

---

## IT Governance Capability Assessment Using COBIT 2019 Framework in STIKI Malang Library Information Systems

Timoty Des Christian<sup>1\*</sup>, Mochamad Dwi Oxta Gyofany<sup>2</sup>, Muhammad Bagas Allbani<sup>3</sup>

<sup>1,2,3</sup>*Sekolah Tinggi Informatika & Komputer Indonesia, Information System, Malang, Indonesia*

---

### Article Information

Accepted: 23-11-2023

Revised: 04-12-2023

Published: 24-12-2023

### Keywords

*IT governance, COBIT 2019, capability assessment, library information systems, APO12, BAI10, DSS04*

### \*Correspondence Email

*timoty.deschristian@gmail.com*

### Abstract

STIKI Malang Library, as a library service manager, requires a capability level review, especially on IT risk aspects, a review of service policies, and the quality of human resources. This study aims to analyze the level of capability and provide recommendations using the COBIT 2019 framework. Data were collected through interviews with the Head of the Library and Staff of Information Systems and Information Technology at STIKI Malang and IT governance document analysis. APO12, BAI10, and DSS04 were chosen based on COBIT 2019 design factors. The results show that these three objectives are currently at level three, with a target of level four. STIKI Malang Library can achieve this target by improving IT risk management, regular reporting to the management, and identifying required resources for business continuity.

### Abstrak

Perpustakaan STIKI Malang sebagai pengelola layanan perpustakaan memerlukan peninjauan tingkat kapabilitas khususnya pada aspek risiko TI, peninjauan kebijakan layanan, dan kualitas sumber daya manusia. Studi ini bertujuan untuk menganalisis tingkat kapabilitas dan memberikan rekomendasi dengan menggunakan framework COBIT 2019. Data dikumpulkan melalui wawancara kepada Kepala Perpustakaan dan Staf Kantor Teknologi Informasi STIKI Malang, serta analisis dokumen tata kelola TI. APO12, BAI10, dan DSS04 dipilih menggunakan faktor desain COBIT 2019. Hasil menunjukkan bahwa ketiga tujuan ini saat ini berada pada level tiga, dengan target di level empat. Perpustakaan STIKI Malang dapat mencapai target tersebut dengan meningkatkan manajemen risiko TI, pelaporan kepada manajemen secara berkala, dan mengidentifikasi sumber daya yang diperlukan untuk kelangsungan bisnis.

---

## 1. Introduction

STIKI Malang Library is one of the organizational units at STIKI Malang that aims to build and maintain knowledge and collections to provide information for research, education, and culture. STIKI Malang Library has implemented information technology through the STIKI library information systems ([perpustakaan.stiki.ac.id](http://perpustakaan.stiki.ac.id)) to support service operations. This service has been developed since 2017 with frequent maintenance to gradually improve the quality of IT services according to user needs. Information Technology implementation opens up opportunities to support essential services, as university libraries are vital organs for institutions responsible for many academic activities (Dalbehera, 2020).

Interviews with the Head of the Library and Information Technology Office suggested that the STIKI Malang library information systems faced obstacles in IT management due to information systems being unable to cover all library operational activities, limited integration with other business units, non-optimal IT risk management plan, incomplete IT disaster recovery plan to encompass all possible IT incident scenarios fully, and, insufficient human resources. Thus, these problems obstructed the continuity of the organization's business operations and IT management. In this regard, information systems audits become a crucial part of continuous monitoring and evaluation of the IT reliability in an organization, allowing them to effectively manage resources, elevate competitive advantages, and maximize the benefit of IT implementation (Ikhsan et al., 2021; Rusman et al., 2022).

This study aims to determine the capability level of the STIKI Malang information systems library using the COBIT 2019 framework. This research outcome was expected to help evaluate and provide feedback to the stakeholders on the current condition and the expected goal of IT governance. COBIT 2019, the most recent version of the COBIT framework, provides guidance on aligning IT governance with business objectives, ensuring a more holistic, flexible, and relevant governance framework (ISACA, 2018a). Several previous studies have confirmed the possibility of using this framework to conduct information system audits in various companies and other institutions (Francolla et al., 2022; Haay & Sitokdana, 2022; Lelengboto et al., 2022; Pradipta & Manuputty, 2022; Sipayung & Yunis, 2022).

## 2. Research Method

### 2.1 Research Design

This research adopted the Design Science Research Methodology (DSRM) model as a framework to conduct this research. This approach was also used in a prior study on information systems governance using COBIT 2019 (Yasin et al., 2020). This information system-oriented methodology facilitates the understanding process for conducting design science research in the information systems field (Peffer et al., 2008). The adopted research framework can be seen in the following Figure 1.

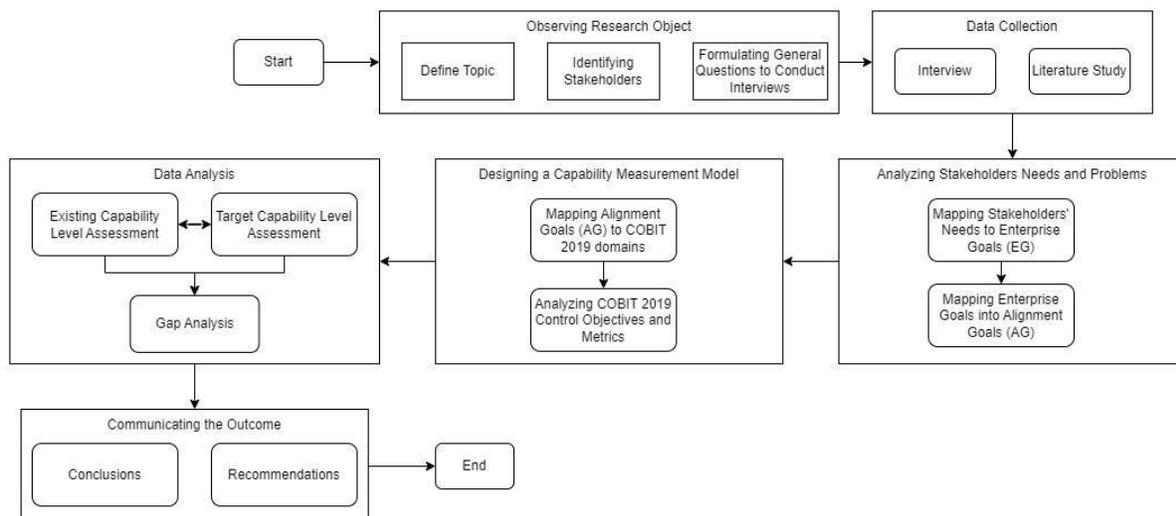


Fig 1. Research model

### 2.2 Data Collection

Data was collected using qualitative methods by conducting multiple interview sessions with the related stakeholders. The stakeholders are the Information Technology Office staff and the Head of the Library at STIKI Malang. The data collected in this study was primary (interview results) and secondary data (IT governance documents review). The questions used in the interview were based on a literature review (Faraby, 2023; Insani, 2021) and observations.

## **2.3 Analyze the Enterprise Goals (EG), Alignment Goals (AG), and Governance and Management Objectives (GMO)**

After the data was collected, the needs and drivers of each stakeholder were identified to be mapped into Enterprise Goals and Alignment Goals to align strategy and managerial goals. Then, alignment goals were mapped according to priority into Governance and Management Objectives. In this step, the researchers identified which activity needs to be evaluated.

## **2.4 Design Factors Calculation**

Design factors were used to help determine the level of urgency related to what objectives are important for measuring the level of capability. Only objectives scored  $\geq 75$  were chosen to measure their capability level based on the 11 design factors defined in COBIT 2019. The objectives with a score  $\geq 75$  indicated that they have a capability level target of level 4.

## **2.5 Capability Level Assessment**

Evaluation of the as-is and to-be capability levels in COBIT 2019 were measured based on the Capability Maturity Model Integration (CMMI). Evaluation of as-is and to-be capability levels in COBIT 2019 is measured based on the Capability Maturity Model Integration (CMMI). The chosen objectives were based on GMO mapping with capability levels ranging from level 0 (incomplete), level 1 (performed), level 2 (managed), level 3 (established), level 4 (predictable), to level 5 (optimizing). Detailed activities and their success indicators for measuring capabilities were referred to the 2019 COBIT book guidelines (ISACA, 2018b).

### **2.5.1 Capability Level Assessment**

The process capability level was obtained by calculating the average value of activities in each domain process and dividing it by the number of respondents.

$$\text{Capability level} = \frac{\sum \text{Average activity score}}{\text{total respondent}} \quad (1)$$

### **2.5.2 Rating Process**

After getting the capability level for each process, the next step was to give a process rating with the following calculations and conditions to determine if specific objectives achieved the capability level using the following formula:

$$\text{Rating Process} = \frac{\text{Capability level achievement}}{\text{maximum score}} \quad (2)$$

Fully achieved is a capability level of more than 85%. Largely achieved is a capability level of more than 50 to 85%. Partially achieved is a capability level between 15 to 50%. Not achieved is a capability level of less than 15% (Herianto & Wasilah, 2022).

## **2.6 Gap Analysis and Proposed Recommendation**

The gap level was obtained by comparing the current value of each process domain with the expected value based on the design factors. The results of this comparison produced a difference or gap between the two values. Lastly, recommendations were given based on the difference between the value in each process domain and the expected value. The results of the suggestions will become evaluation material for the STIKI Malang Library in IT governance and management.

## **3. Results and Discussion**

### **3.1 Analysis of Stakeholders' Needs and Drivers**

Interviews conducted with the Head of the Library and Staff of the STIKI Malang Information Technology Office suggested several aspects needed to be reviewed, especially in risk management (IT and business operations) and the creation of policies/standard of procedures (SOP), especially for collection, management, and library services.

©2023 J-Intech. Published by LPPM STIKI Malang

This is an open access article under the CC BY SA license. (<https://creativecommons.org/licenses/by-sa/4.0/>)  
318

### 3.2 Enterprise Goals, Alignment Goals, and Governance and Management Objectives Analysis

#### 3.2.1 Enterprise Goals (EG)

Based on the interview sessions held, the needs and drivers of each stakeholder were focused on the Financial and Customer aspects of the Balanced Scorecard. The identification results can be seen in Table 1 below.

Table 1. Enterprise Goals Identification

Enterprise Goals	Balance Scorecard (BSC) Dimension	Enterprise Goals	Business Goals
EG 01	Financial	Portfolio of competitive products and services	Human resources capabilities in developing IT
EG 02	Customer	Customer-oriented service culture	Improvement of policies related to library services
EG 06	Customer	Business service continuity and availability	Improvement of management services.

#### 3.2.2 Alignment Goals (AG)

Alignment Goals were determined by mapping the table with Enterprise Goals to get AG with a value of "P" (Primary). Figure 2 shows the mapping results of Enterprise Goals and Alignment Goals.

	EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
	Portfolio of competitive products and services	Managed business risk	Compliance with external laws and regulations	Quality of financial information	Customer-oriented service culture	Business service continuity and availability	Quality of management information	Optimization of internal business process functionality	Optimization of business process costs	Staff skills, motivation and productivity	Compliance with internal policies	Managed digital transformation programs	Product and business innovation
AG01			P								S		
AG02		P											
AG03					S			S	S			P	
AG04				P			P		P				
AG05	P				S			S				S	
AG06	P				S			S				S	S
AG07		P				P							
AG08	P				P			S		S		P	S
AG09	P				S			S	S			P	S
AG10				P			P		S				
AG11		S	P								P		
AG12					S					P			
AG13	P		S									S	P

Fig 2. Alignment Goals Identification

#### 3.2.3 Governance and Management Objectives

The next step is to determine the priorities of the Governance and Management Objectives (GMO) by mapping them with Alignment Goals. The result of mapping Governance and Management Objectives with Alignment Goals can be seen in Figure 3 below.

	AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
	IT compliance and support for business compliance with laws and regulations	Managed IT related risk	Realized benefits from IT enabled investments and services portfolio	Quality of technology related financial information	Delivery of IT services in line with business requirements	Agility to turn business requirements into operational solutions	Security of information, processing infrastructure and applications, and privacy	Enabling and supporting business processes by integrating applications and technology	Delivering programs on time, on budget and meeting requirements and quality standards	Quality of IT management information	IT compliance with internal policies	Competent and motivated staff with mutual understanding of technology and business	Knowledge, expertise and initiatives for business innovation
EDM01	P		P					S			S		
EDM02			P			S		S					S
EDM03	S	P									S		
EDM04			S			S		S	P			S	
EDM05				S						P	S		
AP001	S		P					S	S	S	P		
AP002			S			S		P				S	
AP003			S			P		P					
AP004			S			P		S				S	P
AP005			P					S	S				
AP006			S	P					P	S			
AP007			S					S	S			P	P
AP008			S			P		S	S			P	P
AP009								S					
AP010								S					
AP011			S	S					P	P			
AP012		P					P						
AP013	S	S											
AP014	S	S		S						P			
BAI01			P			S		S	P				
BAI02			S			P		S	P			S	
BAI03			S			P		S	P				
BAI04								S					
BAI05			P			S		P	P			S	
BAI06		S				P		S					
BAI07		S				P		S					
BAI08			S			S		S	S			P	P
BAI09				P						S			
BAI10							P						
BAI11			P			P			P				
DSS01								S					
DSS02		S						S					
DSS03		S						S					
DSS04					P			P					
DSS05	S	P			S		P	P			S		
DSS06	S	S			S		S	P			S		
MEAO1	S		S		P			S	S	P	S		
MEAO2	S	S		S	S		S		S	S	P		
MEAO3	P										S		
MEAO4	S	S		S	S		S			S	P		

Fig 3. Governance and Management Objectives Identification

### 3.3 Design Factors Calculation

The design factors calculation was conducted to determine the urgency of measuring the capability level of each objective in the COBIT 2019 framework. The result suggested that three objectives needed to be measured. Those were the following:

- APO 12 - Managed Risk (85),
- BAI10 Managed Configuration (85), and
- DSS04 – Managed Continuity (85).

These three objectives have an urgency value equal to 85, suggesting that they have a target capability level of level 4. The results of the design factors calculation can be seen in the following Figure 4.

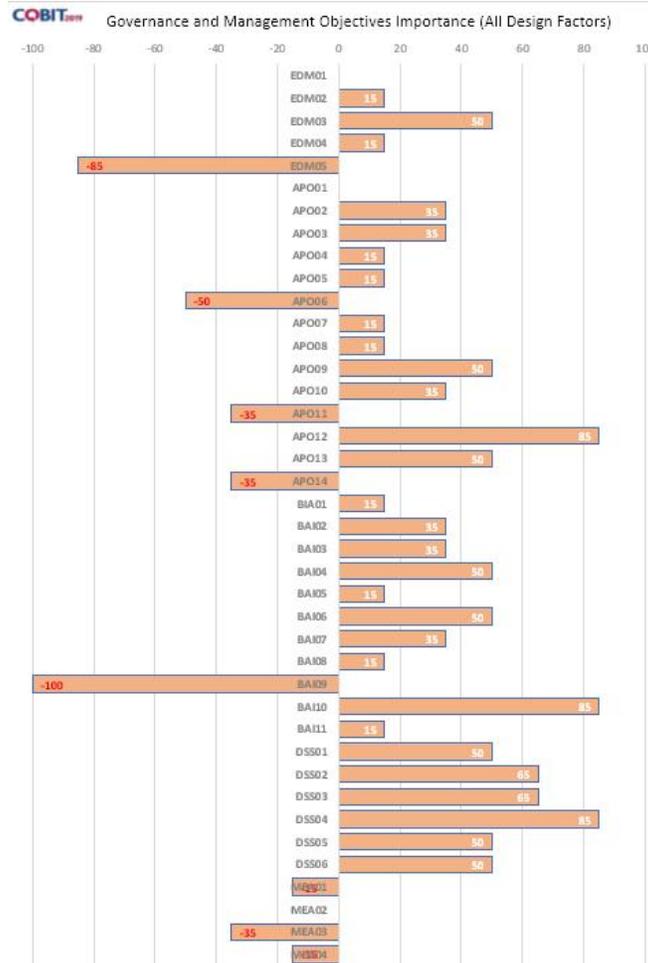


Fig 4. Governance and Management Objectives Identification

### 3.4 Current Capability Level Analysis (as-is)

The findings for the current (as-is) capability level of each objective process can be seen in Table 2 below.

Table 2. Current Capability Level

Objectives	Level	Findings
APO12 – Managed Risk	3	The STIKI Malang Library Information Systems suggested capability level 3. This shows that each process has been well-defined. The Office of Technology Information and the Library have routinely carried out internal audits, assurance reviews, and reporting and documenting the faced risks.
BAI10 – Managed Configuration	3	The STIKI Malang Library Information Systems currently shows capability level 3. The configuration has been defined according to stakeholder needs and is always reviewed whenever an internal audit is carried out
DSS04 – Managed Continuity	3	The STIKI Malang Library Information Systems currently shows capability level 3. Potential and risk analysis has been identified, each position has been well defined, and training and internal evaluations have been routinely carried out every predetermined period.

### 3.5 Expected Capability Level Analysis (to-be)

The desired capability level for each objective is obtained based on the analysis of the design factors. To achieve this level, the organization must meet a certain threshold according to the COBIT 2019 framework, which the summary is shown in the Achievement Description. The analysis of the desired capability level can be seen in Table 3 below.

*Table 3. Expected Capability Level*

No	Objective	Level	Achievement Description
1	APO12 Managed Risk	4	The STIKI Malang Library Information Systems have periodically and thoroughly analyzed the historical I&T risk data and have a mitigation plan that allows quick identification and monitoring of current risk trends. It also has validated the risk and business impact analysis upon decision making, continuously updating and reporting its risk profile, and comparing IT incidents against risk tolerance thresholds.
2	BAI10 Managed Configuration	4	The STIKI Malang Library Information Systems have conducted periodical verification of its live configuration items as defined in the repository, continually reporting and refining the repository's integrity to remove any unauthorized assets and maintaining completeness targets based on the business needs and objectives.
3	DSS04 Managed Continuity	4	The STIKI Malang Library Information Systems thoroughly assessed their human resources capabilities by conducting a post-exercise debriefing, monitoring competencies, evaluating adherence to the documented business continuity and disaster response plan, and determining the effectiveness of plans and overall organizational structures capabilities.

### 3.6 Gap Analysis

Gap analysis compares the current capability level (as-is) with the expected capability (to-be) to provide appropriate recommendations to achieve the desired targets. As seen in Table 4, all the objectives in this study suggested a one-level gap between the existing and the desired capabilities.

*Table 4. Gap Analysis*

No	Objective	as-is	to-be	gap
1.	APO12 - Managed Risk	3	4	1
2.	BAI10 - Managed Configuration	3	4	1
3.	DSS04 - Managed Continuity	3	4	1

The capability level assessment and gap analysis concluded all objectives (APO12 - Managed Risk, BAI10 - Managed Configuration, and DSS04 - Managed Continuity) currently operating at COBIT 2019 capability level 3, indicated that the process is well-defined and established. However, the findings also indicate a gap between the existing and the desired capability level across these three objectives, with all having the desired capability level of 4. The library information systems need to improve aspects in these three areas, mainly IT risk/incident management and human resource management. It must also demonstrate a mature, predictive, data-driven, and proactive strategy well-aligned with the business objectives.

## 4. Conclusions

This study aims to evaluate the capability level of the STIKI Malang information systems library with the COBIT 2019 framework. The three objectives (APO12 - Managed Risk, BAI10 - Managed Configuration, and DSS04 - Managed Continuity) were chosen to be evaluated based on COBIT 2019 design factors. The result suggested that all three objectives were currently at level three with the desired capability of level four. STIKI

Library Information Systems may consider applying these recommendations to achieve the desired capability levels:

- APO12 – Managed Risk

Implement periodical review of IT risk analysis based on historical data and utilizing data science methods to develop a predictive risk evaluation and quantify the magnitude of risks. Regularly update risk profiles to reflect evolving business trends and integrate them with business and technological strategies to strengthen risk prevention. Developing a comprehensive IT disaster recovery plan that covers all possible IT incident scenarios and continuously updating it based on emerging trends will help ensure proactive risk mitigation. Establishing frequent reporting activities and collaboration with management will ensure diverse insights, a comprehensive understanding of risks, and minimization of risk oversight. Incorporating insights from internal auditors and other stakeholders in the risk profile will also help identify gaps, enhance the robustness of the risk management process, and ensure alignment with business objectives.

- BAI10 - Managed Configuration

Enhance the configuration management system with dynamic and advanced automation/integration tools. This includes real-time configuration items monitoring to detect unauthorized access, automated alerts for any discrepancies between the live and the repository configuration, regularly reporting any deviations found in the physical configuration (as defined in the repository) to the management, and strengthening the configuration management process to not only react to changes but also proactively evolving based on the business needs and technological advancements. The organization may also provide hands-on training for staff responsible for updating and maintaining configurations, ensuring the staff understands the importance of accurate data, how to update the system, and how to react to incidents related to configuration management.

- DSS04 - Managed Continuity

Conduct regular and comprehensive scenario-based training sessions covering a wide range of potential operational disruptions, particularly focusing on operational disruptions, cyber threats, data breaches, and compliance with the operational standard procedure defined by the management. The feedback from training sessions can be incorporated to refine and expand the disaster response plan regularly. Continuously updating the plan to reflect rapid changes in the business environment will ensure the effectiveness and adaptability of the plan in addressing business issues. Developing clear and easy-to-understand documentation for disaster response can be done by defining action plans and checklists for specific IT disruption scenarios. Collaborating with external parties may also improve human resource competencies and compliance, gain new insights for evaluating the organization's current condition, and introduce staff to advanced business practices, cutting-edge technology, and risk management innovation.

In concluding the analysis, certain limitations might impact the comprehensiveness of this study. Firstly, the objective processes selected to conduct capability analysis were limited in scope, with only three objectives taken (APO12, BAI10, and DSS04), potentially omitting more extensive factors that could influence the library's operational services. This selective approach could potentially lead to an incomplete and skewed understanding of the library information systems' overall capabilities. Secondly, the data quantity used in this study was limited, potentially compromising the data's robustness, and posing a risk of overgeneralized results. Additionally, with a narrow data set, there is a tendency to draw extensive and biased conclusions, potentially misleading the decision-making process. Future analyses should aim for a more comprehensive range of objectives and a larger, more diverse dataset to ensure the accuracy and robustness of the assessment. Incorporating more extensive data sources and expanding the data collection method (key performance indicators, success metrics, more diverse insights from all personnel involved, and comprehensive document analysis) will ensure that the analysis accurately reflects actual overall capabilities and appropriately provides strategies to achieve business objectives.

## 5. References

Dalbehera, S. (2020). Measuring Service Quality in Digital Library Services by the Research Scholars of S.O.A. University of Odisha Using E-S-QUAL Model. In *International Perspectives on Improving Student*

*Engagement: Advances in Library Practices in Higher Education* (Vol. 26, pp. 111–126). <https://doi.org/10.1108/S2055-364120200000026007>

Faraby, M. A. (2023). *Audit Tata Kelola Teknologi Informasi Pada Dinas Komunikasi dan Informatika Kabupaten Agam Menggunakan Framework Cobit 2019* [UIN Syarif Hidayatullah Jakarta]. <https://repository.uinjkt.ac.id/dspace/handle/123456789/71422>

Francolla, G. B. R., Mandoya, G. R., Debora, M., Lompoliu, E., & Mambu, J. Y. (2022). *Information Technology Governance Audit Using The COBIT 2019 Framework at XYZ Institution*, 8(2), 346–358. <https://doi.org/10.31154/cogito.v8i2.427.346-358>

Haay, N. H., & Sitokdana, M. N. N. (2022). Analysis of Information Technology Governance on Communication and Information Service of Papua Province Using COBIT 2019. *Journal of Information Systems and Informatics*, 4(2), 349-360. <https://doi.org/10.51519/journalisi.v4i2.260>

Herianto, & Wasilah. (2022). Assessment Capability Level dan Maturity Level Tata Kelola TI pada Kantor Kementerian Agama Kabupaten Pesawaran Provinsi Lampung Menggunakan Framework COBIT 2019. *KONSTELASI: Konvergensi Teknologi Dan Sistem Informasi*, 2(2). <https://doi.org/10.24002/konstelasi.v2i2.5553>

Ikhsan, M., Widodo, A. P., & Adi, K. (2021). Systematic Literature Review on Corporate Information Technology Governance in Indonesia using Cobit 2019. *Prisma Sains: Jurnal Pengkajian Ilmu Dan Pembelajaran Matematika Dan IPA IKIP Mataram*, 9(2), 354. <https://doi.org/10.33394/j-ps.v9i2.4370>

Insani, T. M. (2021). *Audit Tata Kelola Teknologi Informasi Pada Balai Penelitian Sungei Putih Menggunakan Framework COBIT 2019* [Universitas Islam Negeri Sumatera Utara]. <http://repository.uinsu.ac.id/id/eprint/13016>

ISACA. (2018a). *COBIT® 2019 Framework: Introduction and Methodology*. ISACA.

ISACA. (2018b). *COBIT 2019 Framework Governance and Management Objectives*. ISACA.

Lelengboto, A., Mandoya, G., & Mambu, J. Y. (2022). Tailoring Governance System Design Through Capability Level Identification Using COBIT 2019 at a Paper and Mills Company. *JURIKOM (Jurnal Riset Komputer)*, 9(6), 1865. <https://doi.org/10.30865/jurikom.v9i6.5192>

Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24(3), 45–77, DOI: 10.2753/MIS0742-122240302

Pradipta, A. W., & Manuputty, A. D. (2022). Perancangan Tata Kelola Teknologi Informasi Menggunakan COBIT 2019 Pada Dinas Perpustakaan Dan Kearsipan Kota Salatiga. *Journal of Software Engineering Ampera*, 3(3), 153–169. <https://doi.org/10.51519/journalsea.v3i3.287>

Rusman, A., Nadlifatin, R., & Subriadi, A. P. (2022). Information System Audit Using COBIT and ITIL Framework: Literature Review. *Sinkron*, 7(3), 799–810. <https://doi.org/10.33395/sinkron.v7i3.11476>

Sipayung, A. B., & Yunis, R. (2022). *Evaluation Of Information Technology Governance at Mikroskil University Using COBIT 2019 Framework with BAI11 Domain*. *International Journal of Research and Applied Technology (INJURATECH)*, 2(2), 128-143. <https://doi.org/10.34010/injuratech.v2i2.8085>

Yasin, M., Akhmad Arman, A., Edward, I. J. M., & Shalannanda, W. (2020). Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ). *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, 1–5. <https://doi.org/10.1109/TSSA51342.2020.9310875>