Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 8, No. 1, February, Pp. 435-444

Risk management using COBIT 5 for risk: a case study on local government in Indonesia

Beny Prasetyo*[1], Lailatul Qomariah[1], Windi Eka Yulia Retnani[2]
Department of Information Systems, Faculty of Computer Science, University of Jember, Indonesia[1]
Department of Informatics, Faculty of Computer Science, University of Jember, Indonesia[2]

Article Info
Keywords:
BP4D Bondowoso, implementation SIPD, risk management, COBIT 5 Enabling Process, COBIT 5 for Risk

Article history:
Received: November 06, 2022
Accepted: January 01, 2023
Published: February 28, 2023

Cite:
B. Prasetyo, L. Q. Toha, and W. E. . Yulia Retnani, "Risk Management using COBIT 5 for Risk : A Case Study on Local Government in Indonesia", KINETIK, vol. 8, no. 1, Feb. 2023.
https://doi.org/10.22219/kinetik.v8i1.1585

*Corresponding author.
Beny Prasetyo
E-mail address:
beny.pssi@unej.ac.id

Abstract
BP4D (Regional Development Planning, Research and Development Agency) Bondowoso utilizes information technology to support its duties and functions, one of which is SIPD (Sistem Informasi Pemerintah Daerah). SIPD provides many benefits and conveniences such as improving the quality of public services, transparency, improving bureaucratic accountability, but in its implementation SIPD can also pose dangerous risks both from processes involving the system and the system itself. These risks can disrupt BP4D Bondowoso's business processes and cause various losses. To protect BP4D Bondowoso from losses caused by risk, risk management is carried out using the relevant framework, namely COBIT 5 Enabling Process and COBIT 5 for Risk with the APO12 risk management process. Data were collected by interview and distributing questionnaires. Fifty-one risks were identified in the implementation of SIPD at BP4D Bondowoso consisting of 48 negative risks and 3 positive risks. The risks found dominate the type of IT Benefit / Value Enablement and the category of regulatory compliance. Identified 3 very high risks in the category of regulatory compliance and software. Overall risk dominates the medium rating, which is 28 risks and the high risk consists of 20 risks. The negative risk response is dominated by mitigate, which is 33 risks.

1. Introduction

BP4D (Regional Research and Development Planning Agency) is an SKPD (Regional Apparatus Work Unit) which is also a regional government agency, where its existence is part of government support in the field of development planning [1]. BP4D is an important function and strategy, because with research and planning it can be known where the regional goals will be taken [2]. To carry out its roles and obligations, BP4D Bondowoso utilizes information technology, one of which is SIPD (*Sistem Informasi Pemerintah Daerah*). SIPD is an integrated system part of the Regional Government Information System launched by the Ministry of Home Affairs in 2019 based on the 2019 Minister of Home Affairs Regulation Number 70 concerning Regional Government Information Systems [3]. SIPD must be used by local governments, some of which are Bondowoso Regional Government, Bondowoso BP4D as OPD (Local Apparatus Organization) and TAPD (Local Government Budget Team) to manage regional development planning as stated in [4]. SIPD is a complex system and has an important role in business processes at BP4D Bondowoso, namely as a means of connecting information to the central government, regulating regional development planning, budgeting regional development funds, so that it can pose a dangerous risk from the system or process activities involving the system. Based on the Minister of Home Affairs Regulation Number 8 of 2014 SIPD is managed by the Regent/Mayor through the district/city BP4D [5].

SIPD is related to the management of data or information on regional development planning which includes the potential of regional resources, both human and natural, regional finance, the economy in general, with the purpose of optimizing, improving the value, effectiveness, efficiency of the regional development planning process [6][7]. SIPD provides many benefits and conveniences such as improving the quality of public services, transparency, improving public services and making accurate decisions [8]. However, in its application, in addition to providing benefits, the use of SIPD also produces risks events [9]. Risk is a deviation from something expected or the influence of the uncertainty of a goal that can have a positive or negative effect negative [10][11][12]. These risks can disrupt BP4D Bondowoso's business processes and cause various losses. Based on pre-research interviews, one of the potential risks that can occur in SIPD BP4D Bondowoso is delays in scheduling or verification of regional development planning which can cause delays in the formation of local government work plans or called *Rencana Kerja Pemerintah Daerah* (RKPD), general budget policies, provisional budget priorities and funding levels and even Regional Revenues and Expenditures Budget. BP4D has not carried out in-depth risk identification, assessment and management of risks related to the implementation of the use of the SIPD system.

To protect BP4D Bondowoso from losses due to SIPD risks, both financial and disruption to business processes, risk management can be carried out. Risk management is a very important aspect of information systems and their development [13]. In this study, two methods were used, namely COBIT 5 for Risk and COBIT 5 Enabling Process to carry out a risk management analysis based on the SIPD business process. COBIT 5 Enabling Process is used to guide SIPD BP4D Bondowoso risk management analysis, the domain to be used is APO (Align, Plan and Organize) in key management APO12 Manage Risk, and is used as a basis for compiling risk mitigation steps recommended by researchers. While COBIT 5 for Risk is used as risk management related to the rules for identifying, analyzing, and responding to risks. Researchers use COBIT 5 for Risk and COBIT 5 Enabling Process as a framework in this study because it can be applied in various types of organizations, has been implemented in various organizations globally, and can be used to evaluate risk management information systems according to needs [14][15]. In addition, the reason researchers use COBIT 5 is because the process in it is very complex, so that it allows holistic management of information technology for the entire company, is able to align IT with existing business processes, and can improve IT governance. [16][17].

It is important to know the business processes in the implementation of SIPD BP4D Bondowoso. This is because the risk analysis departs from the existing activities in the SIPD BP4D Bondowoso business process. This research is only conducted on the function of the annual RKPD in SIPD. Data collection in this study was conducted by conducting semi-structured interviews accompanied by an interview protocol and distributing questionnaires. The purpose of this study was to determine the results of a risk analysis consisting of the risks contained in the SIPD BP4D Bondowoso, the results of a risk assessment, a risk mapping, and a risk response based on COBIT 5 for Risk.

2. Research Method

Risk management in the implementation of SIPD BP4D Bondowoso is part of information technology (IT) risk management. In the context of IT risk management, it is the process of identifying, conducting risk assessments, as well as the process of finding and developing IT risk mitigations such as transfer, avoidance, or mitigation in accordance with the enterprise's risk appetite, accompanied by the preparation of communication strategies that have the potential to harm the organization [18][19][20]. NIST (National Institute of Standards and Technology) defines information technology risk management as a process consisting of risk assessment which is a stage to identify risks and look for possible impacts in order to find appropriate mitigation or handling steps, then risk mitigation, which is the stage to provide prioritizing the magnitude level caused by risk is followed by evaluating the causes and impacts of risk accompanied by the application of appropriate monitoring to address known risks and impacts on the risk process, the last process is evaluation and assessment which is the stage to follow up risk evaluation by providing best practice for successful risk management [21]. COBIT 5 for Risk provides specific guidance regarding all effective enablers for risk management from two perspectives, namely risk function and risk management. The risk function perspective discusses what is needed by the company to determine the risk function. The risk management perspective examines how the core risk management process starts with identifying, analyzing, and handling or responding to a risk. This study uses a risk management perspective because it examines how the core risk management process starts with identifying, analyzing, and deciding how to handle or respond to a risk. In its implementation, the risk management perspective must be equipped with a core risk process, one of which is APO12 Manage Risk [22].

APO12 Manage Risk is one of the subdomains or processes in the APO domain that helps in managing risk and mitigating or handling information technology risks because the activities and processes involved are very complex, starting from identifying ongoing risks, assessing them, and reducing risks related to information technology at a level that is defined and acceptable to all stakeholders, especially executives of the company or organization [16][22]. APO12 manage risk has several activity processes, namely APO12.01 collect data, APO12.02 analyze risk, APO12.03 maintain risk profile, APO12.04 articulate risk, APO12.05 define a risk management action portfolio, APO12.06 respond to risk [16]. APO12 activities that will be carried out only on APO12.01 to APO12.02 because this research has not yet reached the stage of evaluation, monitoring, and updating risk management. The design of this research phase is adapted to the activities of the APO12 process to manage risk. The following are the phases used for SIPD risk management:

2.1 Needs Initiation Phase

This phase begins with conducting interviews in the Regional Development Planning, Controlling, and Evaluation division to find out the latest conditions and explore the problems that exist in BP4D Bondowoso. Then conduct a literature study to understand the concept of risk management based on COBIT 5 for Risk and COBIT 5 Enabling Process.

2.2 Collect Data Phase

This phase is part of a series of activities from APO12.01, which is a meaningful data collection process that allows to identify, analyze and report IT risks efficiently [16][23]. Activities carried out at this phase are data collection, which includes identifying the duties and functions of BP4D Bondowoso related to SIPD, mapping the current SIPD

business process conditions, analyzing the risks that may occur from each business process activity, determining the types and categories of risk, and an analysis of risk factors. Data were obtained from interviews with experts in the Regional Development Planning, Control, and Evaluation division and the head of BP4D.

2.3 Risk Analysis Phase

This phase is a series of activities from APO12.02, namely the process of increasing the use of information in order to support and take into account the linkage of risk factors with business and decision making [16]. The activities carried out at this stage are the creation of risk scenarios, impact analysis, risk frequency, risk assessment, determination of risk mitigation responses, risk mapping to the COBIT 5 Enabling Process and analysis of risk mitigation measures. Scenario development, impact analysis, and risk frequency were obtained through interviews with experts in the Regional Development Planning, Control and Evaluation division, the head of BP4D, and distributing questionnaires to all BP4D employees to obtain risk impact data based on aspects of competitive advantage.

To determine the impact and frequency of risk, the range and rating provided by COBIT 5 for Risk is required. Using the range and rating provided by COBIT 5 for Risk because the organization does not yet have a range and rating that is adapted to its organizational conditions, and this has been discussed with BP4D sources. Based on COBIT 5 for Risk, the impact of risk is viewed from four aspects, namely Productivity (financial loss), Cost of Response (response costs to deal with risk), Competitive Advantage (decreased user satisfaction), Legal (Regulatory Compliance — Fines). For the period used in this study, since the implementation of SIPD at BP4D Bondowoso. This is because the annual RKPD planning is carried out once a year. The rating used is 0-5, following in Table 1 is the range and rating used to measure the impact of risk based on COBIT 5 for Risk [22].

Table 1. Impact Range and Rating

Impact rating	Productivity range	Cost of response range	Competitive advantage range	Legal range	Description
0	I ≤ 0,1%	I ≤ IDR 149 million	I ≤ 0,5	No loss from legal aspect	Very low
1	0,1% < I ≤ 1%	IDR 149 million < I ≤ IDR 1.49 billion	0,5 < I ≤ 1	I < IDR 14.9 billion	Low
2	1% < I ≤ 3%	IDR 1.49 billion < I ≤ IDR 14.9 billion	1 < I ≤ 1,5	I < IDR 149 billion	Medium low
3	3% < I ≤ 5%	IDR 14.9 billion < I ≤ IDR 149 billion	1,5 < I ≤ 2	I < IDR 1.49 trillion	Medium high
4	5% < I≤ 10%	IDR 149 billion < I ≤ Rp 1.49 trillion	2 < I ≤ 2,5	I < IDR 14.9 trillion	High
5	I > 10%	I > Rp 1.49 trillion	2,5 > I	I > IDR 14.9 trillion	Very high

The frequency of risk is the number of risks that have occurred in the period since the implementation of SIPD at BP4D Bondowoso. The following in Table 2 is the range and frequency rating used to determine the frequency of risk based on COBIT 5 for Risk [22].

Table 2. Frequency Range and Rating

Frequency rating	Frequency	Description
0	N ≤ 0,01	Very low
1	0,01 < N	Low
2	0,1 < N ≤ 1	Medium low
3	1 < N ≤ 10	Medium high
4	10 < N ≤ 100	High
5	N > 100	Very high

In carrying out a risk assessment, a risk map is also needed to determine the level of risk. This study uses a risk map that has been provided by COBIT 5 for Risk. There are four ratings or levels given on the risk map, namely very high (marked in red), high (marked in yellow), medium (marked in green), and low (marked in blue). The following in Figure 1 is the risk map used in this study [22].

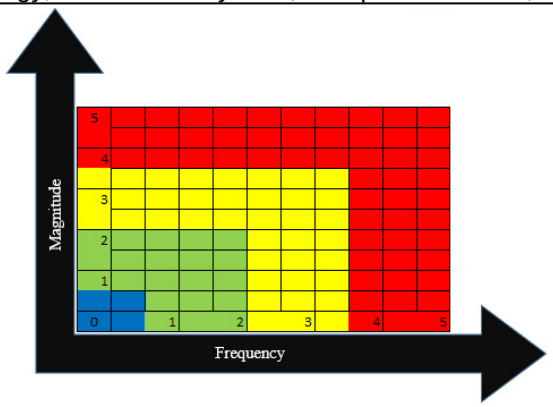

Figure 1. Risk Map

3. Results and Discussion

In this section, the results obtained during the research will be presented along with a discussion or explanation. The results and discussion are based on research methods that have been made previously. The following are the results and discussion of the research.

3.1 Result of the Needs Initiation Phase

In this phase, it was found that BP4D uses several applications to support its duties and functions, one of which is SIPD. The expert in the Regional Development Planning, Control, and Evaluation division said that the system that has an important role in business processes at BP4D Bondowoso is SIPD because it relates to the budget that will be obtained by the regions as well as planning other activities. SIPD has several potential risks that can occur, namely delays in scheduling or verifying regional development planning, which can cause delays in the formation of the RKPD, general budget policies, provisional budget priorities and funding levels, and even the regional revenues and expenditures budget. Although it has the potential to pose a risk, SIPD risk has never been identified and documented. The expert said that the risks that occurred in SIPD were only recorded in the system itself. SIPD also has the potential to experience problems when a system update occurs, namely losing old data, uploading data that is not stored, and data changing places.

3.2 Result of Collect Data Phase

Based on Bondowoso Regent Regulation Number 116 of 2021, and Bondowoso Regent's Decree Number 1178 of 2021 it shows that all employees at BP4D Bondowoso use SIPD in the context of planning the annual RKPD with different access rights, including as Head of BP4D TAPD, Head of Division, Operator (staff), and BP4D Partners (staff BP4D). The scope of this research is only on the implementation of SIPD at BP4D Bondowoso in the context of the annual RKPD planning, so to carry out a risk analysis, the SIPD implementation business process must first be determined. So that in BP4D there are no other parties who do not communicate directly with SIPD but can be exposed to risk. Based on the interviews, the SIPD business process has two functions, namely the function of the head of the BP4D TAPD and the function of BP4D as the OPD. After obtaining the SIPD business process, it is followed by a risk analysis for each activity carried out by BP4D and involving the SIPD system in the framework of the annual RKPD planning. Risk analysis is carried out based on Permendagri Number 86 of 2017, where one of the contents discusses the RKPD [24]. Then confirmation regarding the risk analysis in the Rendalev field and the head of BP4D was carried out.

Based on the risk analysis on several business activities of the SIPD BP4D process, the OPD and TAPD functions there are 51 risks with 48 negative risks and 3 positive risks. The risks that arise from the function of BP4D as an OPD also come from other OPDs throughout Bondowoso Regency. This is because other OPDs have more problems that affect the performance of BP4D as TAPD. The following in Table 3 is an example of the risks found.

Table 3. Example of the Result of SIPD BP4D Bondowoso Risk Analysis

Activity	Risk ID	Negative Risk	Risk ID	Positive Risk
Determination of the planning schedule for the	R01	Delay in setting development priorities in December	R49	The head of BP4D sets the initial design planning schedule at the beginning of

Activity	Risk ID	Negative Risk	Risk ID	Positive Risk
initial draft local government work plan by the Head of BP4D (Function of BP4D TAPD)	R02	There is an excess of the initial design planning schedule for the local government work plan which is more than the 2nd week of February		the time, namely in December the 3rd or 4th week
	R03	The planning schedule for the initial draft local government work plan that was opened had very little time		

Each risk that has been obtained previously, then the type of risk is determined based on the importance of the type of scenario (impact) and the risk itself. Based on COBIT 5 for Risk, the following are the types of risk [22].

a. IT benefit / value enablement risk (TP I): if the risk is related to opportunities (lost) in using IT as a tool or facility (enabler) to improve business solutions, this column type is filled with “P” otherwise it is filled with “S”.
b. IT program and project delivery risk (TP II): if the risk is related to IT programs and projects that are part of the portfolio then this type is filled with "P" but if not filled with "S".
c. IT operations and service delivery risk (TP III): if the risk is related to the availability of IT services, service interruptions and other IT service operations, this type is filled with “P”, but if not filled with “S”.

"P" is the primer used to express the type of risk at a higher level. "S", which is secondary, is used to indicate a lower risk type. In this study, 44 risks were generated with TP I, namely IT Benefit / Value Enablement because the risk is related to lost opportunities in using IT as a tool or facility (enabler) and business improvement, so that the risk is primary (P). There are 7 risks with TP III namely IT Operations and Service Delivery because the risk is related to the availability of IT services and service disruptions, so that the risk is primary (P). BP4D OPD and TAPD functions do not produce IT programs or projects, so TP II is filled with "S" (Secondary).

After analyzing the type of risk, then the risk category mapping analysis is carried out based on the categories that have been provided and determined by COBIT 5 for Risk. There are 20 categories provided by COBIT 5 for Risk, some of which are regulatory compliance, software, environmental, and staff operations (human error and malicious intent) [22]. Based on the results of the mapping of risk categories in this study, it can be seen that most risks are mapped to the regulatory compliance category, which is 29 risks. The category of regulatory compliance relates to regulations that apply within the organization. There are 9 mapped environmental related risks, where environmental relates to the environment or conditions that are being experienced by the organization. The risk categories related to staff operations (human error and malicious intent) are 6 risks. The risk categories related to software are mapped to as many as 7 risks, which means that the risk is software failure. The type and risk category were determined through interviews with experts in the Regional Development Planning, Control and Evaluation division and the head of BP4D.

After categorization, it is followed by an analysis of the causes and risk factors from both the external and internal contexts of BP4D obtained from the interview process. Internal risk factors are generally under the company's supervision and control, although organizational conditions may be inconsistent and changeable. While external factors are generally outside the company's supervision and control. Internal and external factors are adjusted or grouped based on the risk factors provided by COBIT 5 for Risk [22]. The following in Table 4 are examples of the results of types, categories and risk factors.

Table 4. Example of the Result of the Types, Categories and Risk Factors

Risk ID	Risk	Risk Type			Category	Risk Factor	
		TP I	TP II	TP III		Internal	External
R01	Delay in setting development priorities in December	P	S	S	Regulatory compliance	Enterprise goals and objectives – a solid agenda related to the goals and objectives of the organization	-
R02	There is an excess of the initial design planning	P	S	S	Regulatory compliance	-	Regulatory environment - OPD's

Risk ID	Risk	Risk Type			Category	Risk Factor	
		TP I	TP II	TP III		Internal	External
	schedule for the local government work plan which is more than the 2nd week of February						delay in preparing the initial draft local government work plan, so BP4D grants time extension
R03	The planning schedule for the initial draft local government work plan that was opened had very little time	P	S	S	Environmental	Complexity of IT - Server down due to overload, system maintenance	Threat landscape - Weak network
R49	The head of BP4D sets the initial design planning schedule at the beginning of the time, namely in December the 3rd or 4th week	P	S	S	Regulatory compliance	-	Regulatory environment - Permendagri 86 of 2017

3.3 Result of Risk Analysis Phase

This phase begins with the creation of a risk scenario. Risk scenarios are divided into two, namely positive scenarios and negative scenarios. A positive scenario can be interpreted as having a positive or good impact if the possibility of risk does not occur, thus describing an optimal and smooth business process. While the negative scenario is a bad impact that can occur due to risk, resulting in obstacles to business processes[22]. The following Table 5 is an example of a risk scenario in this study.

Table 5. Example of Determining Risk Scenario

Risk ID	Risk	Risk Scenario	
		Positive	Negative
R01	Delay in setting development priorities in December	In accordance with Permendagri 86 of 2017, all OPD, Villages and DPR can properly prepare activity proposals according to development priorities	Inhibiting the determination of the planning schedule for the initial draft local government work plan and narrowing the opening of the planning schedule for the initial draft local government work plan
R02	There is an excess of the initial design planning schedule for the local government work plan which is more than the 2nd week of February	In accordance with Permendagri 86 of 2017, all OPD can prepare the initial draft local government work plan on time	Inhibiting the setting of the design planning schedule and narrowing the opening of the design planning schedule
R03	The planning schedule for the initial draft local government work plan that was opened had very little time	OPD has more time to prepare as well as input data for planning the initial draft of the local government work plan	OPD has limited time to prepare and input data for planning the initial draft local government work plan
R49	The head of BP4D sets the initial design planning schedule at the beginning of the time, namely in December the 3rd or 4th week	Delay in the preparation of the initial draft of the RKPD	The initial RKPD draft was prepared on time

After analyzing the risk scenario, a risk impact analysis is carried out based on each aspect. Then an analysis of risk frequency was carried out, so that 20 risks were found to have a low rating, 10 risks at a medium low rating, 18 risks at a medium high rating, and 3 risks at a high rating. Then proceed to the assessment of each risk item to determine the level of risk. Furthermore, a risk assessment is carried out based on COBIT 5 for Risk in terms of frequency data (probability), risk impact, and risk maps. Table 6 below is an example of the results of a risk assessment. The impact of risk results from calculating the average rating on four aspects, namely Productivity, Cost of Response, Competitive Advantage and Legal [22].

Table 6. Example of Risk Assessment

Risk ID	Risk	Frequency	Risk impact (average)	Risk level
R01	Delay in setting development priorities in December	2	1.75	Medium
R02	There is an excess of the initial design planning schedule for the local government work plan which is more than the 2nd week of February	2	1.75	Medium
R03	The planning schedule for the initial draft local government work plan that was opened had very little time	3	1,74	High
R49	The head of BP4D sets the initial design planning schedule at the beginning of the time, namely in December the 3rd or 4th week	2	1.75	Medium

The result of the risk assessment of this research is that the risk that occupies a very high level comes from the regulatory compliance category, which has 2 risks, and 1 risk comes from the software category. There are 28 risks occupying the medium level, which are dominated by the regulatory compliance category, namely 19 risks, 5 risks from the staff operations category (human error and malicious intent), 2 risks in the environmental category, and 2 risks in the software category. Risks that occupy a high level are 8 risks in the regulatory compliance category, 7 risks in the environmental category, 4 risks in the software category, and 1 risk in the staff operations category (human error and malicious intent). In this study, risks that are rated very high tend to occur frequently or have a high frequency, and have a significant adverse or beneficial impact. So that risks at a very high rating are a top priority for risk response and continue at a high rating, then medium. After conducting a risk assessment, continue to respond to risks. Based on COBIT 5 for Risk, to determine the risk response, consider the following three things [22] :

1. Exposure, which is how important the risk will be to respond, is represented or described by its position on the risk map (which describes the combined frequency and level of impact).
2. The company's ability to implement the response, As the company matures in its risk management process, more sophisticated responses can be applied, but when the company is somewhat immature, it may be better to start with some basic responses.
3. The effectiveness of the response, namely the extent to which the response will reduce the impact and magnitude of the risk.

Based on COBIT 5 for Risk [22] there are several strategies or risk responses that can be applied by organizations for negative risks including:

a. Risk Acceptance, acceptance of risk means that the risk of loss is accepted, no action is taken.
b. Risk Sharing / Transfer, which means minimizing the probability of risk impact frequency by transferring or sharing some of the risk with other parties.
c. Risk Mitigation, means that risk management measures are implemented to minimize failure, frequency and/or risk.
d. Risk Avoidance, namely exiting or refusing to engage in activities or conditions that cause risk.

To respond to a positive risk can be done with the following strategies [25] :

a. Exploit, which is done by creating opportunities that are sure to occur and eliminating all uncertainties.
b. Share, namely sharing positive risks by involving the allocation of ownership to third parties who are best able to handle risks, both in terms of maximizing the possibility of occurrence and in increasing the potential benefits if the risk occurs.
c. Enhance, namely a strategy to respond to risk by changing the size or size of the risk to make it more acceptable.
d. Ignore, is a response strategy by ignoring the positive risks that may occur.

The following in Table 7 is an example of the results of determining the response to risk.

Table 7. Example of Risk Response

Risk ID	Risk	Response
R01	Delay in setting development priorities in December	Mitigate
R02	There is an excess of the initial design planning schedule for the local government work plan which is more than the 2nd week of February	Mitigate
R03	The planning schedule for the initial draft local government work plan that was opened had very little time	Mitigate
R49	The head of BP4D sets the initial design planning schedule at the beginning of the time, namely in December the 3rd or 4th week	Enhance

In the case of negative risk, the risk response is dominated by mitigation, namely 33 risks. There are 8 negative risks with a transfer response, 5 risks with an acceptance response, and 2 risks with an avoidance response. Then for positive risks, 2 risks are responded to with exploit and 1 risk is to enhance response. Mitigation responses are widely applied because it allows BP4D to make efforts to deal with or prevent risks from occurring. The transfer response is implemented because the risk is related to third parties, such as other OPDs, and the central SIPD responsible person who is more likely to handle the risks that occur. It should be noted that the validation in this study was carried out by re-confirming the data that had been obtained from the person source and signed by the person source or expert.

4. Conclusion

This risk management is carried out to protect BP4D Bondowoso from losses caused by SIPD risks, both financial and disruption to its business processes. So that in this study identified 51 risks of SIPD implementation at BP4D Bondowoso consisting of 49 negative risks and 3 positive risks. The identified risks are dominated by the types of IT Benefit / Value Enablement and regulatory compliance categories. This is because the risks that arise are related to missed opportunities in utilizing IT as an enabler to improve business solutions and compliance with existing regulations. Based on the risk assessment carried out, the identified risk dominates the medium rating, with as many as 28 risks and the most categories coming from regulatory compliance. Risks with a high rating consist of 20 risks, with the most in the regulatory compliance category. Identified 3 very high rated risks in the categories of regulatory compliance and software. The majority of negative risks were responded to by being mitigated, namely 33 risks. Then for positive risks, 2 risks are responded to with exploit and 1 risk is to enhance response. It is hoped that further research can do this evaluation of implemented risks and take further action so that it is necessary to use all activities in APO12 to manage risk, namely APO12.01 – APO12.06. Due to time constraints, the scope of the research is limited to the implementation of SIPD in the framework of annual RKPD planning. Future research is expected to be able to explore the quality of the proposals in the framework of annual RKPD planning.

Notation

The following is a description of the notation used:

I : losses caused by risk based on the risk impact aspect.
N : frequency of risk within a certain time span.
APO : Align, Plan and Organize
RKPD : local government work plans or called *Rencana Kerja Pemerintah Daerah*
BP4D : Regional Development Planning, Research and Development Agency
SIPD : Sistem Informasi Pemerintah Daerah
OPD : Local Apparatus Organization
TAPD : Local Government Budget Team
TP I : IT benefit / value enablement risk
TP II : IT program and project delivery risk
TP III : IT operations and service delivery risk
NIST : National Institute of Standards and Technology

Acknowledgement

The researcher would like to thank all parties of BP4D Bondowoso which is the place for the research, supervisors and examiners who have been willing to provide guidance, suggestions in the series of this thesis research. Hopefully this research can make a major contribution to the risk management process for all parties involved and various organizations in Indonesia.

References

[1] Z. G. Tompo, A. G. Kadir, and A. Murfhi, "Analisis Peranan Bappeda dalam Pembangunan di Kabupaten Jeneponto," *J. Ilmu Pemerintah.*, vol. 5, pp. 9–20, 2012.

[2] S. N. Ajizah, E. Wijaya, and F. Meutia, "Peran Badan Perencanaan Pembangunan Daerah (BAPPEDA) Kota Depok Dalam Penyusunan Rencana Pembangunan Jangka Menengah Daerah," vol. 4, no. 1, pp. 44–64, 2021. https://doi.org/10.35814/jlr.v4i1.2966

[3] Kemendagri, "Kemendagri Luncurkan Sistem Informasi Pemerintah Daerah," Kemendagri, 2019.

[4] Menteri Dalam Negeri Republik Indonesia, "Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 70 Tahun 2019 tentang Sistem Informasi Pemerintah Daerah." Indonesia, pp. 1–16, 2019.

[5] Menteri Dalam Negeri Republik Indonesia, "Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 8 Tahun 2014 Tentang sistem Informasi Pembangunan Daerah." pp. 1–29, 2014.

[6] N. K. Sudianing and K. A. Seputra, "Peran Sistem Informasi Pemerintahan Daerah Dalam Menunjang Peningkatan Kualitas Perencanaan Pembangunan Daerah," *Locus Maj. Ilm. FISIP*, vol. 11, no. 2, pp. 1–22, 2019.

[7] F. Dione and U. Faradina, "Implementasi Sistem Informasi Pembangunan Daerah (SIPD) dalam Meningkatkan Koordinasi Pembangunan di Daerah (Studi tentang Penerapan SIPD pada BAPPEDA Kota Bengkulu)," *J. Kebijak. Pemerintah.*, vol. 1, no. January, pp. 21–28, 2020. https://doi.org/10.33701/jkp.v3i1.1061

[8] Mukhsin, "Peranan Teknologi Informasi Dan Komunikasi Menerapkan Sistem Informasi Desa Dalam Publikasi Informasi Desa Di Era Globalisasi," *Teknokom*, vol. 3, no. 1, pp. 7–15, 2020. https://doi.org/10.31943/teknokom.v3i1.43

[9] H. M. Astuti, F. A. Muqtadiroh, E. W. T. Darmaningrat, and C. U. Putri, "Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk," *Procedia Comput. Sci.*, vol. 124, pp. 569–576, 2017. https://doi.org/10.1016/j.procs.2017.12.191

[10] P. Hopkin, *Fundamentals of Risk Management*, 4th ed. USA: Kogan Page Limited, 2017.

[11] D. A. Prastiyawan, A. Ambarwati, and E. Setiawan, "Analisis Manajemen Risiko Layanan Sistem Manajemen Dealer Menggunakan COBIT 5," *Matrix J. Manaj. Teknol. dan Inform.*, vol. 10, no. 2, pp. 43–49, 2020. https://doi.org/10.31940/matrix.v10i2.1913

[12] B. Prasetyo, W. Eka Yulia Retnani, and N. Laily Muhimmatul Ifadah, "Analisis Strategi Mitigasi Risiko Supply Chain Management Menggunakan House of Risk (HOR)," *J. Tekno Kompak*, vol. 16, no. 2, pp. 72–84, 2022. https://doi.org/10.33365/jtk.v16i2.1878

[13] R. Astuti, "Implementasi Manajemen Risiko Sistem Informasi Menggunakan COBIT 5," *Media Inform.*, vol. 17, no. 1, pp. 18–28, 2018. https://doi.org/10.37595/mediainfo.v17i1.7

[14] Y. Supriyadi and C. W. Hardani, "Information system risk scenario using COBIT 5 for risk and NIST SP 800-30 Rev. 1 a case study," *Proc. - 2018 3rd Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2018*, pp. 287–291, 2018. https://doi.org/10.1109/ICITISEE.2018.8721034

[15] E. Ismawan, A. S. Putri, and N. J. Utamaja, "Using COBIT 5 for Risk Management Assessment E-Wallet Information Technology in Indonesia," *Int. J. Progress. Res. Sci. Eng.*, vol. 2, no. 8, pp. 741–745, 2021.

[16] ISACA, *COBIT 5 Enabling Processes*. USA: ISACA, 2012.

[17] F. Adikara, "Implementasi Tata Kelola Teknologi Informasi Perguruan Tinggi Berdasarkan Cobit 5 Pada Laboratorium Rekayasa Perangkat Lunak," *Semin. Nas. Sist. Inf. Indones.*, no. 2, pp. 2–4, 2013.

[18] Y. Kusumaningrum and Wella, "Adoption of COBIT 5 Framework in Risk Management for Startup Company," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 3, pp. 1446–1452, 2021. https://doi.org/10.17762/turcomat.v12i3.942

[19] ISACA, *COBIT 5: A business framework for the governance and management of enterprise IT COBIT 5*. USA: ISACA, 2012.

[20] Megawati and A. Syntia, "Evaluasi Manajemen Resiko Teknologi Informasi Menggunakan Kerangka Kerja Cobit 5.0," *J. Ilm. Rekayasa dan Manaj. Sist. Inf.*, vol. 4, no. 2, pp. 118–122, 2018. http://dx.doi.org/10.24014/rmsi.v4i2.5682

[21] R. D. A. Putra, E. Setiawan, and A. Ambarwati, "Evaluasi Manajemen Risiko Teknologi Informasi Berdasarkan Framework COBIT 5 Pada PT.BTM," *JSI J. Sist. Inf.*, vol. 11, no. 2, pp. 1754–1762, 2019. https://doi.org/10.36706/jsi.v11i2.9103

[22] ISACA, *COBIT 5 For Risk*. USA: ISACA, 2013.

[23] P. P. Thenu, A. F. Wijaya, and C. Rudianto, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus: Pt Global Infotech)," *J. Bina Komput.*, vol. 2, no. 1, pp. 1–13, 2020. https://doi.org/10.33557/binakomputer.v2i1.799

[24] Menteri Dalam Negeri Republik Indonesia, "Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 86 Tahun 2017 Tentang Tata Cara Perencanaan, Pengendalian Dan Evaluasi Pembangunan Daerah, Tata Cara Evaluasi Rancangan Peraturan Daerah Tentang Rencana Pembangunan Jangka Panjang Daerah Dan Rencana." pp. 1–644, 2017.

[25] D. Hillson, "Effective strategies for exploiting opportunities," *Present. Proc. Proj. Manag. Inst. Annu. Semin. Symp. Nashville, TN.*, 2001.