Information Technology Governance Using the COBIT 2019 Framework at PT. Pelindo TPK Bitung

Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 Pada Perusahaan PT. Pelindo TPK Bitung

George Morris William Tangka*[1], Erienika Lompoliu[2]
[1]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Klabat
[2]Manajemen, Fakultas Ekonomi dan Bisnis, Universitas Klabat
email: ***[1]gtangka@unklab.ac.id** , [2]erienika.lompoliu@unklab.ac.id

Abstract

The governance of information technology (IT) is crucial for companies in managing their IT assets. This research investigates the implementation of COBIT 2019 at PT. Pelindo TPK Bitung, a logistics and storage company, aiming to enhance its Information Technology (IT) governance. Facing challenges in IT management, the company adopted COBIT 2019 to improve operational efficiency, reduce security risks, and ensure regulatory compliance. The study employs a structured approach, utilizing the COBIT 2019 Design Toolkit, and includes a literature review, interviews, and systematic evaluations of PT. Pelindo TPK Bitung's IT governance. Findings from the first interview highlight the company's focus on growth, innovation, and strategic IT roles, alongside challenges in integrating IT and operations. The prioritized governance objective, DSS05 - Managed Security Services, achieves a capability level 3, indicating substantial success, though gaps in security aspects necessitate prompt policy reviews. In conclusion, PT. Pelindo TPK Bitung's COBIT 2019 implementation has achieved significant success, reaching a capability level 3, with suggestions provided for sustaining and enhancing security management. This research contributes insights into COBIT 2019 implementation, offering a comprehensive understanding of its impact on IT governance in a specific organizational context

Keywords—*IT governance, COBIT 2019, IT Audit, Design Factor*

Abstrak

Tata kelola teknologi informasi (TI) merupakan aspek yang sangat krusial bagi perusahaan dalam mengelola aset TI yang dimilikinya. Penelitian ini menyelidiki implementasi COBIT 2019 di PT. Pelindo TPK Bitung, sebuah perusahaan logistik dan penyimpanan, dengan tujuan meningkatkan tata kelola Teknologi Informasi (TI) perusahaannya. Menghadapi tantangan dalam manajemen TI, perusahaan mengadopsi COBIT 2019 untuk meningkatkan efisiensi operasional, mengurangi risiko keamanan, dan memastikan kepatuhan regulasi. Studi ini menggunakan pendekatan terstruktur dengan memanfaatkan COBIT 2019 Design Toolkit, dan melibatkan tinjauan literatur, wawancara, serta evaluasi sistematis terhadap tata kelola TI PT. Pelindo TPK Bitung. Temuan dari wawancara pertama menyoroti fokus perusahaan pada pertumbuhan, inovasi, dan peran TI yang strategis, sekaligus tantangan dalam mengintegrasikan TI dan operasional. Sasaran utama tata kelola, yaitu DSS05 - Managed Security Services, mencapai tingkat kemampuan 3, menunjukkan keberhasilan yang signifikan, meskipun terdapat celah pada aspek keamanan yang memerlukan peninjauan kebijakan segera. Sebagai kesimpulan, *implementasi COBIT 2019 di PT. Pelindo TPK Bitung telah mencapai kesuksesan yang signifikan, mencapai tingkat kemampuan 3, dengan saran untuk menjaga dan meningkatkan manajemen keamanan. Penelitian ini memberikan wawasan tentang implementasi COBIT 2019, memberikan pemahaman menyeluruh tentang dampaknya pada tata kelola TI dalam konteks organisasi yang spesifik.*

Kata kunci*—Tata kelola TI, COBIT 2019, Audit IT, Design Factor*

1. INTRODUCTION

Information Technology (IT) governance has become highly important in supporting the success of companies in the rapidly evolving digital era. Companies like PT. Pelindo TPK Bitung, operating in the logistics and storage sector at Bitung Port, face challenges in effective IT management and governance [1]. To address these challenges, the company has adopted an IT management framework, such as COBIT (Control Objectives for Information and Related Technologies), which was updated by ISACA in 2019 [2]. COBIT 2019 is designed to enhance operational efficiency, reduce security risks, and ensure regulatory compliance [3]. The implementation of COBIT 2019 is expected to improve IT governance at PT. Pelindo TPK Bitung, despite challenges such as complexity, cost, and resistance to change.

Furthermore, this research will investigate the implementation of COBIT 2019 at PT. Pelindo TPK Bitung, with the aim of identifying issues, potential improvements, and its impact on IT performance and governance. This research also focuses on the unique context of PT. Pelindo TPK Bitung, differentiating it from previous studies that have discussed IT governance and the use of COBIT. Thus, the results of this research are expected to be beneficial not only to PT. Pelindo TPK Bitung but also to the academic community and practitioners in the field of IT governance using COBIT 2019.

2. RESEARCH METHOD

2.1. Research Method Flow

The researcher applied the research method used to investigate the Information Technology governance system at PT. Pelindo TPK Bitung can be seen in Figure 1.

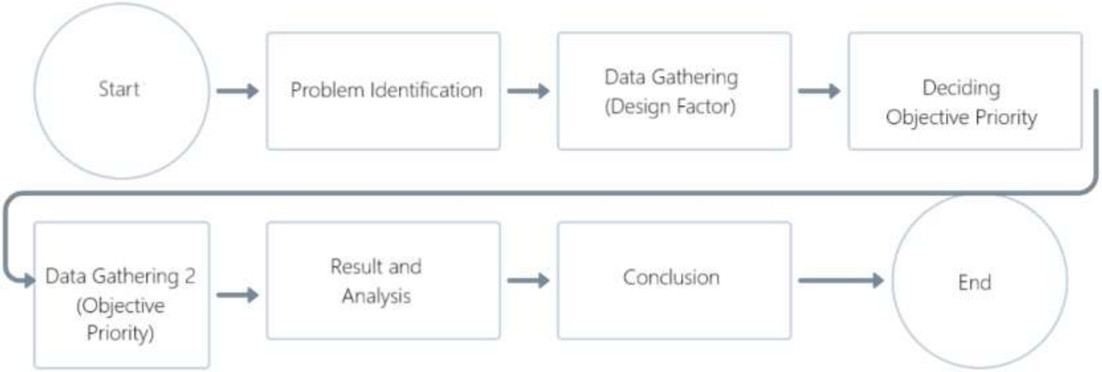
Start
Problem Identification
Data Gathering (Design Factor)
Deciding Objective Priority
Data Gathering 2 (Objective Priority)
Result and Analysis
Conclusion
End

Figure 1. Research Method

The research methodology employed in this study follows a systematic flow to comprehensively address the challenges faced by PT. Pelindo TPK Bitung in implementing COBIT 2019 for effective IT governance. The process initiates with problem identification, acknowledging the existing hurdles in IT management and governance within the organization.

The problem identification was generated from initial interview (all interview can be found on the following link: https://shorturl.at/fwUV2).

Subsequently, data gathering ensues through structured interviews utilizing the COBIT 2019 Design Toolkit, a vital tool in assessing the organization's IT governance framework. This part is where we ask questions from 10 Design Factor form COBIT 2019 design toolkit. The result can be seen here: https://shorturl.at/iBHL2. This step helps us dig deep into how they're currently using COBIT 2019, find any problems, and think about ways to make it work even better. Following this, the research transitions to deciding objective priority, a critical step in determining which governance objectives merit focused attention. The governance objective that we take into priority are the one that is above 75% point. After that, another round of data gathering unfolds through interviews, this time employing the COBIT 2019 Governance Objectives, to prioritize and gain deeper insights into specific objectives crucial for IT governance effectiveness. The research then progresses to result analysis, systematically examining the findings from both sets of interviews, and concludes by drawing meaningful insights and recommendations based on the evaluated data. This structured research flow ensures a holistic understanding of the COBIT 2019 implementation at PT. Pelindo TPK Bitung, offering valuable insights for both academic discourse and practical implications in the field of IT governance.

2.2. Literatur Review

Literature review or review is the process of compiling a research report with the aim of examining and gathering data and information from existing documents [4]. In this section, we list findings from various sources, drawing connections between different studies to establish a solid foundation for our research. By examining the insights and perspectives presented in the existing literature, we aim to identify gaps, contradictions, or areas where further investigation is needed, thereby contributing to the overall academic discourse on the subject.

2.2.1. IT Governance

The management of Information Technology (IT) resources is a crucial concept in efforts to allocate IT resources within an entity. Strong financial leadership in the village and participatory planning, integrated and aligned with other planning, serves as a vital indicator in managing village funds [5]. Additionally, COBIT 2019 is also one of the frameworks that can be used to govern Information Technology (IT) at the organizational level. IT governance refers to the processes of managing and controlling IT resources owned by an organization to achieve business objectives and reduce potential risks [6]. By implementing efficient IT governance, organizations can be more successful in managing risks and achieving their business goals [5]. COBIT 2019 can serve as a tool to evaluate IT governance within an organization and help identify both positive and negative aspects of IT management [3].

2.2.2. COBIT 2019

COBIT is one of the frameworks used in audit standards. This framework was developed by the IT Governance Institute (ITGI), which is also a part of ISACA [7]. COBIT provides a set of guidelines and instructions that assist in guiding information technology management. It helps management, auditors, and users in identifying business risks, needs, and other issues that may arise when information technology is implemented. With the advancement of technology, COBIT continues to evolve [8].

COBIT 2019 is a framework commonly used to assess the management of information technology within organizations [9][10][11]. Its focus is on controlling and enhancing the value of information and technology. The development of COBIT 2019 was triggered by organizations' need to manage information technology responsively, efficiently, and in alignment with their goals, with efforts to avoid duplication [8][12].

2.2.3. Understanding the Company's Context and Strategy

Understanding the context and strategy of a company is a thorough process that involves comprehending the external and internal environment in which the company operates, as well as the long-term plans and goals that the company implements to achieve success and growth. This is highly important in corporate management because it helps the company identify opportunities, manage risks, and allocate resources efficiently to achieve their objectives. Corporate strategy can enhance the company's ability to face competition and achieve its business goals more efficiently and effectively [13][14].

Understanding the context and strategy of a company assists the company in making wise decisions, optimizing operations, and remaining relevant in a constantly changing environment. It also helps the company align its strategies with its long-term goals, enabling it to achieve long-term growth and success.

2.2.4. Defining the Initial Scope of the Governance System (Design Factor 1-4)

Defining the initial scope of a governance system is an important first step in the development of effective governance [15][16]. This process involves identifying and delineating the scope of the governance system, including key aspects such as processes, entities, and resources to be regulated and monitored. By clearly defining the initial scope, organizations can design a governance framework that aligns with their needs and objectives, ensuring that appropriate roles and responsibilities are assigned. It also helps in identifying the resources required for governance implementation and measuring the effectiveness of the system in achieving organizational goals. When determining the initial scope of the governance system, an assessment of factors influencing IT governance development is required, such as financial governance, village planning, and policy regulations [17]. This evaluation can help companies identify weaknesses and strengths in their information technology governance and design action plans to improve IT governance within the company [3].

Design Factor 1 (Enterprise Strategy)

Every company has a unique approach to developing a strategy that aligns with the type of business it operates, which can be expressed through one or more patterns [18]. In design factor 1, corporate strategy is divided into four types: growth/acquisition, which focuses on the company's expansion; innovation/differentiation, where the company focuses on offering innovative products to customers; cost leadership, where the company emphasizes cost minimization; client service/stability, which focuses on providing stable services and customer-centricity. The assessment description for design factor 1 is as follows: a rating of 5 means it is most important or the primary focus, a rating of 4 is very important or the secondary focus, a rating of 3 is important, a rating of 2 is moderately important, and a rating of 1 is not important.

Design Factor 2 (Enterprise Goals)

In design factor 2, it is an essential component in developing and assessing Information Technology (IT) governance based on the COBIT framework. This factor focuses on identifying and assessing the extent to which the company prioritizes enterprise goals related to the use and management of IT. Enterprise goals are high-level objectives that an organization aims to achieve and often encompass aspects such as security, compliance, efficiency, and innovation in the context of IT.

The questions posed to the company regarding Design Factor 2 can help in identifying how much emphasis the company places on these goals and ensuring that they are well integrated into the company's IT strategy and operations.

Design Factor 3 (IT Risk Profile)

COBIT 2019 provides 19 criteria for Risk Profile, such as IT investment decisions, program and project lifecycle management, IT cost oversight, IT skills and behavior, compliance, and data and information management.

Design Factor 4 (IT Related Issues)

In Design Factor 4, the identification and analysis of information technology-related issues are carried out. This identification takes into consideration IT-related issues currently faced or risks that have occurred. Issues related to IT aspects must be clearly identified in accordance with the criteria set within the COBIT 2019 framework. The aim is to address potential future problems more efficiently and effectively.

2.2.5. Improving the Governance System Scope (Design Factor 5-10)

Improving the scope of a governance system is a process that involves evaluating and adjusting the elements included in the governance system of an organization. This is often necessary when there are changes in the business environment, corporate objectives, or internal policies. This process includes changes or adjustments to roles and responsibilities, procedures, policies, and entities regulated within the governance system. By improving the scope of the governance system, organizations can ensure that their governance remains relevant, efficient, and aligned with changing needs and challenges. This process can also help organizations enhance their flexibility and responsiveness to changes in the business environment. This evaluation can assist companies in identifying strengths and weaknesses in their information technology governance and designing action plans to improve IT governance within the company [13][14].

Design Factor 5 (Threat Landscape)

In design factor 5, it is the stage related to the scope of threats within the company. The threats in design factor 5 can help determine the level of security present at PT Pelindo TPK Bitung. These threats in design factor are divided into two categories: normal and high. Normal-level threats imply that the company is operating under normal threat levels, while high-level threats mean that the company is in a highly hazardous environment.

Design Factor 6 (Compliance Requirement)

In the sixth design factor stage, it involves assessing the percentage of compliance within the company with each regulation, especially those related to governance. This stage is divided into three categories: Low, Normal, and High. The Low category indicates that the company's compliance level is considered below average, thus being categorized as low. The Normal category signifies that the company's compliance is on par with the average for companies in general. Meanwhile, the High category indicates that the company's compliance level is considered above average or very high, categorizing it as high.

Design Factor 7 (Role of IT)

In design factor 7, it is the stage to determine the role of IT at PT Pelindo TPK Bitung. In this design factor, it is divided into four categories: first, IT as Support; second, as Factory; third, as Turnaround; and fourth, as Strategic. Therefore, the question asked to the interviewee is, "What is the role of IT in the company?" with ratings given as follows: 1: Not Important, 2: Moderately Important, 3: Important, 4: Very Important, and 5: Most Important.

Design Factor 8 (Sourcing model for IT)

In design factor 8, it is the stage to determine the sources of IT services used by PT Pelindo TPK Bitung. In this design factor, it is divided into three categories: outsourcing, cloud, and insourced. The assessment is determined using percentages. For example, if the company uses services solely from the cloud and does not use outsourcing or insourced services, the assessment would be cloud 100%, outsourcing 0%, insourced 0%.

Outsourcing refers to the practice of using third-party technology services to provide needed services. Cloud refers to the utilization of cloud storage facilities to store files and important information. Insourced means providing specialized staff to manage their own information technology services [19].

Design Factor 9 (IT Implementation Methods)

In this design factor, we inquire about the 3 software development methods used by PT Pelindo TPK. These 3 methods are:

1. Agile: It is an iterative software development method tailored to meet client needs.
2. DevOps: is a set of practices that brings together software development (Dev) and IT operations (Ops) to enhance collaboration and productivity in the software development lifecycle. It aims to automate and streamline the processes of building, testing, deploying, and maintaining software, fostering a culture of continuous improvement and quicker delivery of high-quality software products. The key principles of DevOps include collaboration, automation, and a shared responsibility between development and operations teams.
3. Traditional: It is a software development method, such as the waterfall model, that follows a linear and sequential approach to software development.

Design Factor 10 (Technology Adoption Strategy).

Given the rapid advancement of technology today, design factor number 10 emphasizes the company's technology adoption strategy. Respondents are given three choices: First move, Follower, and Slow adopter.

1. First Mover: When a company takes the first step in adopting new technology as a primary effort or does it as soon as possible to gain a specific advantage.
2. Follower: When a company adopts new technology as a follower, or they first evaluate whether the technology has proven itself before adopting it.
3. Slow Adopter: Refers to how a company is very slow in adopting new technology that is already available [20].

3. RESULT AND DISCUSSION

Below are the results of the analysis from the first interview using the COBIT 2019 Design Toolkit, and the second interview for prioritized Governance Objectives that have been conducted with PT Pelindo TPK Bitung.

3.1. *The First Interview and Its Analysis*

In the first design factor, it was found that the primary focus is on growth, where PT Pelindo TPK Bitung is dedicated to continuous innovation to provide the best service to customers. Cost leadership is not a focus for PT Pelindo TPK Bitung due to the absence of competitors.

PT Pelindo TPK Bitung prioritizes growth through innovation to deliver superior customer service. The lack of competition allows them to be less focused on cost leadership. The interview reveals a high emphasis on various corporate objectives such as managing business risks, complying with external laws and regulations, maintaining the quality of financial information, optimizing business process costs, and managing digital transformation programs. The company also prioritizes product and business innovation, demonstrating a strong commitment to compliance, risk management, and innovation.

The risk profile of PT Pelindo TPK Bitung encompasses various scenarios with significant impacts and probabilities. Key risks include IT investment decision-making, portfolio maintenance, IT expertise and skills, and operational IT infrastructure incidents. Other risks include unauthorized actions, hardware incidents, and software failures, all of which have substantial impacts on business continuity and security. The company actively manages these risks through planned investments, ongoing monitoring, and digital transformation strategies.

PT Pelindo TPK Bitung faces challenges in integrating IT and operations. Issues such as the perceived low contribution of IT to business value, investments in software that do not meet expectations, and vendor management are prominent. However, the company effectively addresses these challenges, complies with government regulations, and maintains strong IT performance. The company also navigates complexities such as balancing IT resources, project management, and aligning business with technical knowledge.

The company has a normal threat landscape, with most threats manageable due to its unique position in the market and synergy with local government and stakeholders. PT Pelindo TPK Bitung also demonstrates a high level of compliance with government regulations, reflecting strong alignment with regulatory requirements.

IT plays a strategic role in PT Pelindo TPK Bitung, significantly influencing operations and innovation. The company's IT resource landscape includes outsourcing (30%), cloud services (20%), and insourcing (50%). In terms of technology implementation methods, Agile dominates (60%), followed by DevOps (30%), and traditional methods (10%). The technology adoption strategy primarily follows the 'Follower' approach (50%), with significant initiatives as 'First Mover' (40%), and minimal 'Slow Adopter' attitude (10%), indicating a balanced and cautious approach to adopting new technology.

3.2. Determination of Objectives Priority

Based on the results of the 10 design factors that have been filled out, it is found that there is 1 objective with a score above 75, which is based on the company's condition as per the interview results. The priority objective in question is DSS05 - Managed Security Services. The results are shown in the figure 2 below.

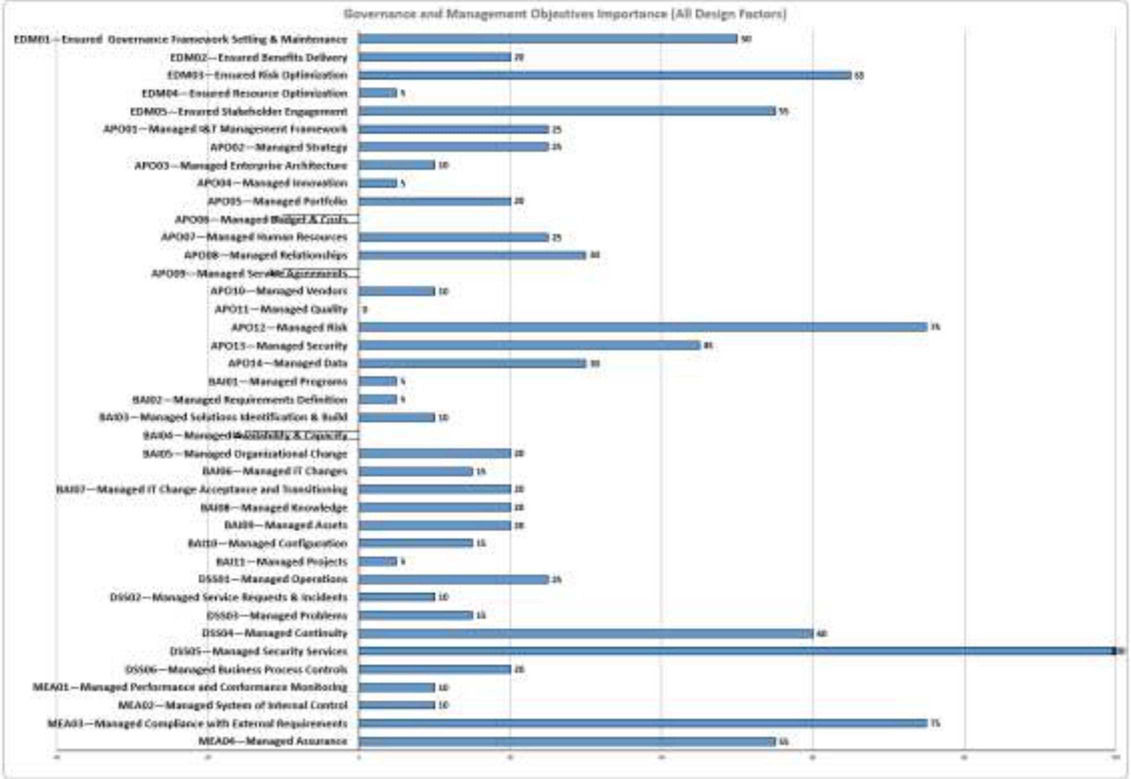

Figure 2. Governance and management objectives importance

3.3. The Second Interview

The table 1contains the results of the interview on priority objectives for DSS05 Level 2:

Table 1. DSS05 Level 2 Activities

No	Activities	Result
1	Is there an IT governance activity for installing and activating protective tools for software at all processing facilities?	✓
2	Is there an IT governance activity to filter incoming traffic, such as email and downloads, to protect against unwanted information (e.g., spyware, email phishing)?	✓
3	Is there an IT governance activity that only allows official devices access to company information?	✓
4	Has IT governance implemented network filtering mechanisms, such as firewalls and intrusion detection software?	✓
5	Has IT governance implemented approved security protocols for network connectivity?	✕
6	Has IT governance configured network equipment securely?	✓
7	Has IT governance configured the operating system securely?	✓

8	Has IT governance implemented device locking mechanisms?	✓
9	Has IT governance implemented remote access management and control?	✓
10	Has IT governance securely managed network configurations?	✓
11	Has IT governance implemented network traffic filtering on end-point devices?	✓
12	Has IT governance protected system integrity?	✓
13	Has IT governance provided physical protection for end-point devices?	✗
14	Has IT governance safely disposed of end-point devices?	✓
15	Has IT governance managed potentially harmful access through email and web browsers? For example, blocking specific websites and disabling click-through links on smartphones.	✓
16	Has IT governance ensured that user access rights are aligned with business functions, process requirements, and security policies? Aligning access rights with defined roles and responsibilities.	✓
17	Has IT governance recorded and monitored all points of entry to IT sites, including registering all visitors?	✓
18	Has IT governance ensured that all staff/users display approved identification correctly at all times?	✓
19	Does IT governance require visitors to be escorted while on-site?	✓
20	Has IT governance restricted and monitored access to sensitive IT sites (e.g., server rooms) by establishing perimeter limits such as walls or security devices at entrances?	✓
21	Has IT governance established procedures/rules for governing the acceptance, transfer, and disposal of sensitive documents and all outputs, both within and outside the organization?	✓
22	Has IT governance ensured that cryptographic controls are available to protect electronically stored sensitive information?	✗
23	Has IT governance continued to use the supported technology, services, and assets portfolio to identify information security vulnerabilities?	✓
24	Has IT governance defined and communicated risk scenarios so that they can be easily recognized, and their potential impacts understood?	✓
25	Does IT governance regularly review log events to detect potential incidents/problems?	✓
26	Has IT governance ensured that security-related incident tickets are created promptly?	✓

From the interview results, it is apparent that there are serious gaps in their security and data protection aspects. Firstly, not implementing security protocols on network connectivity leaves the company vulnerable to cyberattacks such as malware or DDoS attacks, which can threaten data integrity and confidentiality. Secondly, the lack of physical protection for end-point devices increases the risk of data loss and device theft, potentially leading to unauthorized access and leakage of sensitive information. Thirdly, not using cryptographic controls to protect electronically stored sensitive information makes the company's critical data, such as customer information and financial data, highly susceptible to theft and misuse. Overall, these deficiencies indicate that the company is highly vulnerable to cyberattacks, data loss, and potential reputation damage. Therefore, it is crucial for the company to promptly review and strengthen their IT security policies to protect their business assets and information more effectively.

However, based on the calculations for the priority objective DSS05 level 2, we obtained a percentage of 88%, which is above the threshold for "Largely Achieved" standards, indicating that it can proceed to level 3 assessment.

3.4. Activities at DSS05 Level 3

Here is the table containing the interview results for the priority objectives of DSS05 Level 3:

Tabel 2. Activities at DSS05 level 3

No	Activities	Result
1	Does the IT governance include activities for periodic training of staff on awareness of harmful software and procedures to handle it?	✕
2	Has the IT governance centralized the distribution of all protective software using centralized configurations?	✓
3	Has the IT governance implemented encryption of information based on its classification?	✕
4	Has the IT governance established and maintained security connectivity policies based on risk assessments?	✓
5	Has the IT governance created mechanisms to support secure information transmission and reception?	✓
6	Has the IT governance encrypted information in storage according to its classification?	✕
7	Has the IT governance managed all access rights changes in a timely manner?	✓
8	Has the IT governance minimized the number of required and actively managed accounts?	✓
9	Has the IT governance identified all information processing activities based on roles/positions?	✓
10	Has the IT governance authenticated access to all information based on functional roles/positions?	✓

11	Has the IT governance ensured that all users (internal, external, and temporary) and their activities on the system can be identified?	✓
12	Has the IT governance managed access permissions to gain access to IT/computing facilities?	✓
13	Does the IT governance ensure that profiles (e.g., ID cards) remain current for access to IT sites (e.g., server rooms)?	✓
14	Has the IT governance conducted periodic physical information security awareness training?	✕
15	Has the IT governance assigned access rights for sensitive documents or outputs?	✓
16	Has the IT governance created an inventory of sensitive documents and conducted routine reconciliations?	✕
17	Has the IT governance established appropriate physical protection for sensitive documents?	✓
18	Does the IT governance record every security-related event and store records according to their retention period?	✓

The interview results above indicate critical deficiencies in their information security management. Specifically, the absence of encryption of information according to its classification, both in transmission and storage, exposes a serious gap in data protection, increasing the risk of leakage and exploitation of sensitive data by unauthorized parties. Additionally, the lack of physical information security awareness training suggests that employees may not be fully aware or equipped to address physical risks to data, such as theft or device damage. The absence of organized inventory and routine reconciliation of sensitive documents also highlights weaknesses in managing and tracking critical information, which could lead to difficulties in responding to security incidents and recovering lost or disrupted data. This overall situation underscores the urgent need for improvement and strengthening of the company's information security policies, which are crucial to protecting assets and data integrity in an increasingly digital and interconnected business environment.

Regarding the calculation results for priority objective DSS05 level 3, a percentage of 77% was obtained, so it will not proceed to level 4 because it did not reach the 85% threshold.

4. CONCLUSION

After completing the ten design factors in the COBIT 2019 toolkit, one priority objective was identified, which is DSS05 - Managed Security Services. This process involves careful steps in identifying and understanding relevant design factors to achieve the desired security goals. Following these steps, researchers conducted a series of in-depth interviews and calculations related to this priority objective. From the research findings, it can be concluded that the priority objective, DSS05, achieved a capability level 3 with a category of "largely achieved," indicating significant achievement. This means that this objective has successfully met most of the established goals and standards. Achieving a capability level 3 indicates that the security management process has reached a sufficient level of maturity. These results provide insight into the successful implementation of the priority objective in ensuring effective and efficient system security, reflecting a commitment to best practices and excellence in security services. This data offers an in-depth understanding that aids in decision-making for further development and improvement in security service management within the organization.

5. SUGGESTION

Based on the findings that indicate the priority objective, DSS05 - Managed Security Services, has successfully achieved a capability level 3 with significant progress, here are some suggestions that can be proposed for PT Pelindo TPK Bitung to further strengthen and enhance the effectiveness of security management within the organization:

1. Reinforce the Identification of Design Factors: Ensure that the steps for identifying design factors remain meticulous and comprehensive. This involves gaining a deep understanding of the factors that influence security, thus providing a strong foundation for the implementation of the priority objective.
2. Enhance Collaboration and Communication: Promote closer collaboration and open communication among relevant stakeholders, including the security management team, related departments, and other internal parties. This can improve coordination to support the achievement of security goals.
3. Regular Evaluation and Ongoing Monitoring: Establish a process for regular evaluation and continuous monitoring of the implementation of DSS05. This can help identify potential improvements and observe changing security trends that require further attention.
4. Employee Training and Development: Ensure that the team involved in security management has the necessary knowledge and skills. Employee training and development can support a deeper understanding of best practices and the latest developments in security.
5. Implementation of Proactive Security Initiatives: Propose proactive security initiatives that can identify and address potential security risks before they become serious problems. This includes the adoption of the latest technologies and practices to mitigate potential security threats.

These suggestions are aimed at enhancing overall sustainability and effectiveness in security management to achieve and maintain the already significant capability level 3 accomplishments.

REFERENCES

[1] P. P. (Persero) Tbk, “Laporan Tahunan PT PP(Persero) Tbk,” in *TATA KELOLA PERUSAHAAN GOOD CORPORATE GOVERNANCE*, 2020.

[2] ISACA, “Introduction and Methodology,” in *COBIT 2019 FRAMEWORK*, 2018.

[3] Y. N. Nyoman Rai Widartha Kesuma, Irman Hermadi, “EVALUASI TATA KELOLA TEKNOLOGI INFORMASI DI DINAS PERTANIAN GIANYAR MENGGUNAKAN COBIT 2019,” *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 19 Juni 2023, 2023.

[4] M. Solehuddin, Z. Hulwani, and A. P. Widodo, “Perencanaan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 pada DPMPTSP,” *J. Ilm. Komputasi STI&K*, vol. 20, 2021.

[5] T. A. Safitri and R. N. Fathah, “PENGELOLAAN ALOKASI DANA DESA DALAM MEWUJUDKAN GOOD GOVERNANCE,” *J. LITBANG SUKOWATI*, vol. 2, pp. 89–105, 2018.

[6] ISACA, “A Business Framework for the Governance and Management of Enterprise IT,” in *Cobit 5*, 2012.

[7] A. M. Syuhada, "KAJIAN PERBANDINGAN COBIT 5 DENGAN COBIT 2019 SEBAGAI FRAMEWORK AUDIT TATA KELOLA TEKNOLOGI INFORMASI," *J. Ilm. Indones.*, vol. 6, 2021.

[8] S. F. Bayastura, S. Krisdina, and A. P. Widodo, "9," *Anal. DAN Peranc. TATA KELOLA Teknol. Inf. MENGGUNAKAN Framew. COBIT 2019 PADA PT. XYZ*, vol. 4, pp. 68–75, 2021.

[9] A. Ishlahuddin, P. W. Handayani, K. Hammi, and F. Azzahro, "Analysing IT Governance Maturity Level using COBIT 2019 Framework: A Case Study of Small Size Higher Education Institute (XYZ-edu)," *3rd Int. Conf. Comput. Informatics Eng.*, 2020.

[10] M. V. Lim and M. I. Fianty, "Enhancing Information Technology Governance: A Comprehensive Evaluation Of The 2019 COBIT Framework In The Retail Industry," *Int. J. Sci. Technol. Manag.*, vol. 4, 2023.

[11] L. H. Atrinawati *et al.*, "Assessment of Process Capability Level in University XYZ Based on COBIT 2019," *J. Phys. Conf. Ser.*, 2020.

[12] ISACA, "Designing an Information and Technology Governance Solution," in *COBIT 2019 DESIGN GUIDE*, 2018.

[13] G. M. W. Tangka, A. T. Liem, and J. Y. Mambu, "10.1," *Inf. Technol. Gov. Audit Using COBIT 5 Framew. XYZ Univ.*, 2020.

[14] E. M. Lompoliu, G. B. R. Francolla, G. R. Mandoya, and M. D. Walangitan, "Information Technology Governance Analysis Using The COBIT 2019 Framework at XYZ Institution," *Cogito Smart J.*, vol. 8, 2022.

[15] G. B. R. Francolla, G. R. Mandoya, M. D. Walangitan, E. Lompoliu, and J. Y. Mambu, "Information Technology Governance Audit Using The COBIT 2019 Framework at XYZ Institution," *Cogito Smart J.*, vol. 8, 2022.

[16] ISACA, "Governance and Management Objectives," in *COBIT 2019 FRAMEWORK*, 2018.

[17] A. M. Fikri, H. S. Priastika, N. Octaraisya, Sadriansyah, and L. H. Trinawati, "Rancangan Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: PT XYZ)," *Inf. Manag. Educ. Prof.*, vol. 5, pp. 1–14, 2020.

[18] B. A. M. Pangaribuan and S. Fernandez, "Tata Kelola Teknologi Informasi Menggunakan COBIT 2019 Pada Val," *J. Ilm. Komput. Graf.*, vol. 16, pp. 196–208, 2023.

[19] T. M. A. Prasetyo and M. N. N. Sitokdana, "Analisis Tata Kelola Pusat Data dan Informasi Kementerian XYZ Menggunakan COBIT 2019," *J. Appl. Comput. Sci. Technol.*, vol. 2, pp. 95–107, 2021.

[20] I. Taliwongso, J. Y. Mambu, E. Y. Putra, and J. Waworundeng, "DESIGNING IT GOVERNANCE USING COBIT 2019 AT PT UNICHARM INDONESIA," *J. Indones. Manaj. Inform. dan Komun.*, vol. 4, 2023.