JOURNAL OF APPLIED INFORMATION SYSTEMS AND INFROMATICS

INFORMATION TECHNOLOGY GOVERNANCE ASSESSMENT USING THE COBIT 2019 FRAMEWORK AND ISO/IEC 38500 AT RSUD XYZ

Berliana Azzahra [a], Andi Nur Rachman[b,*], Euis Nur Fitriani Dewi [b]

[a] *Department of Informatic, Siliwangi University, Tasikmalaya, Indonesia*
[b] *Department of Information System, Siliwangi University, Tasikmalaya, Indonesia*
Corresponding author: andy.rachman@unsil.ac.id

***Abstract*— The advancement of Information Technology (IT) is a crucial prerequisite for bolstering the efficacy and efficiency of organizational operations, encompassing healthcare establishments like RSUD XYZ. But problems like unreliable networks, antiquated computers, and a lack of IT knowledge in human resources (HR) arise. Therefore, to guarantee efficient IT usage, a thorough IT governance assessment is required. In order to help overcome current challenges, this study intends to assess IT governance at RSUD XYZ utilizing the COBIT 2019 framework and ISO 38500 standards.**

Three primary processes are assessed using the Capability Maturity Model Integration (CMMI) framework: Ensured Risk Optimisation (EDM03), Managed Risk (APO12), and Human Resources (APO07). According to the evaluation results, APO07 successfully attained level 4 as intended, APO12 was at level 3 of goal 5, and the EDM03 process was at level 2 of target 4. The identified competency gaps formed the basis for the preparation of improvement recommendations. In addition, this research also proposes introducing other processes such as ITIL for IT service management and TOGAF integration to support enterprise architecture.

It is anticipated that these findings would enable agencies to strengthen their IT governance capacities in order to minimize current gaps and meet more ideal goals. This study offers RSUD XYZ thorough guidelines for enhancing more effective and efficient IT governance, hence facilitating the integration of IT plans with hospital business objectives.

***Keywords*— Information Technology, IT Governance, COBIT 2019, ISO 38500.**

Manuscript received 19 Sep. 2024; revised 22 Sep. 2024; accepted Nov. 2024. Date of publication Nov. 2024.

I. INTRODUCTION

Information Technology (IT) has now become a very important requirement for almost all corporate organizations, both government and private, as a support in improving the effectiveness and efficiency of the performance process [1]. IT implementation has a high risk and requires a large investment, so IT implementation must be thoroughly monitored against IT governance mechanisms so that it can really help companies achieve their business goals in an effective and efficient way [2], [3], [4], [5]. Information technology governance is a framework of policies or procedures and a series of organizational processes that aim to ensure the alignment of IT implementation with efforts to achieve institutional goals, by optimizing the benefits and opportunities provided by IT, managing the use of IT resources, and managing IT-related [6], [7], [8], [9]

XYZ Regional General Hospital is one of the agencies engaged in the health sector. Based on an interview with one of the IT staff at XYZ RSUD, information was obtained about the problems currently faced. Some of the problems faced are networks that are often disconnected and the use of outdated computers, so that the computer equipment is less capable of processing data or systems optimally. In addition to problems with the equipment, the management of Human Resources (HR) is also still relatively minimal in understanding IT. Utilization of governance at XYZ Hospital can help analyze deficiencies in hardware, software, and brainware aspects, so that obstacles to employee performance in providing services can be overcome. Based on the existing problems, IT governance needs to be implemented through a capability assessment using the information technology assistance assessment scheme [10], [11]

There are several information technology governance frameworks in managing IT. These frameworks include the International Standard Organization (ISO), Information Technology Infrastructure Library (ITIL), Control Objectives for Information and related Technology (COBIT). Based on the research analysis of [12]. The difference between COBIT and other frameworks / standards is that COBIT provides a more comprehensive framework, by aligning all relevant standards at the highest level such as ITIL, TOGAF. Various

studies have explored the implementation of IT governance using the COBIT framework with ISO 38500 integration in various organizations. [13] proposed an integrated approach, mapping the main principles of ISO 38500 with COBIT 2019 domains and processes, this approach proved to be effective in the significance of the importance of IT work within the organization and studying the limitations of the organization in detail in order to select processes, practices that are suitable for the organization. And research by [14]. found that the use of COBIT 5 and ISO 38500 frameworks resulted in better governance, with [14] specifically recommending the use of ISO 38500 to achieve higher capability levels, but there are research gaps that are of major concern according to [15]. COBIT 5 is considered less flexible regarding the activity assessment process including in terms of COBIT process objectives. COBIT 2019 reflects profound changes in current technological demands and a maturing understanding of best practices in IT management [16], [17], [18].

The reference will be used as a reference in this study which focuses on conducting research that can help agencies to produce an IT governance assessment at XYZ Hospital with an update on the different activity level assessment processes using the CMMI-based capability model process. ISO 385000 was chosen together with COBIT 2019 to support recommendations from the evaluation results carried out according to the principles of the ISO / IEC 38500 standard to achieve a higher level of capability. The use of COBIT 2019 and ISO 38500 best practices in organizational strategic planning or considering the optimal IT position in accordance with business objectives [13].

II. THE MATERIALS AND METHOD

To examine IT governance in a business or organization, the study steps include altering the COBIT 2019 framework and including ISO/IEC 38500. The goal of this research is to ensure that a company's IT operations are in line with its business strategy.

A. Data Collection Methods

Where in this observation, the researcher monitors how the condition of the RSUD itself, then the researcher conducts an interview with an expert in the field of IT governance, namely the Head of IT. In this interview, the researcher obtained some information related to the IT governance process, as well as getting an overview of the problems faced by XYZ Hospital then a literature study was conducted in the context of this research to collect data, references, and recommendations that are in accordance with the problem under study. Journals, company documents, COBIT 2019 modules published by ISACA, and previous research can provide theories and explanations that researchers use to support this research.

B. Data Processing

The data analysis stage in this research was obtained from the data collection method section. Some processes data processing include:

1) *Capability Level (as-is):* The capacity level of a process within an organization is known as Capacity Level Process (CLP). These results were collected through surveys that had previously been sent to the agency, observations and interviews and then obtained the as-is capability results.

2) *Capability Level (to-be):* In the COBIT 2019 Framework module: Governance and Management Objectives, it has been determined to determine the target competency level for each objective process. Then the expected target capability level (to-be) is appropriate in terms of COBIT 2019 objective process measurement.

3) *Gap Analysis:* When the expected (to-be) and current (as-is) capability levels are known, a gap analysis is performed. The purpose of this analysis is to identify IT governance tasks that require improvement so that the current level of competence (as-is) can eventually rise to the expected level of capability (to-be).

C. Reporting of results and recommendations for improvement

A report summarizing the findings of the capability level and gap analysis, which can be used as improvement suggestions to achieve the desired state (to-be) in accordance with ISO/IEC 38500 principles.

III. RESULT AND DISCUSSION

A. COBIT 2019 Process Objective Mapping

From each Governance Management Objectives in COBIT 2019, of course, it has detailed control objectives as a control tool for the GMO itself. The following are detailed control objectives EDM03, APO12, APO07 which have become process objectives in this study based on COBIT 2019 and the background of the research problem.

1) *Mapping Enterprise Goals with Alignment Goals*

Identifying Alignment goals (AG) from Enterprise goals that have been mapped previously. In determining this, namely using the mapping table of the Enterprise Goals obtained with the Primary value or symbol “P” in the COBIT 2019 Framework module: Governance and Management Objectives [19]. From the identification mapping of Enterprise goals, it can be concluded which Alignment goals can be aligned with the company's business. The mapping of the identification of Alignment goals from Enterprise goals is as follows.

TABLE I
ENTERPRISE GOALS TO ALIGNMENT GOALS MAPPING

Kode EG	Enterprise goals	Kode AG	Alignment goals
EG06	Continuity and accessibility of business administration	AG07	Privacy, processing infrastructure and applications, and information security.
EG10	Staff skills, motivation and productivity.	AG12	Competent and motivated staff with a mutual understanding of technology and business.
EG13	Product and business advancement	AG13	Business expertise, knowledge and innovation efforts.

2) *Governance and Management Objectives Alignments goals Mapping*:

Then, from the mapping above, the results are shown in the table below:

TABLE 2
MAPPING GOVERNANCE AND MANAGEMENT OBJECTIVES

AG	*Governance and Management Objectives*					
AG07	EDM03	APO12	APO13	BAI10	DSS04	DSS05
AG12	APO07	APO08	BAI08			
AG13	APO04	APO07	APO08	BAI08		

3) *Critical Point Alignment*

The next stage of the alignment goal is the identification of IT processes. IT process identification is carried out by referring to the IT processes contained in the 2019 COBIT book. At this stage, the IT processes that are selected based on the objectives are The alignment will be readjusted to the critical points so that the appropriate IT processes will be obtained.

TABLE 3
MAPPING GOVERNANCE AND MANAGEMENT OBJECTIVES

No	Domain	IT Process	Critical Point
1	EDM03	Ensured Risk Optimization	Obstacles in infrastructure issues connecting with partners such as network outages, damaged computer hardware.
2	APO12	Managed risk.	Report management is not yet orderly
3	APO07	Managed human resources.	Managerial roles and human resources that are classified as still lacking IT and limited IT personnel.

It can be seen in table 3 that the objective process has been concluded based on the mapping stage of enterprise goals, alignment goals, and crisis points in the company. The researcher concluded that the objective process that the researcher will audit is:

a. EDM03 – Ensured Risk Optimization
b. APO07 – Managed Human Resources
c. APO12 – Managed Risk

The reason the researcher chose these three domains or objective processes is because the background of the problem at RSUD XYZ is closely related to human resources, ensuring risk optimization, and how this RSUD anticipates risks.It can be said, that these three things are very related and researchers must conduct an audit in order to know the capability level of each of these process objectives.

B. Capability Level Analysis

In this study, the determination of the level of capability that will be carried out in each IT process starts from level 2 (two) to level 5 (five) [18]. The availability of levels for each activity certainly refers to the COBIT 2019 Framework guidebook: Governance and Management Objectives. As already explained, the questionnaire will be distributed in the form of a Guttman Scale value that is worth Yes (1), or No (0), to respondents who have been adjusted to the RACI Chart mapping[20]. Each question has 4 to 5 levels.

1) Calculation Capability Level EDM03 - Ensured Risk Optimization:

The following are the results of the calculation of the capability level process data questionnaire that has been distributed to the objective process EDM03 at RSUD XYZ.

TABLE 4
TABLE 4. DATA PROCESSING CAPABILITY LEVEL QUESTIONNAIRE - EDM03

EDM03 – *Ensured Risk Optimization*								
Level	**Level**	**Process**	**Responden**				**Total**	
			R1	**R2**	**R3**	**R4**	**Score (%)**	**Score (%)**
2	EDM03.01	1	1	1	0	0	50	62,5
		2	1	1	0	1	75	
		3	1	1	0	1	75	
		4	1	0	0	1	50	
	EDM03.02	1	1	1	0	1	75	93,75
		2	1	1	1	1	100	
		3	1	1	1	1	100	
		4	1	1	1	1	100	
	EDM03.03	1	1	1	0	1	75	75

Table 4 shows that the objective process EDM03 - Ensured Risk Optimization at RSUD XYZ has a maturity level value of 77.7%, which means that the capability level is at the Largely level (50%-85%), It can be concluded that the capability level objective process EDM03 at RSUD XYZ has an audit status not achieved at level 2 and stopped at the level assessed, namely level 2, then did not proceed to the calculation of capability level 3.

2) Caculating Capability level APO07 - Managed Human Resources.

The following are the results of the calculation of the capability level process data questionnaire that has been distributed at objective process APO07 at RSUD XYZ.

TABLE 5
DATA PROCESSING CAPABILITY LEVEL QUESTIONNAIRE – APO07

APO07 – *Managed Human Resources*									
Level	**Level**	**Process**	**Respondents**					**Total**	
			R1	**R2**	**R3**	**R4**	**R5**	**Score (%)**	**Score (%)**
2	APO07.01	1	1	1	1	1	1	100	100
		2	1	1	1	1	1	100	
		3	1	1	1	1	1	100	
	APO 07.02	1	1	1	1	1	1	100	80
		2	1	1	0	0	1	60	
		3	1	1	1	1	0	80	
	APO 07.03	1	1	1	1	1	1	100	90
		2	1	1	1	1	0	80	
	APO 07.04	1	1	1	1	0	0	60	70
		2	1	1	1	0	0	60	
		3	1	0	1	1	1	80	
		4	1	0	1	1	1	80	
	APO 07.05	1	1	1	1	1	1	100	100
	APO 07.06	1	1	1	1	1	1	100	92
		2	1	1	1	1	1	100	
		3	1	0	1	0	1	60	
		4	1	1	1	1	1	100	
		5	1	1	1	1	1	100	
3	APO 07.01	1	1	1	1	1	1	100	100
	APO 07.02	1	1	1	1	0	0	60	60
	APO 07.03	1	1	1	1	0	1	80	86,67
		2	1	1	1	1	1	100	
		3	1	1	1	1	0	80	
	APO 07.04	1	1	1	1	1	1	100	95
		2	1	1	1	1	0	80	
		3	1	1	1	1	1	100	
		4	1	1	1	1	1	100	
	APO 07.05	1	1	1	1	0	1	80	90
		2	1	1	1	1	1	100	
	APO 07.06	1	1	0	1	0	1	60	60
4	APO 07.03	1	1	1	1	0	1	80	80
	APO 07.05	1	1	1	1	0	1	80	80
	APO 07.06	1	1	1	1	1	1	100	100
		2	1	1	1	1	1	100	

Table 5 shows that objective process APO07 - Managed Human Resources at RSUD XYZ has a maturity level value of 90%, which means that the capability level is at the Fully Achieved level (85%-100%). It can be concluded that the capability level objective process APO07 at RSUD XYZ has an audit status achieved at the expected target, namely the level of 4.

3) Calculating Capability level APO12 - Managed Risk

The following are the results of the calculation of the capability level process data questionnaire that has been distributed at objective process APO07 at RSUD XYZ.

TABLE 6.
DATA PROCESSING CAPABILITY LEVEL QUESTIONNAIRE – APO12

APO12 – *Managed Risk*								
Level	**Level**	**Process**	**Respondents**				**Total**	
			R1	**R2**	**R3**	**R4**	**Score (%)**	**Score (%)**
2	APO12.01	1	1	1	1	1	100	100
		2	1	1	1	1	100	
	APO12.03	1	1	0	1	1	75	66,67
		2	1	1	1	1	100	
		3	1	1	1	0	75	
	APO12.05	1	1	0	1	1	75	75
3	APO12.01	1	1	0	1	0	50	75
		2	1	1	1	1	100	
	APO12.02	1	1	0	1	1	75	75
		2	1	0	1	0	50	

	3	1	1	0	0	50	
	4	1	1	1	1	100	
	5	1	1	1	1	100	
	6	1	1	1	0	75	
APO12.03	1	1	0	1	0	50	50
	2	1	0	1	0	50	
APO12.04	1	1	1	1	1	100	93,75
	2	1	1	1	1	100	
	3	1	1	1	1	100	
	4	1	0	1	1	75	
APO12.05	1	1	1	0	0	50	62,5
	2	1	1	1	0	75	
APO12.06	1	1	1	1	1	100	100
	2	1	1	1	1	100	

Table 6 shows that the objective process APO12 - Managed Risk at RSUD XYZ has a maturity level value of 77.8%, which means that the capability level is at the Largely level (50%-85%), It can be concluded that the capability level of objective process APO12 at RSUD XYZ has an audit status not achieved at level 3 and stops at the assessed level, which is level 2, so it is not continued to the calculation of the capability level 4.

C. Capability Level Objective Process Result Conclusion

The results of the recapitulation of the capability level questionnaire data for RSUD XYZ for domain EDM03 (Ensured Risk Optimization), APO07 (Managed Human Resources) and finally APO12 (Managed Risk). The following is a graph of the capability level and gap level analysis for domains EDM03, APO07, and APO12:

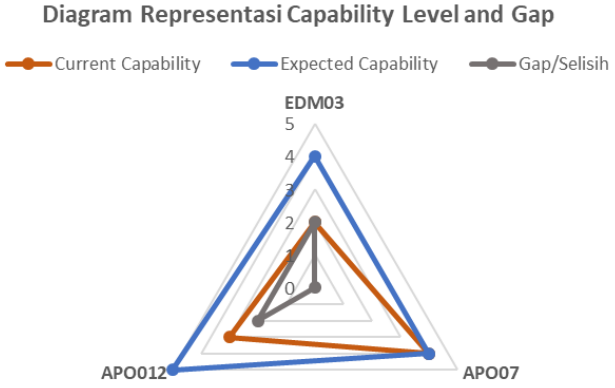

Fig. 2 Diagram Representasi Capability Level and Gap

Figure 2 is the result of the three process domains, EDM03 current condition is at level 2, which can be categorized as operationally running, there is a gap of 2 to achieve the expected process target. APO12, the current condition is at level 3, categorized as carried out in a more organized manner using organizational assets, there is a gap of 2 to achieve the expected process target. APO07 is at level 4, categorized as having achieved its objectives, being well defined and achieving the expected process targets.

D. Recommendations based on ISO 38500 activities

A report that summarizes the findings of the capability level and gap analysis, which can be used as recommendations/suggestions built in accordance with ISO/IEC 38500 principles as improvements to achieve the desired state (to-be), and aims to assure stakeholders that they can have confidence in the organization's IT governance by following the guidelines and procedures suggested by this standard, ISO/IEC 38500. There are 6 principles of enterprise IT governance outlined in ISO/IEC 38500 [21], these principles articulate the desired behavior that will direct the organization's decision making. The following are some recommendations for optimizing governance that can be implemented:

1) EDM03 – Ensured Risk Optimization
   - Responsibility
     RSUD XYZ plans, evaluates and monitors employee competencies to carry out the tasks and functions that have been determined for IT risk management. Periodically conduct a risk level assessment process so that the hospital can identify and manage risks, and protect the availability of information vital to hospital operations..
   - Strategy
     RSUD XYZ evaluates, directs and monitors the level of alignment of IT risk strategy with enterprise risk strategy and ensures that it is below the organizational risk capacity and associated risks that the company is willing to take in pursuit of corporate objectives.
   - Acqusition
     RSUD XYZ evaluates, directs and monitors risk management activities related to costs incurred to the possibility of risks that will occur both from investment to the use of technology that suits your needs.
   - Performance
     RSUD XYZ evaluates, directs and monitors key objectives and metrics of risk governance and management processes against targets, analyzes causes of deviations, and initiates corrective actions to address underlying causes.
   - Conformance
     RSUD XYZ evaluates, directs, and monitors IT strategy activities carried out in accordance with policies and procedures or does not violate existing rules that have been published and escalated or conveyed according to what happens in the field to the leadership.
   - Human Behaviour
     RSUD XYZ evaluates, directs, and monitors the training activities conducted so that the knowledge

delivered is relevant both related to IT competencies to responsibilities and reporting in accordance with applicable regulations. Then, identify and evaluate employee deviant behavior in IT activities.

2) APO12 – Managed Risk
- Responsibility
  RSUD XYZ evaluates, directs and monitors each organizational unit overseeing risks, takes responsibility and categorizes I&T risk control measures with capabilities, evaluates, directs and monitors process improvement, response requirement improvement. Ensure risk governance procedures cover causes, required responses and process improvements.
- Strategy
  RSUD XYZ evaluates, directs and monitors draft policies and plans related to I&T risk scenarios. Consider each relevant risk element and assess existing operational controls. Use third-party services to review and validate the results of the risk analysis and business impact analysis (BIA) to ensure accuracy and completeness.
- Acqusition
  RSUD XYZ directs, evaluates and monitors operational activities. Examine the costs and benefits of several risk response strategies, including accept and use, minimize and avoid. Verify the best risk response, calculate the probability and size of gain or loss associated with the I&T risk scenario.
- Performance
  RSUD XYZ directs, evaluates and monitors operational activities, implements a more in-depth and structured root cause analysis (RCA) method to identify the main factors that cause incidents and losses. In addition, ensuring which IT infrastructure resources and IT services are required to keep business processes running smoothly.
- Conformance
  RSUD XYZ directs, evaluates and monitors operational activities in accordance with applicable policies and rules, or does not violate existing rules and determines acceptable risks or high risks. Conduct periodic audits and then report the business impact to stakeholders to ensure alignment with company standards and needs.
- Human Behaviour
  RSUD XYZ evaluates, directs and monitors training activities to conduct surveys and data analysis more efficiently and accurately. Build partnerships with similar IT-related organizations to take responsibility and share incident data and risk trends. Participating in industry forums can help in gaining access to broader data.

3) APO07 – Managed Human Resources

RSUD XYZ continues to evaluate, direct, and monitor and ensure the company and IT functions have sufficient resources and identify the competencies and skills of currently available internal and external resources to support the company's goals and objectives. Maintain business and IT personnel recruitment and retention processes in line with overall company personnel policies and procedures.

IV. CONCLUSION

The capability level results for the EDM03 Ensured Risk Optimization process are at level 2 while the expected capability level target is 4 so that there is a Gap level of 2 to be able to achieve the expected target, so these results can be used as a reference for recommended improvements. Then the results of the capability level for the APO12 Managed Risk process are at level 3 while the expected target capability level is 5 so that there is a Gap level of 2 to be able to achieve the expected target, so these results can be used as a reference for making recommended improvements. On the other hand, the results of the capability level for the APO07 Human Resources process are at level 4 and the expected target capability level is 4 so that it has an audit status achieved at the expected target, which is level 4, so these results can be used as a reference for maintaining current capabilities. The results of the recommendations are compiled based on COBIT 2019 by aligning the principles in ISO 38500 as improvements to increase the level that has not been achieved / gap that exists.

REFERENCES

[1] R. T. F. Palar, Y. D. Y. Rindengan, and S. R. Sentinuwo, "Analisa Kematangan Dinas Komunikasi dan Informatika Kota Manado Menggunakan Framework COBIT 5 Pada Domain Monitor, Evaluate and Assess," *Jurnal Teknik Elektro dan Komputer*, 2021.

[2] E. Widilianie, A. D. Manuputty, E. W. Fakultas, and T. Informasi, "EVALUASI KINERJA SI PROJECT MANAGEMENT MENGGUNAKAN FRAMEWORK COBIT 5 SUBDOMAIN MEA 01," *Jurnal SITECH*, vol. 2, 2019, [Online]. Available: http://www.jurnal.umk.ac.id/sitech

[3] M. N. B. Lobo, T. V. Perez, and D. Rico-Bautista, "Systematic Mapping of Literature: Governance and IT Management Practices in organizations, under the COBIT 2019 reference framework," in *Applications in Software Engineering - Proceedings of the 11th International Conference on Software Process Improvement, CIMPS 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 1–9. doi: 10.1109/CIMPS57786.2022.10035692.

[4] E. Dela Marcela and M. Indah Fianty, "Performance Evaluation IT Governance on Universities: COBIT 2019 Approach with Measurement Capability Levels," *Indonesian Journal of Computer Science Attribution202*, vol. 12, no. 4, p. 1760, 2023.

[5] M. B. Ardima, R. Gernowo, and V. G. Slamet, "PENGUKURAN TINGKAT KAPABILITAS SISTEM TATA KELOLA TI MENGGUNAKAN COBIT 5 DENGAN ISO 38500 CAPABILITY LEVEL MEASUREMENT OF IT GOVERNANCE SYSTEM USING COBIT 5 WITH ISO 38500," vol. 7, no. 3, 2020, doi: 10.25126/jtiik.202073059.

[6] A. M. Syuhada, "Kajian Perbandingan Cobit 5 dengan Cobit 2019 sebagai Framework Audit Tata Kelola Teknologi Informasi," *Syntax Literate ; Jurnal Ilmiah Indonesia*, vol. 6, no. 1, p. 30, Jan. 2021, doi: 10.36418/syntax-literate.v6i1.2082.

[7] R. K. Sari, R. H. Ginardi, and A. S. Indrawanti, "Perancangan Tata Kelola Teknologi Informasi Berbasis COBIT 2019: Studi Kasus di Divisi Information Technology PT Telkom Indonesia Kota Bandung," *JURNAL TEKNIK ITS*, vol. 12, 2023.

[8] D. J. Robayo Jácome and V. D. L. M. Villarreal Morales, "Convergencia de COBIT e ISO 38500 en el Gobierno de Tecnologías de la Información," *INNOVA Research Journal*, vol. 5, no. 2, pp. 1–25, May 2020, doi: 10.33890/innova.v5.n2.2020.1163.

[9] D. Henriques, R. Pereira, R. Almeida, and M. M. da Silva, "It governance enablers," *Foresight and STI Governance*, vol. 14, no. 1, pp. 48–59, 2020, doi: 10.17323/2500-2597.2020.1.48.59.

[10] A. Wildan Aulia, M. Ulfa, and T. Ibadi, "Audit Tata Kelola Teknologi Informasi Di RSUD Sekayu Menggunakan Framework Cobit 2019," *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)*, vol. 8, no. 2, pp. 816–828, 2023, [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

[11] R. Moryanda, V. Pujani, and Y. Marpaung, "Evaluasi Sistem Informasi Manajemen Rumah Sakit Menggunakan Framework COBIT 2019 (Studi Kasus: Semen Padang Hospital)," *Jurnal Nasional Teknologi dan Sistem Informasi*, vol. 9, no. 3, pp. 299–306, Jan. 2024, doi: 10.25077/teknosi.v9i3.2023.299-306.

[12] P. Mulgund, P. Pahwa, and G. Chaudhari, "Strengthening IT Governance and Controls Using COBIT," *Int J Risk Conting Manag*, vol. 8, no. 4, pp. 66–90, Oct. 2019, doi: 10.4018/ijrcm.2019100104.

[13] B. Visitsilp and N. Bhumpenpein, "Guidelines for Information Technology Governance Based on Integrated ISO 38500 and COBIT 2019," in *Proceedings - 2021 Research, Invention, and Innovation Congress: Innovation Electricals and Electronics, RI2C 2021*, Institute of Electrical and Electronics Engineers Inc., Sep. 2021, pp. 14–18. doi: 10.1109/RI2C51727.2021.9559772.

[14] T. Toifur, K. Kusrini, and A. Budi, "Evaluation of Information Technology Governance Using COBIT 5 and ISO/IEC 38500," *Jurnal Online Informatika*, vol. 7, no. 1, p. 17, Jun. 2022, doi: 10.15575/join.v7i1.814.

[15] M. Ranjbarfard and S. R. Mirsalari, "IT Capability Evaluation through the IT Capability Map," 2020.

[16] Anadya Tafdhilla, J. Hasna Iftinan, Azzahra Rahmadani, and Anita Wulansari, "Penilaian Penggunaan Framework COBIT 2019 dalam Pengelolaan Teknologi Informasi Pada Institusi Perguruan Tinggi," *Bulletin of Computer Science Research*, vol. 4, no. 1, pp. 91–100, Dec. 2023, doi: 10.47065/bulletincsr.v4i1.314.

[17] I. Ayu, A. Padmi, D. Putra Githa, A. A. Ngurah, and H. Susila, "AUDIT TATA KELOLA TEKNOLOGI INFORMASI RUMAH SAKIT UMUM X MENGGUNAKAN FRAMEWORK COBIT 2019," 2022.

[18] ISACA, *COBIT 2019 Framework Governance and Management Objectives*. 2019.

[19] ISACA, *Implementing and Optimizing an Information and Technology Governance Solution Personal Copy of Madalin Bratu (ISACA ID: 1283013)*. 2019. [Online]. Available: http://linkd.in/ISACAOfficial

[20] ISACA, *COBIT 2019 Design guide designing an information and technology governance solution*. 2019.

[21] ISO/IEC 38500:2015, "IT Governance from the standardization perspective-ISO 38500:2015," 2018.