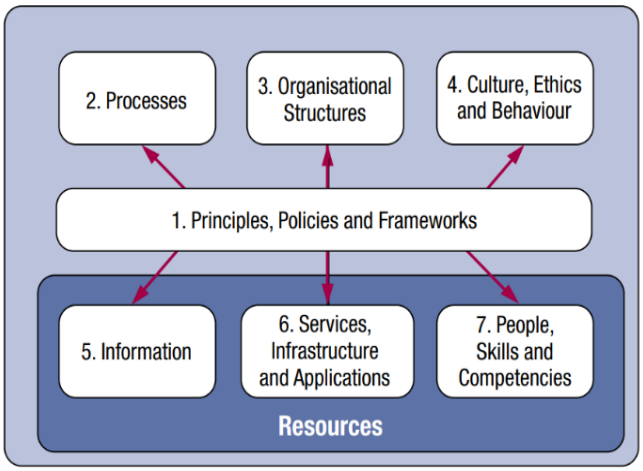


Figure 3. Enabler COBIT 5

1. Principles, policies, and frameworks guide enterprise IT operations according to stakeholder needs.
2. Processes provide details of actions to achieve enterprise IT goals.
3. Organizational structure influences decision-making and needs to consider stakeholder goals and needs.
4. Culture, ethics, and behavior are important in achieving organizational values and goals.
5. Information is required for decision making and problem solving.
6. Services, infrastructure, and applications are the main drivers in COBIT 5 to achieve corporate IT goals.
7. People, Skills and Competencies to carry out tasks in accordance with business objectives.

2.13 COBIT 5 Mapping

By prioritizing tasks based on the nature of the problem at hand, COBIT 5 mapping seeks to align an organization's IT objectives with business objectives. The results of the mapping are used to determine the level of capability. The following COBIT 5 mapping is taken from [19].

1. Enterprise Goals, using the Balance Scorecard (BSC) as a guide, Enterprise Goals map organizational goals into 17 EG points from a BSC perspective. The company's vision and mission are translated into operational goals and activities by the BSC.
2. Mapping Enterprise Goals (EG) with IT-Related Goals (ITR), harmonizing the relationship between EG and ITG is a mapping process known as Mapping EG with IT-Related Goals (ITG). ITGs define the COBIT 5 enablers required to achieve these IT goals and link the organization's key business objectives into specific IT goals.
3. Mapping IT-Related Goals (ITR) with process domains, this mapping is a key stage in integrating information technology-related goals with ITG process domains. This is done by carefully aligning each ITR with the most relevant and mutually supportive domain processes

2.14 COBIT 5 Framework Domains

According to [20], COBIT 5 has a domain in its management process, as in Figure 4.

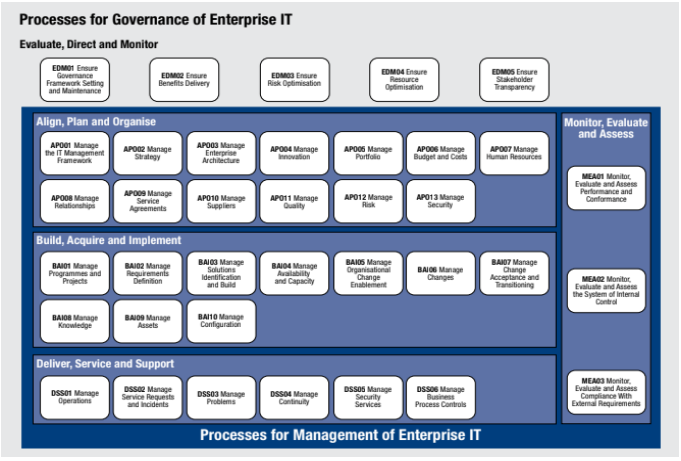


Figure 4. COBIT 5 Process Stages

1. Domain Evaluated, Direct and Monitor (EDM)
   This domain explains that IT governance assesses the conditions, needs, and preferences of stakeholders to ensure the achievement of organizational or business goals. This domain has 5 subprocesses and 15 subprocesses.
2. Domain Align, Plan and Organise (APO)
   This domain covers the use of technology and information and how best the organization uses them to achieve goals. There are 13 sub-processes and 72 sub-sub-processes in the APO domain.
3. Domain Build, Acqure and Implemant (BAI)

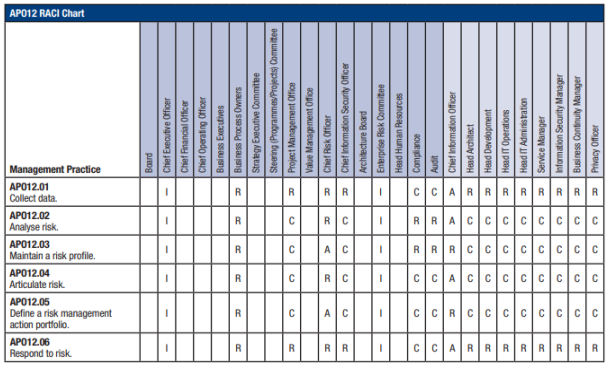
The BAI domain identifies information technology (IT) needs, acquires technology and implements it into the company's ongoing business process activities. There are 10 sub-processes and 68 sub-processes in the BAI domain.

4. Domain Deliver, Service and Support (DSS)
   The DSS domain covers, among other things, the implementation and results of systems and processes that support the efficient and successful implementation of IT systems. There are 6 sub-processes and 38 sub-processes in the DSS domain.
5. Domain Monitor, Evaluated and Asses (MEA)
   The MEA domain is an organization's or company's strategy for assessing the needs and whether the current IT system implementation can still achieve the planning and control objectives required for compliance. The MEA domain consists of 3 sub processes and 17 sub processes.

According to [21], COBIT 5 has two processes related to information technology (IT) risk management, namely domain APO12 and domain EDM03.

2.15 RACI Chart

According to [22], the diagram that connects resources and activities in each organizational process is called RACI. The purpose of the RACI Chart mapping is to identify the parties who play the role of responsible, accountable, consulted and informed. RACI Chart APO12 as shown in Figure 5.



APO12 RACI Chart

Management Practice	Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering (Programme/Projects) Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO12.01 Collect data.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R
APO12.02 Analyse risk.		I				R			C		R	C		I		R	R	A	C	C	C	C	C	C	C	C
APO12.03 Maintain a risk profile.		I				R			C		A	C		I		R	R	R	C	C	C	C	C	C	C	C
APO12.04 Articulate risk.		I				R			C		R	C		I		C	C	A	C	C	C	C	C	C	C	C
APO12.05 Define a risk management action portfolio.		I				R			C		A	C		I		C	C	R	C	C	C	C	C	C	C	C
APO12.06 Respond to risk.		I				R			R		R	R		I		C	C	A	R	R	R	R	R	R	R	R

Figure 5. RACI Chart APO12

The following is an explanation of the RACI Chart [23].

1. Responsible: The person who does the work.
2. Accountable: The person responsible for the success of the task.
3. Consulted: The person who contributes by gathering information.
4. Informed: People who receive information for task monitoring.

2.16 Process Capability Level

The achievement of process attributes is the basis for determining the level of process capability which is certainly adapted to [24]**.** In the risk management Capability Level process can be categorized at six levels. The category consists of level 0 to level 5, the following is an explanation of each level:

1. Level 0 – Incomplete Process
   The information technology (IT) management process is not successfully implemented by the company or organization.
2. Level 1 – Performed process
   The process of achieving or achieving predetermined goals is then implemented. Process attributes at level 1 are shown in Table 1.

Table 1. Performed Process

Level 1-Performed Process	
Attributes	**Attributes**
PA 1.1 Performed Process	Measures how many process objectives are achieved. The result of this attribute is reflected in each process that produces the expected output.

3. Level 2 (Managed Process)
   At level 2, process execution is carried out with planning, monitoring and adjustment and work results are identified, monitored and maintained properly. There are two process attributes at this level as seen in Table 2.

Table 2. Managed Process

Level 2-Managed Process	
Attributes	**Objectives**
PA 2.1 Performed Management	Regulates how much the execution of the process is regulated.
PA 2.2 Work Product Management	Meausuring how much work product is produced by a well organized process.

4. Level 3 (Estabilished Process)
   At this stage, the company has implemented IT processes and is well standardized, the established procedures have two process attributes as can be seen in Table 3.

Table 3. Estabilished Process

Level 3-Estabilished Process	
Attributes	**Objectives**
PA 3.1 Process Definition	Measures how much the process is defined to support the execution of the process
PA 3.2 Process Deployment	Meausures how much the process standards are implemented effectively

5. Level 4 (Predictable Process)
   The company has implemented the IT implementation process within the specified limits to achieve the desired results. This level there are two process attributes can be seen in Table 4.

Table 4. Predictable Process

Level 4 – Predictable Process	
Attributes	**Objectives**
PA 4.1 Process Measurement	Measuring how far the results obtained, will then be used to ensure that the quality of the process can support the achievement of company goals.
PA 4.2 Process Control	Measures how far a process can quantitatively produce a stable, capable

	and predictable process within predefined limits.

6. Level 5 (Optimizing Process)
   At Level 5, processes are continuously improved to carry out current and projected future organizational goals. At this level there are two process attributes, as shown in Table 5.

Table 5. Optimizing Process

Level 5 – Optimizing Process	
Attributes	**Objectives**
PA 5.1 Process Innovation	Measures how much process change is identified from process execution and from the innovation approach to process execution.
PA 5.2 Process Optimizing	Measuring how much change is defined, effectively managing process execution to support the achievement of process improvement goals.

As described by [25]. This assessment process involves the use of scores associated with each level, which will then be used as a basis for determining the value of each point presented in detail in Table 6.

Table 6. Capability Level Rating Scale

Code	Description	Range
N	Not Achieved	0%-15%
P	Partially Achieved	>15%-50%
L	Largely Achieved	>50%-85%
F	Fully Achieved	>85%-100%

2.17 Questionnaire Data Processing

According to [7], data management is carried out by based on the results of respondents' answers by filling out a questionnaire according to a likert scale to calculate and summarize the respondents' answers to the questionnaire. Therefore, it can be explained with the following assessment formula:

1. Calculating the Percentage of Questionnaire Answers

$$C = \frac{H}{JR}\ x\ 100\%$$

   Description:
   C = Recapitulation of Capability Level questionnaire answers (in the form of percentage on each answer choice in each activity)
   H = Number of answers to the Capability Level questionnaire on each answer choice in each activity
   JR = Number of Respondents
2. Calculating the capability value of each subdomain

$$NK = \frac{(Lp\ x\ Nk0) + (Lp\ x\ Nk1) + (Lp\ x\ Nk2) + (Lp\ x\ Nk3) + (Lp\ x\ Nk4) + (Lp\ x\ Nk5)}{100}$$

   Description:
   NK = Maturity value of the IT process
   LP = Level Percentage (percentage level in each distribution of Capability Level questionnaire answers)
   Nk = Maturity value listed in the answer mapping table, value and maturity level.
3. Calculating Capability Level

$$Capability\ Level = \frac{\sum \textbf{Capability Value}}{\sum Process\ Domain}$$

3. METHODOLOGY

3.1 Research Stages

This section will explain how to do research work so that the work stages become more organized, systematic and efficient. The following are the steps of the method that will be carried out:

1. The first stage, literature Study is carried out by collecting various information and references related to the research topic. This is done to support knowledge in performing risk management on the Health Center Information System (DGS). The literature used includes academic books, articles, theses and journals related to risk management, as well as standard framework guidelines.
2. The second stage, COBIT 5 Mapping. This step involves mapping Enterprise Goals, IT-Related Goals and IT processes that produce priority domains in this study.
3. Stage three, collecting data needed for information technology assessment, by observation, interviews, and questionnaires.
4. Fourth stage, data processing and analysis. At this stage, perform data processing and analysis of data collection to determine the Capability Level so that you can identify Expected Capability, Current Capability and Gap.
5. Fifth Stage, evaluate the results of the analysis to develop a recommendation.
6. The last stage, making conclusions from all research activities and providing suggestions for further research.

4. RESULT AND DISCUSSION

4.1 Mapping of COBIT 5

The results of mapping Enterprise Goals produce four points, of which three points are included in the Customer Balance Scorecard (BSC), namely, Customer oriented service culture, Business service continuity and availability, Agile responses to a charging busines environment, and one point in BSC Learning and Growth, namely, Product and business innovation culture. The next step is to align IT goals with agency goals by mapping enterprise goals and IT-related Goals in accordance with COBIT 5.

The next step is to align IT goals with agency goals by mapping enterprise goals and IT-related Goals in accordance with COBIT 5. Mapping above alignment is achieved by identifying agency IT-related Goals derived from the agency's mission, namely, the realization of a healthy and independent community in the Kasihan II Health Center area. Based on this mission, the appropriate IT-related Goals are point 04 Managed IT-related business risk, point 07 Delivery of IT services in line with business requirements, point 09 IT agility, point 10 Security of information, processing infrastructure and applications, point 14 Availability of reliable and useful information for decision making.

The next step is to map the IT-related Goals to the COBIT 5 domain processes, specifically mapping with the alignment between both IT-related Goals with all the appropriate domain processes. The selected domain has a P (Primary) value, because the primary domain has a significant relationship to the achievement of IT goals. The process domain that is the focus of the formulation of this research problem is the APO12

(Manage Risk) domain, because other domains are not found to have an important relationship with existing IT-Related Goals.

4.2 Determination of Respondents

The RACI Chart is a management tool that details the roles and responsibilities of individuals or groups within a project. Its function is to provide a clear understanding to all parties involved, based on the person in charge at the Kasihan II Bantul auxiliary health center Table 7.

Table 7. Results of Determining Respondents APO12

No	Organizational Structure	ID
1.	Head of Service	R1
2.	Head of Basic and Traditional Health Services and Quality Development Section	R2
3.	Program Substance and Reporting Group Staff	R3
4.	Medical Record Officer of Kasihan II Bantul Health Center	R4
5.	Staff of Kasihan II Bantul Health Center	R5

4.3 Recapitulation of Questionnaire Responses

The recapitulation of APO12 (Risk Management) questionnaire responses is a process that involves careful data analysis, where the results are divided into six different subdomains, namely APO12.01 to APO12.06. The information presented in these recapitulated results is very detailed and granular, and all the details can be found in Table 8.

Table 8. Questionnaire Answer APO12.01

No	Status	Distribution of Answers (%)					
		0	1	2	3	4	5
1.	As is	0	0	0	40	40	20
	To be	0	0	0	20	0	80
2.	As is	0	0	0	20	60	20
	To be	0	0	0	0	0	100
3.	As is	0	0	0	40	40	20
	To be	0	0	0	0	0	100
4.	As is	0	0	0	60	20	20
	To be	0	0	0	20	0	100
5.	As is	0	0	0	60	20	20
	To be	0	0	0	20	0	80
6.	As is	0	0	0	40	40	20
	To be	0	0	0	0	0	100
7.	As is	0	0	0	20	60	20
	To be	0	0	0	0	0	100
8.	As is	0	0	0	40	40	20
	To be	0	0	0	0	0	10
9.	As is	0	0	0	40	40	20
	To be	0	0	0	0	0	100
10.	As is	0	0	0	40	40	20
	To be	0	0	0	0	0	100
11.	As is	0	0	0	40	40	20
	To be	0	0	0	0	0	100
12.	As is	0	0	0	40	60	0
	To be	0	0	0	0	0	100
13.	As is	0	0	0	40	20	40
	To be	0	0	0	0	0	100
14.	As is	0	0	0	60	20	20
	To be	0	0	0	0	20	80
15.	As is	0	0	0	60	20	20
	To be	0	0	0	0	20	80
Amount	As is	0	0	0	640	560	300
	To be	0	0	0	60	40	1330
Average	As is	0	0	0	42,67	37,33	20
	To be	0	0	0	4	2,67	88,67

Based on the information documented in Table 8, which is a recapitulation of the answers to Questionnaire APO12.01, it can be concluded that the majority of respondents gave an assessment of the current condition (as is). The results of this assessment indicate that the level of risk management is at level 3, with around 42.67% of the respondents giving an assessment at that level. Meanwhile, when looking at the expected conditions (to be), the majority of respondents anticipate that risk management will reach level 5, with around 88.67% of them predicting this. This shows that there is a fairly strong expectation from the relevant parties that risk management can be improved to a higher level in the future.

Table 9. Questionnaire Answer APO12.02

No	Status	Distribution of Answers (%)					
		0	1	2	3	4	5
1.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
2.	As is	0	0	0	40	60	0
	To be	0	0	0	0	40	80
3.	As is	0	0	0	60	20	20
	To be	0	0	0	0	20	80
4.	As is	0	0	0	40	40	20
	To be	0	0	0	0	40	80
5.	As is	0	0	0	60	20	20
	To be	0	0	0	0	40	60
6.	As is	0	0	0	40	40	20
	To be	0	0	0	0	40	80
7.	As is	0	0	0	80	0	20
	To be	0	0	0	0	40	60
8.	As is	0	0	0	60	20	20
	To be	0	0	0	0	20	80
9.	As is	0	0	0	60	20	20
	To be	0	0	0	0	20	80
10.	As is	0	0	0	60	20	20
	To be	0	0	0	0	20	80
11.	As is	0	0	0	60	20	20
	To be	0	0	0	0	20	80
12.	As is	0	0	0	60	20	20
	To be	0	0	0	0	20	80
Amount	As is	0	0	0	660	320	220
	To be	0	0	0	0	340	920
Average	As is	0	0	0	55	26,7	18,3
	To be	0	0	0	0	28,3	76,7

Based on the analysis contained in Table 9, it can be concluded that the majority of respondents provide a general assessment (as is) of risk management, where the level of satisfaction reaches level 3 with a proportion of 55%. Meanwhile, when referring to the expected conditions (to be), it can be seen that the majority of informants projected a risk management level of 5, and this was achieved with a percentage of around 76.7%. This result reflects a positive perception of expected improvements in risk management in the future, along with improvement efforts that may have been identified in the current assessment.

Based on Table 10 recapitulation of answers to Questionnaire APO12.03 that the majority of informants provide an assessment of the current condition (as is). The assessment results show that risk management is at level 4 with a percentage of 43.08%. As for the expected conditions (to be),

most informants estimate risk management to be at level 5 with a percentage of 80%.

Table 10. Questionnaire Answer APO12.03

No	Status	Distribution of Answers (%)					
		0	1	2	3	4	5
1.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
2.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
3.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
4.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
5.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
6.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
7.	As is	0	0	0	40	60	00
	To be	0	0	0	0	20	80
8.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
9.	As is	0	0	0	20	60	20
	To be	0	0	0	0	20	80
10.	As is	0	0	20	20	40	20
	To be	0	0	0	0	20	80
11.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
12.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
13.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
Amount	As is	0	0	20	480	560	240
	To be	0	0	0	0	260	1040
Average	As is	0	0	1,54	36,92	43,08	18,46
	To be	0	0	0	0	20	80

Table 11. Questionnaire Answer APO12.04

No	Status	Distribution of Answers (%)					
		0	1	2	3	4	5
1.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
2.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
3.	As is	0	0	0	60	20	20
	To be	0	0	0	0	20	80
4.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
5.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
Amount	As is	0	0	0	220	180	100
	To be	0	0	0	0	100	400
Average	As is	0	0	0	44	36	20
	To be	0	0	0	0	20	80

Based on the analysis conducted on Table 11, which is a recapitulation of the answers to the APO12.04 questionnaire, it can be concluded that the majority of respondents provide an assessment of the current conditions in accordance with the existing reality. The data shows that the current level of risk management is at level 3, with a percentage of 44%. Meanwhile, when referring to the expected conditions (to be), it can be seen that the majority of respondents tend to give a more positive assessment of risk management, with most assessing that the level is at level 5, reaching a percentage of 80%.

Table 12. Questionnaire Answer APO12.05

No	Status	Distribution of Answers (%)					
		0	1	2	3	4	5
1.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
2.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
3.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
4.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
5.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
Amount	As is	0	0	0	200	200	100
	To be	0	0	0	0	100	400
Average	As is	0	0	0	40	40	200
	To be	0	0	0	0	20	80

Based on Table 12 recapitulation of answers to Questionnaire APO12.05 that the majority of informants provide an assessment of the current condition (as is). The assessment results show that risk management is at level 3 with a percentage of 40%. As for the expected conditions (to be), most informants estimate risk management to be at level 5 with a percentage of 80%.

Table 13. Questionnaire Answer APO12.06

No	Status	Distribution of Answers (%)					
		0	1	2	3	4	5
1.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
2.	As is	0	0	0	60	20	20
	To be	0	0	0	0	40	60
3.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
4.	As is	0	0	0	20	60	20
	To be	0	0	0	0	20	80
5.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
6.	As is	0	0	0	40	40	20
	To be	0	0	0	0	20	80
Amount	As is	0	0	0	240	240	120
	To be	0	0	0	0	140	460
Average	As is	0	0	0	40	40	20
	To be	0	0	0	0	23,33	76,67

Based on the analysis contained in Table 13, the recapitulation of the answers to the APO12.06 questionnaire indicates that the majority of respondents provide an assessment of the current conditions with reference to the actual situation (as is). The assessment results show that risk management is placed at level 3, reaching a percentage of 40%, while at level 4 the percentage is also 40%. Meanwhile, when detailing expectations related to the desired condition (to be), most respondents tend to assess that risk management should be at level 5, with a percentage reaching 76.67%. Thus, it can be concluded that there are differences in perceptions between current conditions and desired expectations regarding risk management according to respondents' responses.

4.4 Determination of Capability Level

In this section, the determination of the APO12 capability level is based on the results of the calculation of the capability value recorded in each subprocess, as shown in Table 14 regarding the determination of the APO12 capability level.

Table 14. Determination of Capability Level APO12

No	Subdomain	Capability Value		Capability Level	
		As is	To be	As is	To be
1	APO12.01	3,77	4,66	4	5
2	APO12.02	3,63	4,97	4	5
3	APO12.03	3,78	4,80	4	5
4	APO12.04	3,76	4,80	4	5
5	APO12.05	3,80	4,80	4	5
6	APO12.06	3,80	4,77	4	5
Average		3,76	4,80	4	5

The APO12 process in the current condition (As is) is at level 4 (Predictable Process), while in the expected condition (To be) is at level 5 (Optimizing Process), it can be seen in Figure 6 of the APO12 process graph as follows.

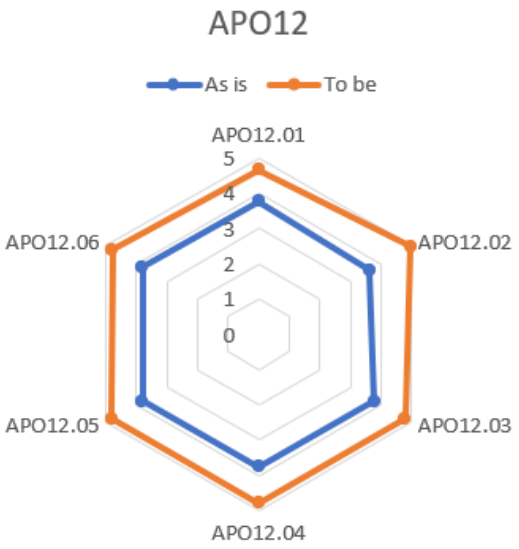


Figure 6. APO12 Process Graphics

4.5 Gap and Recommendations

In this section, the results of the calculation of the gap value of the APO12 process (manage risk) are taken from the results of the questionnaire and the analysis is carried out based on the comparison of the expected capability level value of the Kasihan II Bantul Health Center DGS with the current capability level value, as shown in Table 15.

Table 15. Gap APO12

No	Subdomain	Capability Level	
		As Is	To Be
1.	APO12.01	4	5
2.	APO12.02	4	5
3.	APO12.03	4	5
4.	APO12.04	4	5
5.	APO12.05	4	5
6.	APO12.06	4	5
Gap		1	

In Table 15, the gap value of the APO12 process is 1. The current condition is at level 4, while the goal is to reach level 5. From this difference, it can be concluded that DGS Health must make improvements to the APO12 process in order to reach the expected level. To achieve this level of capability, recommendations are made based on the results of the achievement of the APO12 process so that the recommendations provided are in accordance with the current needs of the agency.

Table 16. Recommendation APO12

No	Recommendations
1.	Create a process plan for IT risk management that includes information on process performance goals.
2.	Establish an appropriate and organized framework for the management of Health DGS.
3.	Create documentation for IT risk management processes that includes information about respondents (RACI).
4.	Conduct risk assessments in cooperation with third parties to ensure continuous observation.
5.	Implement an appropriate and efficient monitoring and evaluation system to improve performance and align it with organizational goals.
6.	Ensure the performance monitoring process is properly and efficiently executed to meet the set performance targets.
7.	Improve the performance monitoring and evaluation process to make better judgments, increase productivity, and meet set performance targets.

Based on the information in Table 16 above, recommendations were developed to address the issues facing DGS Health. This allows the agency to implement the recommendations and improve services and risk management while preventing future hazards that could jeopardize the agency.

5. CONCLUSION

From the results of this study can be drawn conclusions, Based on the results of the assessment of the capability level of APO12 (Risk Management) Puskesmas Kasihan II Bantul shows that the current condition is at level 4 (Predictable Process), with a value of 3.76. Furthermore, at a value of 4.80 the expected condition capability level reaches level 5 (Optimized Process), and obtains a gap of one. Based on the gap findings, recommendations are made as shown in Table 4.36 to achieve the desired level and manage risks based on the results of the APO12 process.

6. REFERENCES

[1] A. Ambarwati, C. Darujati, and Jonny, “Risk Assessment of Health Center and Asset Management Information System Data Using ISO27005,” 2020.

[2] J. K. Sitinjak, I. A. Fajar, and R. Hanafi, “Assessment of the Implementation of IT Governance Processes Using COBIT Version 5 in the BAI Domain for IPOS Case Study Application Development at PT. POS Indonesia,” Agustus, vol. 2, no. 2, p. 5334, 2015.

[3] R. Gunawan, Y. Suherman, and N. Z. Auliya, “Design of a Web-based Goods Procurement Information System at PT. Sintas Kurama Perdana Karawang,” vol. 14, no. 1, pp. 101–113, 2021, [Online]. Available: http://journal.stekom.ac.id/index.php/E-Bisnis

[4] P. P. Bandung, L. Emalia, and G. Sausan, “Design of a Web-Based Print Ordering Information System Using Laravel at Hd Card Bandung,” 2022.

[5] S. F. Bhaskoro, "Risk Assessment Analysis of the Presence Information System Using the COBIT 5 Framework," 2022.

[6] D. Agustina, F. Nazzilla Pramadista, and T. Fara Regyna, "Information Security Management System," 2022.

[7] Indriyanto, "Risk Assessment Analysis of the Stock Information System Using the COBIT 5 Framework," 2021.

[8] E. Zuraidah and C. Budihartanti, "Audit of information systems and management using COBIT 4 and 5," 2021.

[9] R. Astuti, "Implementation of Information Systems Risk Management Using COBIT 5," 2018.

[10] G. W. Lantang, A. D. Cahyono, and M. N. N. Sitokdana, "Information Technology Risk Analysis on SAP Applications at PT Serasi Autoraya Using ISO 31000," 2019, doi: 10.46984/sebatik.v23i1.441.

[11] Sungadi, "Information Security and Library Risk Management," 2020.

[12] S. Sugiyanto, D. P. Arum, and A. A. Rahayu, "Implementation and Formulation of Risk Management Strategies in the Dairy Cattle Business Unit and Milk Production of Kud Sarwa Mukti," Jurnal Soshum Insentif, vol. 4, no. 1, pp. 79–88, Apr. 2021, doi: 10.36787/jsi.v4i1.514.

[13] T. Nurdiansyah and M. Hendayun, "Analysis and Implementation of Risk Management of Monitoring Applications and Information Security Management Systems Using SNI ISO / IEC 27001: 2013 (Case Study: KPID West Java)," 2022.

[14] Maulana and Supangkat, Modeling Information Technology Risk Management Framework for Companies in Developing Countries, 2006.

[15] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Risk Management Analysis Using ISO 31000 at Smart Canteen SMA XYZ," Journal of Computer Research, vol. 7, no. 1, p. 91, Feb. 2020, doi: 10.30865/jurikom.v7i1.1791.

[16] M. I. Fachrezi, A. Dwika Cahyono, and P. F. Tanaem, "Information Technology Asset Security Risk Management Using ISO 31000:2018 Salatiga City Diskominfo," Information Systems Department, vol. 8, no. 2, 2021.

[17] M. F. A. Nazir and M. N. H. Ryandono, "Operational Risk Management at the National Amil Zakat Institution," Journal of Islamic Economics Theory and Application, vol. 6, Nov. 2019.

[18] ISACA, Enabling Processes, vol. b. Rolling Meadows, 2012.

[19] ISACA, COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT, vol. a. Rolling Meadows, 2012.

[20] D. Rohmatulloh, "Evaluation of the Hospital Management Information System (SIMRS) at Rsu Kaliwates Jember Using COBIT 5 Domain DSS (Deliver, Sevice, Support)," Jember, 2019.

[21] R. Abdul Aziz, Kusrini, and Sudarmawan, "Evaluation of Information Technology Risk Management in State-Owned Companies Using COBIT 5 Standards (Case Study: PT TASPEN PERSERO)," Jurnal IT CIDA, vol. 4, no. 2, 2018.

[22] N. S. F. M. Messakh and A. R. Tanaamah, "Analysis of Information Systems Based on Cobit 5 (Case Study: LTC UKSW)," vol. 8, no. 1, 2021, [Online]. Available: http://jurnal.mdp.ac.id

[23] ISACA, COBIT5: Implementation. Rolling Meadows, 2012.

[24] ISACA, Process Assessment Model (PAM): Using COBIT 5. Rolling Meadows, 2013.

[25] ISACA, COBIT5 Self Assessment Guide Using COBIT. Rolling Meadows, 2013.