ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN1542

Adopting COBIT 2019 for the Evaluation of Information Technology Risk Management in a Startup Company

Aulia Oktaviana[1]; Kusworo Adi[2]; Budi Warsito[3]
[1] Magister Information System, Postgraduate School; [2] Department of Physics; [3] Department of Statistics
Diponegoro University Semarang, Indonesia

Abstract:- The start-up XYZ operates in tourism and digital agencies, where every business activity relies on IT from the outset. We must implement good risk management to ensure optimal operation of all business processes and minimize risks, particularly in light of the post-pandemic changes. The study uses the COBIT 2019 framework to evaluate the risk management of the company's business processes. The study comprises five stages: a preliminary study, a research planning phase, data collection, data analysis, and a recommendation phase. As a result, the company has successfully identified potential risks, along with their respective impact levels, and gained insights into IT-related issues. However, the company still requires an extensive evaluation for its field implementation. While the company believes it has effectively managed risks, subsequent assessments reveal that it is still in the early stages, necessitating numerous improvements in risk management implementation. This is evident from the evaluation of the EDM03 and APO12 processes; the company's capacity is currently at level 1 with a gap of 2. The overarching recommendation is for companies to document all past risks, standardize SOPs, and regularly evaluate them to ensure continuous improvement in future business processes.

Keywords:- *Startup, COBIT 2019, Risk Management, EDM03, APO12.*

I. INTRODUCTION

Currently, startups are increasingly prevalent and expanding entities in the realm of information technology. The business operations primarily revolve around concepts such as ideas, creativity, innovation, and the development of new products or services. These aspects are given significant consideration in the first stages of the process. Furthermore, the majority of the business's activities heavily depend on Information Technology (IT). The pervasive and growing adoption of information technology (IT) in firms, particularly startups, positions IT as a crucial component that enhances the competitive advantage of the company [1]. Moreover, employing technology in a methodical and focused approach can enhance productivity and operational efficiency, so generating additional value for the organization. This exemplifies the significant importance of the IT position in the company's business operations, prompting many organizations to allocate substantial financial resources in order to reap the advantages it provides.

However, in practice, IT deployments do not always yield excellent results, and the expenditures made by firms can generate uncertainty, leading to unmet expectations and even financial losses for the company [2]. The senior management consistently prioritizes investments based on their benefits, irrespective of the risks, threats, and vulnerabilities present within the organization. Specifically, challenges related to information technology have an unintended effect on the company's business performance, both in a direct and indirect manner [3]. The ambiguous result poses a substantial obstacle for corporate executives, as it is arduous to ascertain the degree to which uncertainty brings out both hazards and opportunities. Hence, it is vital to have regulated administration to guarantee the smooth operation and execution of IT through the adoption of risk management.

XYZ, an Indonesian startup that operates in the tourism and digital agency sectors, is also subject to the aforementioned conditions. From its inception, information technology is utilized in every business activity of the venture, XYZ. The services and products offered include online ticketing for event organizers and travelers, as well as social media management, digital advertising, and project management for other entrepreneurs. The company's objective is to establish consumer confidence and satisfaction by utilizing a B2B (business-to-business) business model that focuses on companies or business actors rather than end- customers. One approach to accomplishing this objective is to optimize the utilization or investment in information technology and oversee the company's management to mitigate business risk and preserve the trust and contentment of customers. The absence of significant obstacles allowed XYZ to operate its business processes and organizations with ease for three (3) years of operation, with the exception of occasional small-scale and uncommon occurrences of risk. Nevertheless, the circumstances have evolved since the COVID-19 pandemic, requiring a start-up approach. As part of a risk management phase, XYZ has implemented modifications to its business processes to guarantee its ongoing existence. One-step toward the development of appropriate strategies for the company's operational preparedness and recovery during or after the pandemic is the implementation of self-risk management [4]. As a precautionary measure against an unprecedented pandemic or extraordinary event, that impacts all sectors domestically and internationally, XYZ implemented a virtual tour service by mid-2020, in accordance with the government's standard new policy [5]. The initial objective of this type of risk management was straightforward: to guarantee the company's survival. However, the organization experiences advantages from modifications to its operations and procedures, as demonstrated by the development of more dynamic business processes, even during the pandemic's height. Furthermore, there has been a rise in the number of online tourists, including both individuals and groups, as new clients appreciate virtual tour activities. This has resulted in an increase in company turnover and the recruitment of new employees.

Over time, the severity of the epidemic increased, and people began adjusting to the new set of rules. This development provided a fresh opportunity to standardize the business operations at XYZ Company. Online ticketing services started to reopen gradually, in contrast to virtual tour services, which saw a decrease in user interest. The issue relates to the change in customer behavior, which has grown more discerning when engaging in economic transactions [6]. Amidst the epidemic, XYZ enterprises secured their business continuity by implementing a range of strategic alterations to their business models. In the aftermath of the pandemic, organizations have returned to their normal business practices, requiring an examination of the risks they face and their strategy for managing those risks in order to quickly minimize or address prospective concerns. Risk management is a strategic method of arranging corporate actions in order to mitigate potential adverse consequences. The method entails comprehending, discerning, and assessing any potential hazards that may arise [7]. IT risks are unpredictable and can arise in any situation or location. Therefore, it is crucial to establish and oversee a company's IT risk management process in order to minimize potential financial losses, handle uncertainties, risks, and opportunities, and improve the company's ability to restore its value [8][9]. Furthermore, IT risk management plays a crucial role in achieving a balance between a company's outcomes and its profitability while also ensuring the continuation of its business operations [10][11].

IT risk management is part of the IT governance system, with the main objective of this governance being to ensure that the company's IT strategy is in line with the business strategy, as well as that IT investments can support the business strategy and reduce the risk of their use. Enterprises can apply several frameworks to their IT governance [12], with COBIT (Control Objectives for Information and Related Technology) being the most popular and widely used framework in Indonesia [13]. Furthermore, Cobbit is also one of the globally recognized and most comprehensive frameworks covering the other framework standards [14]. Cobit 2019 is a framework for ensuring effective corporate governance over information and technology, as well as optimizing risk and resource utilization.

The introduction of the most recent COBIT 2019 framework represents a significant departure from the previous version, as it divides the five principles that were previously present into two main classifications, each with its own set of principles. The latest version's change of principle implies that COBIT aspires to be a framework that is more dynamic, adaptable, and open to the organization's requirements. Additionally, COBIT adheres to the harmonization principle by incorporating a variety of more precise technical standards [15]. In addition to these distinctions, the most recent version includes modifications to the system and management components. The previous version included seven (seven) enablers for the IT value governance objective. COBIT 2019 refers to the seven enablers as components of a governance system. The component also has four focus areas: security, risk, operational development, and SMEs. The division of the focus area enhances COBIT's flexibility and practicality, tailored to the company's requirements [15]. It is not mandatory for all organizations to execute COBIT as a complete undertaking [5]. Nevertheless, organizations may use COBIT implementation outcomes as a framework for system and process implementation and enhancement. Implementation procedures may begin with the identification, selection, application, and adaptation of administrative and management practices relevant to a specific focal area, in response to specific requirements. Consequently, COBIT 2019 has effectively established industry-specific best practices that cater to the requirements of organizations of all sizes and sectors.

COBIT 2019 has established two process domains that are pertinent to the implementation of organizational risk management: EDM03 and APO12. The EDM 03 Ensured Risk Optimization Domain ensures that companies have a comprehensive understanding of their risk appetite and tolerance, which allows them to identify and manage risks that affect the value of IT-related enterprises. Subsequently, the APO12 process domain identifies, evaluates, and mitigates IT-related risks to prevent them from exceeding the designated tolerance limits. The ApO12 domain also tries to combine IT-related enterprise risk management with overall corporate risk management. This will help balance the pros and cons of managing IT-related corporate risks [16]. The post-pandemic era presents an opportunity for XYZ companies to integrate both process domains into their risk management practices. This will allow them to identify risk profiles, assess and map risks, and achieve a balance between corporate governance and risk management. Our goal is to improve XYZ companies' risk awareness and caution in their decision-making processes, particularly in the current post-pandemic era, through the implementation of risk management.

II. LITERATURE REVIEW

➢ *COBIT 2019*

The Control Objective for Information and Related Technology (COBIT), also known as EGIT, is a framework for governing information and technology enterprises. The Information Systems Audit and Control Association (ISACA), an international professional membership organization that serves as a resource for individuals interested in or employed in IT audit, IT risk, and IT governance, developed the COBIT framework. Since its inception in 1967 [1], ISACA has become an internationally recognized organization, with a membership of more than 150,000 individuals worldwide. Table 1 illustrates the primary distinctions between COBIT 2019 and its predecessors.

Table 1 Differences of Cobit 5 and Cobit 2019

No	*Difference*	*COBIT 5*	*COBIT 2019*
1	Overview COBIT	No design factor	11 design factors
2	Principle	5 principle	9 principle
3	Process Domain Core Model	37 domain – verb	40 domain – objective
4	Goal Cascade	5 goal cascade	4 goal cascade alignment goals and IT goals
5	Measuring maturity level	Capability level	Maturity level and capability level
6	Governance	Enabler	Governance Components

➢ *EDM03 and APO12*

EDM03 and APO12 are special domains at COBIT 2019, which pertain to the administration of IT risks within organizations or companies. The EDM03 process domain, also known as Ensured Risk Optimization, provides a comprehensive explanation of the process of identifying and managing the impact of IT risk on the company's value, understanding risk appetite and tolerance, and minimizing the potential failure of compliance [17]. EDM03.02 Direct risk management is the process by which the management level directs the development of risk management practices to ensure that they are appropriate for the actual IT risk and do not exceed the specified risk. EDM 03.03, Monitor Risk Management, is the final course. The course outlines how the management level oversees the primary objectives and metrics of the risk management process, and how to identify, monitor, and improve any deviations or issues.

Process Domain of APO12 Managed risk, or risk management, is a comprehensive management system that identifies, evaluates, and controls IT-related risks within the tolerance levels established by the company's executive management is known as managed risk or risk management. The goal of APO-12 is to reconcile the costs and benefits of administering IT risk management, as well as integrate IT risk management with corporate risk management as a whole.

➢ *Risk Management*

The coordinated activity of risk management directs and regulates the organization of risk-related matters. The management process includes risk identification, assessment, and anticipation, as well as monitoring and evaluation of potential risks [18][7]. In order to identify potential events that could affect its business processes, a company implements corporate risk management in a strategic setting. It is one of the processes within an organization that is dynamic and responsive to change, including safeguarding value and decision-making [19]. Risk management is a method by which a company can make continuous advancements due to its dynamic, responsive nature. In order to assist management entities in achieving performance and profitability objectives, as well as prevent resource loss, this capability is inherent in company risk management. In practice, enterprise risk management assists the entity in achieving its desired objectives, avoiding unexpected pitfalls or obstacles that arise during the business process, and ensuring business continuity [9][10]. The corporate governance system integrates risk management into the business process, thereby facilitating the achievement of targets, innovation, and enhanced performance.

III. METHODOLOGY

This research use a qualitative approach that focuses on COBIT 2019. The framework of Figure 1 visualizes the five stages of the research procedure.

➢ *Preliminary Studies*

The preliminary study stage involves the collection of the data and initial information needed for the research. The activities included the study of the library and searching for references from sources of writing related to the use of the COBIT framework primarily for risk management at startups. Such references come from international journals, national journals, books, or other relevant sources.

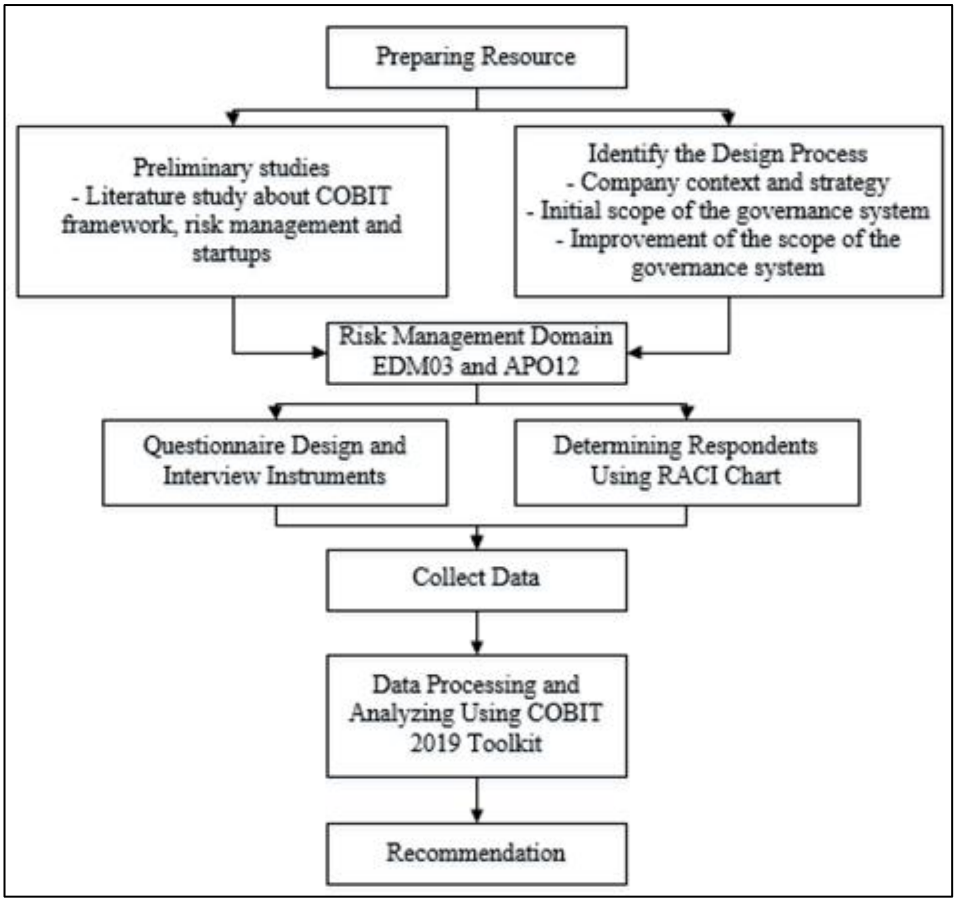
Preparing Resource
Preliminary studies
- Literature study about COBIT framework, risk management and startups
Identify the Design Process
- Company context and strategy
- Initial scope of the governance system
- Improvement of the scope of the governance system
Risk Management Domain EDM03 and APO12
Questionnaire Design and Interview Instruments
Determining Respondents Using RACI Chart
Collect Data
Data Processing and Analyzing Using COBIT 2019 Toolkit
Recommendation

Fig. 1. Research Method

➢ *Design*

During this phase, we strategize our research requirements, which include outlining the necessary tools and resources for the research, choosing the study subjects, defining the goals of the COBIT process, and creating a research schedule. The research object is the startup firm XYZ, which operates in the tourist and digital agency sectors and is located in Semarang City, Central Java. The RACI chart designated four individuals as respondents for the survey: the CEO, CTO, CFO, and Tourism System Specialist. The subsequent domains or objectives of the COBIT process are EDM03 (Ensured Risk Optimization) and APO12 (Managed Risk).

➢ *Collect Data*

The third phase entails collecting primary data from the XYZ company using an associated questionnaire and in-depth interviews. The tools utilized are obtained from the COBIT 2019 governance management objectives, practices, and activities toolkit, specifically focusing on risk profiles, risk-related issue mapping, and the EDM03 and APO12 process domains. The risk profile questionnaires, risk-related issue evaluations, and EDM03-process domains will be sent to corporate stakeholders or CEOs, while the APO-12 process domain questionnaire will be allocated to CTOs, CFOs, and tourism system specialists.

➢ *Analyze*

During this stage, the risk value will be calculated as the sum of the impact value and the probability of occurrence. The color markers and characters in the matrix order represent the risk category. For instance, L denotes low risk, N denotes normal risk, H denotes high risk, and VH denotes extremely high risk.

Risk Matrix		Impact				
		1	2	3	4	5
Likelihood	1	L	L	L	N	N
	2	L	N	N	N	H
	3	L	N	H	H	VH
	4	N	N	H	VH	VH
	5	N	H	VH	VH	VH

Fig. 2. Risk Matrix

The next section consists of a comprehensive assessment of enterprise IT risk-related matters. It includes 20 statements that evaluate the significance of IT risk-related concerns for the organization. The data will be taken into account when formulating the conclusive recommendations pertaining to IT risk management that XYZ organizations must undertake.

The third step involves assessing and examining the practical areas of EDM03 and APO12 using the NPLF scale, which is displayed in Table 2. The analysis of the activity is conducted incrementally, taking into account the degree of proficiency determined by the rating process activities (refer to Table 2). Activities that achieve the full capacity level (F) are eligible to go to the next level. The questionnaire on the EDM03 and APO12 process domains consists of two stages: level 2 and level 3. To progress to level 3 in the EDm03 process domain, eight out of nine statements must have a F value. On the other hand, in the APO 12-process domain, either six statements or all statements must have an F value. If neither of the process domains is suitable to go to level 3, the data collection will cease at level 2.

We have conducted a gap analysis to identify any necessary tasks that can enhance IT management, particularly in the context of risk management. Equation 1 shows that the gap is caused by the difference between current ability and future capacity. If there is a deficiency, we will provide an unbiased suggestion to enhance any procedure that requires improvement to reach the desired level of proficiency.

$$Gap = (to - be) - (as - is) \qquad (1)$$

➢ *Recommendation*

At this point, a concise overview will be created based on the collected data. Subsequently, recommendations will be provided as a strategic plan for the startup firm to implement in order to enhance their research objectives. The objective is to optimize the company's IT risk management in order to reduce potential losses and assure business continuity.

IV. RESULT AND DISCUSSION

COBIT 2019 categorizes the organization's approach into four fundamental patterns, each accompanied by a matching priority scale. During the epidemic, corporations prioritize cost leadership as a means to ensure the company's survival. The company's management has implemented the strategy of developing new products that offer value to customers and can be marketed without incurring any development costs, even during the pandemic. Following the epidemic, firms began focusing their attention on expansion initiatives and improving customer service. This entailed delivering reliable and customer-centric services. This change will inevitably affect the company's aims as a direct result of its strategy. Initially, the company focused on ensuring the uninterrupted provision of business services. However, these objectives later expanded to include business risk management as well as fostering innovation in both products and business practices. According to the COBIT 2019 benchmark, it refers to EG02 (managed business risk) and EG06 (business service continuity and availability). The objectives are consistent with the alignment goals of AG02 (risk management related to technology and innovation) and AG07 (information security, infrastructure and application development, and privacy). In business, corporate management implements several measures, such as conducting risk assessments, reintroducing the company's flagship product at the usual scheduled time, and enhancing customer service throughout the product development process by introducing improved iterations.

➢ *Mapping Risk Profile*

Based on the COBIT 2019 factor design, a risk profile mapping consisting of 19 categories is used to identify the types of T&I risk present in the XYZ startup business processes, particularly in the face of post-pandemic times.

There are two categories of risk scenarios that are highly profiled, and there are seven categories of high-profile risk scenarios. Companies frequently incorporate Technology and Innovation (T&I) into their business processes, and decisions about IT investments, portfolio definition, and maintenance significantly influence the company. Improper execution of these tasks can lead to investment waste and substantial losses. Furthermore, managing the portfolio effectively is crucial for the company, as it can portray the company's image to clients, thereby preventing potential losses.

Table 2 Risk Profile Mapping – DF3

No	Risk Category	Impact	Likelihood	Risk Profile
1	IT investment decision making, portofolio definition & maintenance	4	4	Very High
2	Program & projects life cycle management	3	3	High
3	IT cost & oversight	3	3	High
4	IT expertise, skills & behaviour	4	4	Very High
5	Enterprise/ IT architecture	3	2	Normal
6	IT operational infrastructure incidents	4	3	High
7	Unauthorized actions	2	1	Low
8	Software adoption/ usage problems	3	2	Normal
9	Hardware incidents	1	1	Low
10	Software failures	2	2	Normal
11	Logical attacks (hacking, malware, etc)	2	2	Normal

No	Risk Category	Impact	Likelihood	Risk Profile
12	Third-party/ supplier incidents	1	1	Low
13	Noncompliance	3	2	Normal
14	Geopolitical issues	2	2	Normal
15	Industrial action	3	3	High
16	Acts of nature	3	3	High
17	Technology-based innovation	4	3	High
18	Environmental	3	3	High
19	Data & information management	4	2	Normal

- *Mapping IT-Related Issues*

There are 20 IT-related issue statements divided into three levels: 1 not a problem, 2 problems, and 3 very serious problems. Table 3 shows the results of the mapping of IT-related issues at XYZ Company.

The problem mapping revealed no IT-related issues with a value of 3, indicating they were not of a very serious nature. Therefore, the aforementioned list of problems does not pose a threat to the company's business sustainability. However, it's crucial to remember that some IT-related problems are more significant than others, necessitating the management of these risks to prevent them from becoming severe.

Table 3 IT-Related Issues Mapping – DF4

No	Risk Category	Importance
1	Frustration between different IT entities across the organization because of a perception of low contribution to business value	1
2	Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value	1
3	Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	2
4	Service delivery problems by the IT outsourcer(s)	2
5	Failures to meet IT-related regulatory or contractual requirements	1
6	Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems	1
7	Substantial hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets	1
8	Duplications or overlaps between various initiatives, or other forms of wasted resources	2
9	Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	1
10	IT-enabled changes or projects frequently failing to meet business needs and delivered late or over budget	1
11	Reluctance by board members, executives or senior management to engage with IT, or a lack of committed business sponsorship for IT	1
12	Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	2
13	Excessively high cost of IT	1
14	Obstructed or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	1
15	Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languages	1
16	Regular issues with data quality and integration of data across various sources	1
17	High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation	2
18	Business departments implementing their own information solutions with little or no involvement of the enterprise IT department (related to end-user computing, which often stems from dissatisfaction with IT solutions and services)	1
19	Ignorance of and/or noncompliance with privacy regulations	1
20	Inability to exploit new technologies or innovate using I&T	2

- *Capability Level EDM03*

Based on interviews with respondents, we obtained the evaluation of EDM03 process domain level 2, as shown in Table 4. The results indicated that we had not fully implemented a domain at level 2, leaving it at level 1. The interview halted at level 2 and could not proceed to level 3, as only one process domain, valued at F, was present among the nine statements.

Table 4 EDM03 Level 2

No	Process Domain	Result
1	EDM03.01.01	L
2	EDM03.01.02	L
3	EDM03.01.03	L
4	EDM03.01.04	L
5	EDM03.02.01	L
6	EDM03.02.02	L
7	EDM03.02.03	L
8	EDM03.02.04	F
9	EDM03.03.01	L

- *Capability Level APO12*

Based on the results of interviews with respondents, the APO12 process domain assessment level 2 was obtained, as shown in Table 5. The results showed that there was only 1 F value on R1 in the second statement, zero F value in R2, and 1 F worth in R3 in the sixth statement. In addition, there was 1 P value for R2 in the first statement and 1 P worth for R3 in the first declaration, while the other statement was L. The condition revealed that XYZ had not fully implemented level 2 of the APOs process domain, resulting in the current state remaining at level 1. So the interview stopped at level 2 and could not proceed to level 3.

Table 5 APO12 Level 2

No	Process Domain	R1	R2	R3
1	APO12.01.01	L	P	P
2	APO12.01.02	F	L	L
3	APO12.03.03	L	L	L
4	APO12.03.04	L	L	L
5	APO12.03.05	L	L	L
6	APO12.05.06	L	L	F

- *Gap Analysis*

The company aims to achieve a target capacity level of level 3 in the EDM03 and APO12 domains. The respondents express hope that the implementation of risk management has been appropriate and has a positive impact on the company, ensuring a balance between the benefits obtained and the costs incurred. However, the results indicate that both process domains are at level 1, resulting in a discrepancy between the expected capacity and the current capacity, as illustrated in Table 6. To reach the targeted level, companies must complete the activities at levels 2 and 3 of the COBIT Governance Practice with a score above 85%.

Table 6 Gap Capability Level

Domain	*Capabililty Level*		*Gap*
	As – is	*To – be*	
EDM03	1	3	2
APO12	1	3	2

- *Recommendation*

The company can improve its IT risk management by implementing the recommendations generated by the gap capability level analysis. Table 7 illustrates the recommendations.

Table 7 Recommendation

No	Activity
Domain EDM03	
1	Companies have the ability to record and document the execution of IT risks and the actions taken to reduce or eliminate them.
2	It is necessary to develop more transparent risk limit measurements that can be effectively conveyed to stakeholders and other management teams. These metrics will serve as a reference point for decision-making. Companies have the ability to record and document the execution of IT risks and the actions taken to reduce or eliminate them.
3	The company can develop more accurate risk tolerance measurements that are consistent with the organizations past risk paperwork.
4	The organization guarantees that the gathered IT risk documentation effectively functions as a point of reference for establishing risk limitation or tolerance criteria.
5	The strategies and risk mitigation can be aligned with the existing documents.
6	Create a Standard Operating Procedure (SOP) for risk mitigation.
7	The company has the capability to provide simulation or risk mitigation training to all teams in accordance with the established Standard Operating Procedures (SOPs).
8	Enhance the collective assurance of all teams in their ability to collaborate, mitigate risks, and accurately document them.
9	The corporation regularly engages in reviews, either monthly or at certain intervals, with the Commissioner to discuss the execution of risk management.
Domain APO12	
1	The company formulates standard operating procedures (SOPs) to identify dangerous scenarios or conditions connected to IT risks.

No	Activity
Domain EDM03	
2	The company records all IT risks that have occurred within the organization or with its partners.
3	The company consistently records all IT service-related business processes, both internal and external, in a comprehensive manner, covering the entire process from beginning to end.
4	The company compiles a roster of IT service goals encompassing both software and hardware, with the aim of enhancing the company's sustainability.
5	The company comprehensively records the IT services it has delivered to clients, subsequently categorizing them based on category, business line, or functional area.
6	The company implements a standard operating procedure for risk management.

V. CONCLUSION

The company has made changes and adjustments according to the circumstances. On the other hand, the company has successfully mapped potential risks and their impact levels, and has a thorough understanding of IT issues. However, the implementation of these changes in the field still requires extensive evaluation. Therefore, we expect the company to document all potential risks, both internal and external, for creating a standardized Standard Operating Procedure (SOP) that management and operational levels can discuss collaboratively. Subsequently, the SOPs that have been implemented are expected to be evaluated on a regular basis to ensure a periodic improvement in future business processes.

ACKNOWLEDGMENT

I acknowledge my gratitude to the Indonesia Endowment Fund for Education Agency (LPDP) under the Ministry of Finance of the Republic of Indonesia for awarding the scholarship and providing funding for this research.

REFERENCES

[1]. S. De Haes, W. Van Grembergen, J. Anant, dan T. Huygh, Enterprise Governance of Information Technology. Achieving Alignment and Value in Digital Organizations, Third Edit. Springer Nature Switzerland AG, 2020.

[2]. J. S. Suroso dan B. Rahadi, “Development of IT risk management framework using COBIT 4.1, implementation in it governance for support business strategy,” ACM Int. Conf. Proceeding Ser., vol. Part F1306, no. July 2017, hal. 92–96, 2017, doi: 10.1145/3124116.3124134.

[3]. B. C. Alberts dan A. Dorofee, Managing Information Security Risks : The OCTAVE SM Approach, First Edit. Addison-Wesley Longman Publishing Co., Inc., 2002.

[4]. O. Ozdemir, T. Dogru, M. Kizildag, M. Mody, dan C. Suess, “Quantifying the economic impact of COVID-19 on the U.S. hotel industry: Examination of hotel segments and operational structures,” Tour. Manag. Perspect., vol. 39, no. November 2020, hal. 100864, 2021, doi: 10.1016/j.tmp.2021.100864.

[5]. D. F. Tanjung, A. Oktaviana, dan A. P. Widodo, “Analisis Manajemen Risiko Startup Pada Masa Pandemi COVID-19 Menggunakan COBIT® 2019,” J. Teknol. Inf. dan Ilmu Komput., vol. 8, no. 3, hal. 635–642, 2021, doi: 10.25126/jtiik.202184914.

[6]. A. P. Auliya dkk., “Online Business Transformation in the Covid-19 Pandemic Era (Case Study of Msme Activities in Tangerang City),” Int. J. Econ. Account. Res., vol. 6, no. 1, hal. 546–552, 2022, [Daring]. Tersedia pada: https://jurnal.stie-aas.ac.id/index.php/IJEBAR/article/view/4744/2108.

[7]. H. M. Astuti, F. A. Muqtadiroh, E. W. T. Darmaningrat, dan 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, hal. 569–576, 2017, doi: 10.1016/j.procs.2017.12.191.

[8]. P. P. Thenu, A. F. Wijaya, dan C. Rudianto, “Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus: Pt Global Infotech),” J. Bina Komput., vol. 2, no. 1, hal. 1–13, 2020, doi: 10.33557/binakomputer.v2i1.799.

[9]. dkk Richard M. Steinberg, “Enterprise Risk Management-Integrated Framework,” Comm. Spons. Organ. Treadw. Comm., Sep 2004, doi: 10.1002/9781119201939.app4.

[10]. V. Raval dan R. Sharma, “Small business interruptions,” ISACA J., vol. 3, hal. 18–21, 2019.

[11]. A. Rafeq, “Using COBIT 2019 to Proactively Mitigate the Impact of COVID-19,” ISACA Journal, 2021.

[12]. R. M. Maskur, Nixon Adolong, “IMPLEMENTASI TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 5 DI BPMPTSP BONE BOLANGO Kabupaten Bone Bolango dipetakan untuk,” J. Masy. Telemat. dan Inf., vol. 8, no. 2, hal. 109–126, 2017.

[13]. F. Jingga, R. Kosala, B. Ranti, dan S. H. Supangkat, “It governance implementation in indonesia: A systematic literature review,” Int. J. Sci. Technol. Res., vol. 8, no. 10, hal. 2074–2079, 2019.

[14]. ISACA, “Introducing COBIT 2019 - OVERVIEW November 2018,” no. November, 2018, [Daring]. Tersedia pada: http://www.isaca.org/COBIT/Documents/COBIT-2019-Toolkit_fmk_eng_1118.zip.

[15]. ISACA, “Introducing COBIT 2019, Major Differences with COBIT 5,” 2018, [Daring]. Tersedia pada: https://www.isaca.org/resources/cobit.
[16]. ISACA, Governance and Management Objectives. 2018.
[17]. D. Lanter, COBIT 2019 Framework Introduction and methodology. 2019.
[18]. N. A. N. Dewi dan I. G. P. H. Yudana, “Analisa Manajemen Risiko Pada Sistem Akademik di STMIK STIKOM Bali,” Semin. Nas. Teknol. Inf. dan Multimed. 2016, hal. 6–7, 2016.
[19]. A. B. : Charles R. Vorst, D.S. Priyarsono, Manajemen Risiko Berbasis SNI ISO 31000, Edisi Pert. Jakarta: Badan Standardisasi Nasional, 2018.