



Leveraging COBIT 2019 to Implement IT Governance in Mineral Mining Company

Ray Farhan Mubarak¹, Melissa Indah Fianty^{2,*}

¹Information Systems, Universitas Multimedia Nusantara University, Tangerang, Banten, Indonesia
Email: ¹ray.farhan@student.umn.ac.id, ²melissa.indah@umn.ac.id

Abstract

The integration of Information Technology (IT) in companies comes with its own set of challenges. One major issue is the loss of operational data, which directly affects the company's workflow and disrupts its activities. To tackle this problem, the company assesses its IT capability using the COBIT 2019 framework. This framework outlines the objectives of different IT processes and assigns predetermined values to each process. The assessment reveals three levels of IT capability for specific processes within the company: EDM03 (Ensured Risk Optimization) at level 3, APO13 (Managed Security) at level 2, and MEA03 (Managed Compliance with External Requirements) at level 3. The company aims to reach level 4 for these processes. Consequently, recommendations for improvement primarily focus on enhancing the management of information security risks and information security management systems, as well as increasing compliance with policies and regulations.

Keywords: Capability Level, COBIT 2019, Information Technology, IT Governance

1. INTRODUCTION

In the contemporary era of advanced technology, numerous challenges emerge, prompting companies to integrate information technology into their business processes. These companies utilize their business procedures to reinforce information technology, aiming for a more efficient and functional system that can yield optimal outcomes. Information technology entails the application of technology to process data, encompassing operations such as data processing, collection, storage, and manipulation using various methods. The goal is to generate high-quality information characterized by its relevance, accuracy, and timeliness. Such information serves personal and business objectives, playing a crucial role in strategic decision-making[1].

Information Technology (IT) stands as a pivotal catalyst that enables companies to venture into new markets, foster innovation, and develop fresh products and services, thereby supporting corporate expansion. The revolution in information technology and the advent of the internet empowers companies to achieve



remarkable financial performance by exchanging information through digital means and online platforms, thereby streamlining global business transactions. Empirical evidence underscores the immense significance of IT in corporate contexts[2]. IT Governance pertains to the framework and processes that organizations employ to regulate and oversee the utilization of information technology (IT) in alignment with business goals[3]. This approach ensures adherence to regulatory requirements, facilitates effective IT risk management, and maintains synergy between IT and broader business objectives[4]. In mining companies, IT challenges encompass issues such as server downtime and delays in transmitting mining activity reports. The company primarily relies on outsourced IT services to facilitate its operational undertakings[5]. The predicaments encountered by the company wield a direct influence on its operational workflows, manifesting as disruptions in operational activities and sluggish responsiveness to issues arising in the mining sector, thereby impeding decision-making processes. A summary of these challenges is presented in Table 1.

Table 1. Scope of the Problem

| Scope of the problem | Impact |
|--|--|
| Server downtime on operational systems | Loss of operational data that includes information on day-to-day activities at the mine, including production, inventory, and logistics. Delays in operational activities. |
| Activity reports on late mining. | Disruption in decision-making, especially when problems occur in the mining area because information received when problems occur is not fast. |

IT governance is a critical approach adopted by companies or organizations to realize their objectives through the implementation of Information Technology (IT)[6]. The management of IT ensures the assessment of the efficiency and effectiveness of an organization's business processes through IT-related structures in alignment with strategic objectives[7]. This is achieved by incorporating industry best practices into the planning, administration, implementation, execution, and monitoring of IT activities[8]. The overarching goal is to ensure that IT operations robustly contribute to the attainment of corporate goals[9]. The governing framework employed in this process is the 2019 version of COBIT (Control Objectives for Information and Related Technologies)[10].

COBIT serves as a comprehensive framework designed for the governance and management of enterprise information and technology[11]. It is intended to encompass the entire scope of a company's operations[12]. Enterprise IT encompasses all technological and information processing activities employed by a company to achieve its objectives, regardless of their location within the organization[13]. This signifies that corporate IT extends beyond the confines of

the IT department and encompasses various facets of the organization[14]. The choice of the COBIT framework is rooted in its status as an international standard for IT governance. COBIT strives for broad adoption within the realm of management, serving both as a practical tool and a standard for IT management practices[15].

2. METHODS

The method employed in the implementation of IT Governance using the COBIT 2019 framework within a company utilizes a qualitative approach. This approach involves gathering data related to the condition and requirements of IT to analyze the level of IT governance capability within the company[16].

2.1. Research Methods

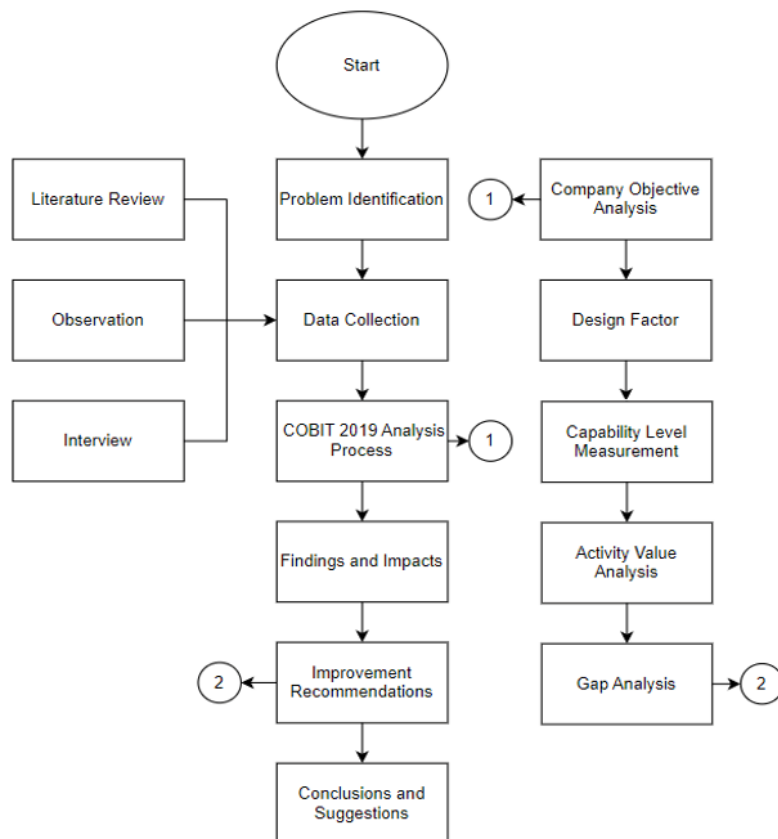


Figure 1. Research Flow

Figure 1 represents the framework utilized for the research on measuring governance capability based on a case study of a company using the COBIT 2019 approach.

1. **Problem Identification:** In this initial stage, the identification of IT problems that directly affect the company's business processes is conducted. These issues are identified through interviews conducted with the company's director. After conducting interviews about these IT challenges, two areas of problems are identified.
2. **COBIT 2019 Analysis Process:** During this stage, the selected domain is determined based on the identified problems. Furthermore, the company's level of information technology capability is measured. This process involves utilizing the COBIT 2019 analysis approach, which includes steps such as analyzing company objectives, designing a factor toolkit, creating a RACI Chart, assessing capability levels through audit documents, analyzing the value of activities within the chosen domain, and identifying gaps[17].
3. **Findings and Impact:** The objective of this stage is to generate findings derived from the value assessment of activities within the chosen domain. If an activity's value is below 50%, it signifies the need for further exploration. The outcomes of this process lead to the identification of findings and their corresponding impacts, which subsequently guide the formulation of recommendations[17].
4. **Improvement Recommendations:** This phase aims to provide recommendations based on the identified findings. These recommendations are aligned with the guidelines established by COBIT 2019. They serve as a roadmap for the company to initiate planning and implement improvements, building upon the recommendations provided[18].
5. **Conclusion:** During this stage, conclusions are drawn by considering critical points from each preceding phase. The results obtained from the audit process are synthesized at this juncture. The recommendations and results stemming from the audit can be harnessed by the company for enhancing its IT landscape. These insights contribute to the company's desired improvement trajectory and serve as a reference for future enhancements[18].

2.2. Data Analysis Technique

There are 3 data analysis techniques used:

1. COBIT 2019 Design Factor Toolkit

In this study, the data analysis technique employed is the COBIT 2019 Design Factors Toolkit provided by ISACA. The COBIT 2019 Design Factors Toolkit aids in determining process objectives for the company's governance system and measures the level of process factor influence. The process of utilizing the provided COBIT 2019 Design Factors Toolkit involves interviewing the company

to design and implement critical design factors within the Information Technology (IT) system and processes. These design factors are crafted to ensure that the IT system effectively and efficiently supports the organization's business objectives and needs. This step includes 11 criteria, presenting questions based on the Design Factors Toolkit and generating values to acquire the COBIT 2019 domain[19].

2. Capability Level Analysis

The analysis of the capability level or level of capability in this study was based on the interviewees' answers regarding the evaluation given to informants during interviews for all selected COBIT-19 functions. This assessment will consider the scale used to determine whether the COBIT-19 process stops or continues to the next level[20]. The following is the scale used:

- 1) N: Not Achieved (0 to 15%)
We found little or no evidence-gaining scale related to the computed process attributes.
- 2) P: Partially Achieved (> 15% to 50%)
There is some evidence of the scale of the estimated process attribute gain. Some attribute gains may be unpredictable.
- 3) L: Largely Achieved (> 50% to 85%)
There was evidence of a systematic approach to scale and significant achievement of the calculated process attributes. Some of the weaknesses related to this attribute are that it is contained in the calculated process.
- 4) F: Fully Achieved (> 85% to 100%)
Found complete evidence of a systematic approach scale and full achievement of the calculated process attributes.

3. GAP Analysis

In this research, the second data analysis technique is to look for gaps from the results of the current capability level with the target capability level desired by the company. The value of the gap is obtained from the results of interviews with the company through audit documents. This value is obtained from the calculation between the desired capability target and the capability that has been obtained. The step to determine the gap is by calculating the results of the target level that has been achieved with the target level determined by the company. This process generates a gap score that is used as an evaluation by companies to improve their IT governance[21].

3. RESULTS AND DISCUSSION

Here are the results of the analysis and discussion of the study, along with the stages of the COBIT 2019 framework.

3.1 Problems Identification

The initial stage in conducting a measurement of the company's IT governance involves identifying issues occurring in the company's IT that directly impact its business processes. The interviews yielded the following problems:

- 1) Server downtime resulting in the loss of operational data, leading to delays in operational activities.
- 2) Delay in delivering mining activity reports, impacting planning decision-making and response to decision-making during mining site issues.

3.2 COBIT 2019 Objective Mapping

The level of IT governance capability can be measured by first mapping the COBIT objectives. Mapping COBIT objectives is done using the COBIT 2019 Design Toolkit. The COBIT 2019 Design Toolkit measures the level of influence of each existing design factor. In this study, the level of influence of design factors will be measured for mapping the COBIT objectives as determined by the company's goals, thus determining the company's priorities[22].

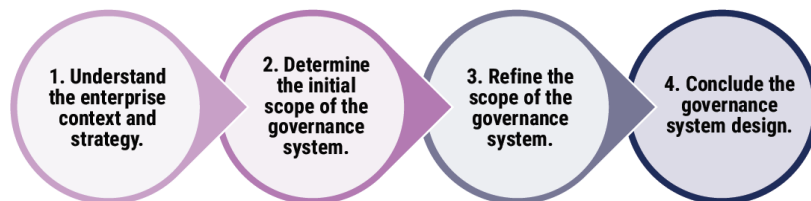


Figure 2. Governance System Design Workflow

Figure 2 the workflow of the COBIT 2019 governance design, consisting of 4 steps. These steps will yield prioritized governance objectives for the company, in order to create a governance system that aligns with the company's needs[23].

3.2.1 Understanding the Enterprise Context and Strategy

The company conducts an examination of the company's strategy, company objectives, IT risk profile, and IT-related issues, with a focus on providing services to customers.

3.2.2 Determine the Initial Scope of the Governance System

The company establishes the initial scope of the governance system by measuring design factors 1-4 to ascertain the company's strategy, objectives, risk profile, and IT-related issues.

3.2.3 Improving the Scope of the Governance System

The enterprise expands the initial scope of the governance system by measuring design factors 5-11 to determine vulnerabilities, compliance, IT roles, IT resources, IT implementation methods, used technologies, and company size.

3.2.4 Concluding the Governance System Design

The company generates a governance system design for the enterprise that encompasses prioritized governance and management objectives in order to formulate the governance system design and attain COBIT 2019 objectives[24].

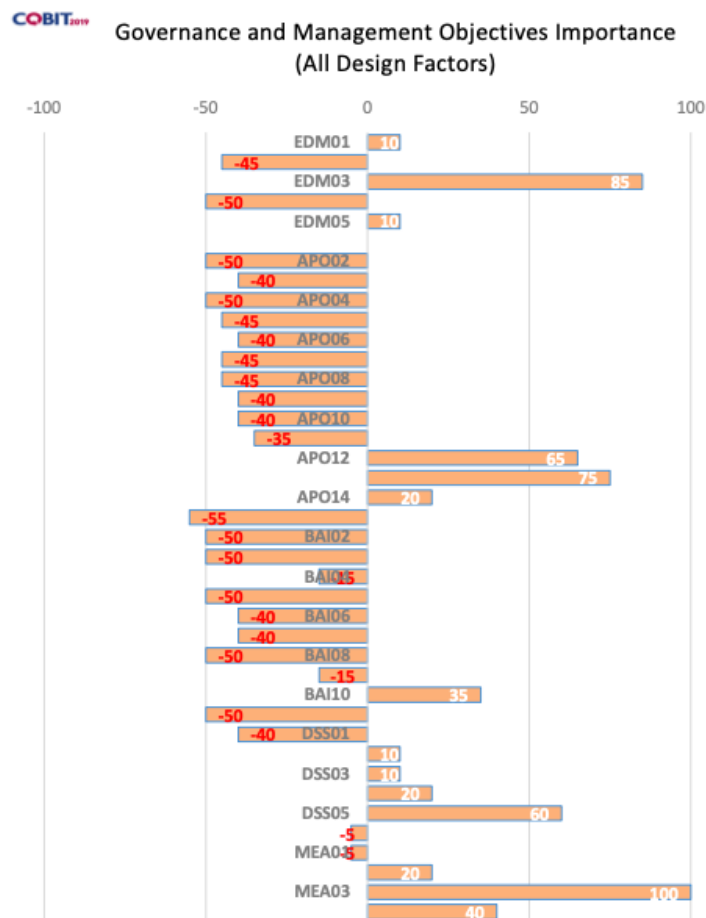


Figure 3. Design Factors Conclusions [25]

Figure 3 shows the outcomes of the process mapping using the COBIT 2019 Design Factors Toolkit, acquired through company interviews to determine process objectives. The mapping results revealed 3 domains with values of 75 or above: EDM 03 (Ensured risk optimization), APO13 (Managed security), and MEA03 (Managed compliance with external requirements).

3.3 Measuring Capability Level

Based on the assessment results obtained from interviews with the Head of IT Division and the Head of Business, here are the average calculations for each objective and its capability level.

3.3.1 EDM03 (Ensured risk optimization)

The average calculation results for EDM03 are as follows.

Table 2. EDM03 Calculation Results

| Table 2: EDM03 Calculation Results | | |
|------------------------------------|---------|-------|
| Process | | Score |
| EDM03.01 | | 56% |
| EDM03.02 | | 48% |
| EDM03.03 | | 48% |
| Capability Level Results | Total | 152% |
| | Average | 50.6% |

Table 2 represents the assessment results of EDM03 Level 2, obtaining a score of 85.25%. After calculating the scores for each activity within the EDM03 domain, it turns out that EDM03 yields values above 85%. Furthermore, upon advancing to Level 3 assessment, a score of 54.6% was achieved. Progressing to Level 4 is not feasible, as the required minimum increase to the next level is 85% or higher. These findings have resulted in conclusions and recommendations to be provided on the following page. Activities scoring below 50% will lead to findings and their associated impacts. Recommendations are given in hopes of resolving this issue.

3.3.2 APO13 (Managed security)

The average calculation results for EDM03 are as follows.

Table 3. APO13 Calculation Results

| Table 5.11.1.1.3 - Calculation Results | | |
|--|---------|-------|
| Process | Score | |
| APO13.01 | 59.5% | |
| Capability Level Results | | |
| | Total | 59.5% |
| | Average | 59.5% |

Table 3 represents the results of measuring the capability level of the APO13 domain, which is at Level 2 after an assessment of the APO13 domain activities. This is due to the failure to meet the minimum requirement for a level increase of 85%. The total score obtained for APO13 Level 2 is 59.5%. Consequently, this result cannot progress to Level 3. APO13 is the only domain that does not advance to Level 3, primarily due to the multitude of issues, systems, and SOPs that the company has yet to address. This situation has revealed findings and impacts, which will be accompanied by recommendations to enhance information technology within the company.

3.3.3 MEA03 (Managed compliance with external requirements)

The average calculation results for EDM03 are as follows.

Table 4. MEA03 Calculation Results

| Process | Score | |
|--------------------------|---------|--------|
| MEA03.01 | 65% | |
| MEA03.02 | 55% | |
| MEA03.03 | 51.6% | |
| MEA03.04 | 60% | |
| Capability Level Results | Total | 231.6% |
| | Average | 57.9% |

Table 4 represents the results of the capability assessment at Level 3 within the MEA03 domain, encompassing the sub-processes MEA03.01, MEA03.02, MEA03.03, and MEA03.04, resulting in a score of 57.9%. This result cannot be elevated to Level 4 as the assessment outcomes for activities within the MEA03 domain at Level 3 do not meet the required threshold of 85% for progression. This outcome is satisfactory for the company as it remains at Level 3. From their perspective, at this level, the company has demonstrated adequate compliance with government-established policies, regulations, and standards.

3.4 Gap Analysis

The results of all activity assessments for the selected domains, namely EDM03, APO13, and MEA03, have been calculated and the results obtained at the level of each domain. The next process is to analyze the gaps in each domain. The process of comparison between the actual state (as-is) with the desired condition (to-be) or expected standard.

Table 5. GAP Analysis

| No | Domain | Expected Level | Current Level | Gap |
|----|-----------------------------------|----------------|---------------|-----|
| 1 | EDM03 (Ensured risk optimization) | 4 | 3 | 1 |
| 2 | APO13 (Managed security) | 3 | 2 | 1 |

| No | Domain | Expected Level | Current Level | Gap |
|----|---|----------------|---------------|-----|
| 3 | MEA03 (Managed compliance with external requirements) | 4 | 3 | 1 |

Table 5 it shows the domains EDM03, APO13, and MEA03. The expected level for each domain is 4, and the assessment results for the capability levels of each domain are at level 3. Therefore, each domain has a gap of 1 level from the expected capability level. Below is a radar chart depicting the gap analysis.

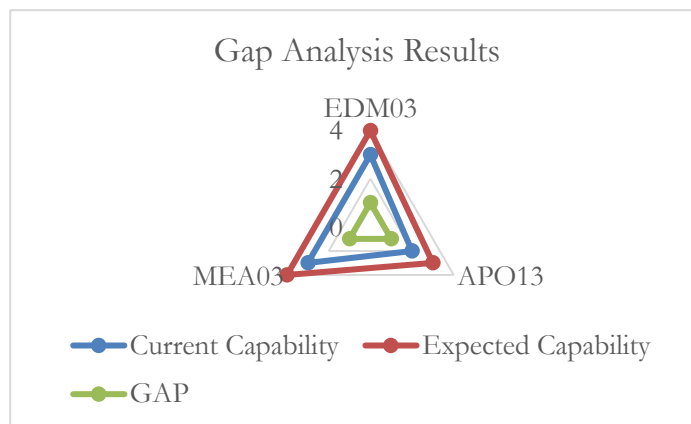


Figure 4. Radar Chart GAP Analysis

Figure 4 shows the radar chart of the gap analysis of the 3 selected domains that have produced capability levels, namely EDM03, APO13, and MEA03. From these results it can be identified data gaps with level expectations, then from the results of these measurements obtained findings and impacts of sub-processes that cause the level of capability levels not in line with level expectations.

Table 6. Expected Company Capability Target

| Domain | Description | Expected Level |
|--|---|----------------|
| EDM03 (Ensured risk optimization) | Ensuring that the company's taste and risk tolerance are understood, articulated, and communicated, and that risks to the company's value related to the use of I&T are identified and managed. | 4 |
| AP013 (Managed security) | Defining, operating, and monitoring the information security management system. | 3 |
| MEA03 (Managed compliance with external requirements) | Evaluating that both the I&T processes and the business processes supported by I&T comply with laws, regulations, and contractual requirements. Obtaining assurance that requirements have been | 4 |

| Domain | Description | Expected Level |
|--------|---|----------------|
| | identified and adhered to; integrating IT compliance with overall corporate compliance. | |

Table 6 represents the targets for each process that the company aims to achieve, none of which, across all three domains, have reached the desired level set by the company.

3.5 Recommendations

Recommendations are provided as a reference for the enterprise to improve process activities that are still at level 4, thereby enabling the enterprise to enhance activities and elevate the level of capability. Additionally, these recommendations are expected to align the use of IT with business activities, allowing the company's objectives to be achieved.

Table 7. Level 4 Recommendations for EDM03

| Process | Recommendations |
|----------|--|
| EDM03.01 | Company needs to create and develop the skills and knowledge required in the internal personnel of the company in the field of IT risk management. |
| EDM03.02 | Company needs to conduct a comprehensive analysis of business requirements relevant to risk management. This involves a deep understanding of the organization's goals, business strategies, and the risks it faces. |

Table 7 shows the recommendations for EDM03 level 3 activities based on the identified findings and impacts. These recommendations are in line with the COBIT 2019 guidelines. Below is a table detailing the improvement recommendations for the APO13 activity.

Table 8. Level 3 Recommendations for APO13

| Process | Recommendations |
|----------|--|
| APO13.01 | Company needs to enhance management awareness regarding the significance of implementing and operating an Information Security Management System (ISMS). |
| | Company comprehensive analysis is necessary to identify and understand the relevant scope of the Information Security Management System (ISMS) for the organization. |

Table 8 shows indicates the improvement recommendations for APO13 activity at level 2 based on the identified findings and impacts. These recommendations

are in accordance with the COBIT 2019 guidelines. Below is a table detailing the improvement recommendations for the MEA03 activity.

Table 9. Level 4 Recommendations for MEA03

| Process | Recommendations |
|------------|---|
| MEA03.01 | Company should consider engaging an independent consultant who possesses expertise and relevant experience in the applicable laws, regulations, or standards within the industry or operational environment of the company. |
| MEA03.02 | Company needs to establish a structured and planned communication approach to inform relevant personnel about new and changing requirements. |
| MEA03.03 1 | Company needs to conduct a comprehensive evaluation of its existing policies, standards, and procedures to identify compliance gaps. |

Table 9 shows recommendations for improving MEA03 Level 3 activities based on the identified findings and impacts. These recommendations are based on the COBIT 2019 guidelines. The provided recommendations are aimed at addressing the deficiencies based on the previously identified findings and impacts. It is expected that these recommendations can be implemented to resolve issues in the MEA03 domain.

4. CONCLUSION

The assessment of the Information Technology capability level within the company, conducted through the COBIT 2019 framework, indicates that in the EDM03 domain, the level is at 3, in the APO13 domain, it's at 2, and in the MEA03 domain, it's also at 2. These results are used to measure, evaluate, and enhance IT governance practices within the company's mining operations. The targeted capability levels are set at levels 3 and 4. It's evident that there is a one-level difference between the current capability level and the targeted capability level. The recommended improvements primarily revolve around information security risk management, strengthening the information security management system, and enhancing compliance with established policies and regulations. Additionally, emphasis is placed on ensuring that employees have a comprehensive understanding of their roles in maintaining information security, managing information security systems, and evaluating policies and regulations that haven't been implemented yet.

REFERENCES

- [1] R. S. Naibaho, "Peranan Dan Perencanaan Teknologi Informasi Dalam Perusahaan," *War. Ed.* 52, no. April, pp. 1–12, 2017.

- [2] M. I. Mgunda, "The Impacts Information Technology On Business," *J. Int. Conf. Proc.*, vol. 2, no. 3, pp. 149–156, Dec. 2019, doi: 10.32535/jicp.v2i3.656.
- [3] P. Weill and J. W. Ross, *IT governance : how top performers manage IT decision rights for superior results*. Harvard Business School Press, 2004.
- [4] K. Rizki and N. Bahtiar, "Analisis Tata Kelola Teknologi Informasi (IT Governance) Menggunakan COBIT 5 (Studi Kasus di UPT Puskom Universitas Diponegoro)."
- [5] A. P. Rabhani *et al.*, "Audit Sistem Informasi Absensi Pada Kejaksaan Negeri Kota Bandung Menggunakan Framework Cobit 5," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 2, pp. 275–280, Aug. 2020, doi: 10.32736/sisfokom.v9i2.890.
- [6] M. I. Fianty and M. Brian, "Leveraging COBIT 2019 Framework to Implement IT Governance in Business Process Outsourcing Company," vol. 5, no. 2, pp. 568–579, 2023, doi: 10.51519/journalisi.v5i2.492.
- [7] U. Devti, U. Telkom, R. N. Rachman, and I. Santosa, "Rencana Audit Teknologi Informasi Menggunakan COBIT 2019 pada Unit DevTI Universitas Telkom," *J. Ilm. Komputasi*, vol. 20, no. 3, pp. 307–317, 2021, doi: 10.32409/jikstik.20.3.2785.
- [8] D. U. Setya and W. Wella, "COBIT 5.0: Capability Level of Information Technology Directorate General of Treasury," *Int. J. New Media Technol.*, vol. 5, no. 1, pp. 18–24, 2018, doi: 10.31937/ijnmt.v5i1.614.
- [9] A. Nisri, "Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja Cobit 2019," *J. Tata Kelola dan Kerangka Kerja Teknol. Inf.*, vol. 9, no. 1, pp. 34–41, 2023, doi: 10.34010/jtk3ti.v9i1.9672.
- [10] R. K. Sari, R. V. Hari Ginardi, and A. S. Indrawanti, "Perancangan Tata Kelola Teknologi Informasi Berbasis COBIT 2019: Studi Kasus di Divisi Information Technology PT Telkom Indonesia Kota Bandung," *J. Tek. ITS*, vol. 12, no. 1, 2023, doi: 10.12962/j23373539.v12i1.100436.
- [11] A. S. Sukanto, H. Novriando, and A. Reynaldi, "Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 (Studi Kasus: UPT TIK Universitas Tanjungpura Pontianak)," *J. Edukasi dan Penelit. Inform.*, vol. 7, no. 2, p. 210, 2021, doi: 10.26418/jp.v7i2.47859.
- [12] R. Almeida, R. Pereira, and M. Mira Da Silva, "IT governance mechanisms: A literature review," in *Lecture Notes in Business Information Processing*, 2013, vol. 143 LNBIP, pp. 186–199, doi: 10.1007/978-3-642-36356-6_14.
- [13] S. Ahriz, A. El Yamami, K. Mansouri, and M. Qbadou, "Cobit 5-based approach for IT project portfolio management: Application to a Moroccan university," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 4, pp. 88–95, 2018, doi: 10.14569/IJACSA.2018.090416.
- [14] D. Z. Darmawan and Wella, "IT governance evaluation on educational institutions based on COBIT 5.0 framework," in *Proceedings of 2017 4th International Conference on New Media Studies, CONMEDLA 2017*, Jul. 2017,

- vol. 2018-Janua, pp. 50–55, doi: 10.1109/CONMEDIA.2017.8266030.
- [15] M. Destriani and Y. H. Putra, “Rencana Audit Tata Kelola Sistem Informasi Di Universitas Subang Menggunakan Framework COBIT 2019,” *J. Tata Kelola dan Kerangka Kerja Teknol. Inf.*, vol. 9, no. 1, pp. 19–33, 2023, doi: 10.34010/jtk3ti.v9i1.9164.
- [16] H. M. J. Saputra, A. I. N. F. Abdullah, D. B. Tandirau, E. Ramadhani, and L. H. Atrinawati, “Penyesuaian Sistem Tata Kelola Pada Institut Teknologi Kalimantan Dengan Menggunakan Cobit 2019,” *JSI J. Sist. Inf.*, vol. 12, no. 2, p. 2020, 2020, doi: 10.36706/jsi.v12i2.11582.
- [17] ISACA Governance and Manajement, *COBIT 2019 Governance and Management Objectives (ISACA)*. 2019.
- [18] ISACA, *COBIT® 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*. 2018.
- [19] ISACA, *COBIT 2019 Framework - Introduction and Methodology*. 2019.
- [20] I. P. Windasari, A. F. Rochim, S. N. Alfiani, and A. Kamalia, “Audit Tata Kelola Teknologi Informasi Domain Monitor, Evaluate, and Asses dan Deliver, Service, Support Berdasarkan Framework COBIT 2019,” *J. Sist. Info. Bisnis*, vol. 11, no. 2, pp. 131–138, 2022, doi: 10.21456/vol11iss2pp131-138.
- [21] C. Jienardy, “Gap analisis persepsi dan ekspektasi konsumen terhadap kualitas layanan, harga, kualitas produk esus,” *J. Manaj. dan Start-Up Bisnis*, vol. 1, no. 6, pp. 703–710, 2017.
- [22] P. Novita Anastasia and L. Happy Atrinawati, “Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 Pada Hotel Xyz,” *JSI J. Sist. Inf.*, vol. 12, no. 2, p. 2020, [Online]. Available: <http://ejournal.unsri.ac.id/index.php/jsi/index>.
- [23] R. Fadhilah, “Rencana Audit Teknologi Informasi Menggunakan Cobit 2019 Pada Unit Isti Universitas Telkom,” *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 3, pp. 157–163, 2021, doi: 10.33387/jiko.v4i3.3325.
- [24] S. C. A. KUMAPE, “Perancangan Tata Kelola Teknologi Informasi Menggunakan Cobit 2019 Pada PT.X,” *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 1568–1580, 2022, doi: 10.35957/jatisi.v9i2.2115.
- [25] T. Maulariqa Insani and A. Ikhwan, “Implementasi Framework Cobit 2019 Terhadap Tata Kelola Teknologi Informasi Pada Balai Penelitian Sungei Putih,” *Univ. Islam Negeri Sumatera Utara Jl. Lap. Golf*, vol. 6, no. 1, 2022.