Journal of Emerging Information Systems and Business Intelligence
ISSN: 2774-3993
Journal homepage: https://ejournal.unesa.ac.id/index.php/JEISBI/

Risk Assessment on Wilujeng Hospital IT Process Using COBIT 2019 Framework

Sindy Rosita Sari[1], I Kadek Dwi Nuryana[2]

[1,2]*Information System, Faculty of Engineering, State University of Surabaya, Surabaya, Indonesia*

sindy.19001@mhs.unesa.ac.id, *dwinuryana@unesa.ac.id*

ABSTRACT

The utilization of information technology within hospitals introduced risks to both operational efficiency and patient information security. Risks at Wilujeng Hospital include information systems tracking not being updated by staff, human error due to a lack of computer skills, no available personnel dedicated to the protection of computer information, and no clear task for all staff members on how to understand systems. The hospital did not perform a risk management capability assessment which is an important part of assessing risk management maturity. This study reviewed Wilujeng Hospital's risk management capabilities using the COBIT 2019 framework and provided suggestions for improving governance. Data collection and analysis were based on the COBIT 2019 principles, specifically on capabilities through design factor analysis. The study examined three relevant components of COBIT, including DSS05 (Managed Security Services), APO07 (Managed Human Resources) and APO12 (Managed Risk). The findings indicated that all three areas achieved competency level 1 with respective scores of 61.5%, 80.55%, and 58.33%. This indicates that the hospital's risk management capabilities are still evolving and that security and human resources management should be improved to enhance IT governance and data protection.

Keywords : Risk, Capability, COBIT, Hospital, Wilujeng

Article Info:
Article history:
Received July 11, 2025
Revised August 27, 2025
Accepted September 11, 2025

Corresponding Author
Sindy Rosita Sari
Universitas Negeri Surabaya, Surabaya, Indonesia
sindy.19001@mhs.unesa.ac.id

1. INTRODUCTION

IT governance, or information technology management, is a key strategy for ensuring that an organization helps achieve its strategic and operational goals through IT investments [1]. Effective IT governance serves as a critical success factor (CSF) that improves organizational resources, performance, and goals [2].

Wilujeng Hospital in Kediri has implemented IT in its healthcare services. The IT Unit at Wilujeng Hospital is responsible for information systems, computer networks, software development and maintenance, and incident management.

However, the use of IT at Wilujeng Hospital faces many challenges, including human factors, lack of training for new staff, lack of specific SOPs on risk management, and lack of staff with data protection skills. In addition, Wilujeng Hospital has never conducted a risk or opportunity assessment to determine the level of risk management within the organization.

IT risk assessment is very important because it helps hospitals identify and evaluate the steps they can take to increase the chances of success and reduce the chances of failure. However, to date, Wilujeng Hospital has never conducted a systematic IT risk assessment.

Available IT risk management frameworks include COBIT, COSO, ITIL, ISO, and the IT Risk Framework; COBIT (Control Objectives for Information and Related Technologies), published by ISACA, provides guidance on what organizations can do for IT in terms of controls, activities, measurement, and documentation [3] COBIT has become a global guide for IT governance and management, and the latest version of COBIT 2019 is recognized as practical and relevant to business needs. COBIT 2019 is recognized as practical and relevant to business needs [4].

In this study, the COBIT 2019 framework is used to assess IT risk management by analyzing the capabilities of Wilujeng Hospital focusing on the areas DSS05, APO07, and APO12. The analysis is expected to determine the level of Wilujeng Hospital's capabilities to address the identified risks and identify the gap between expected and current levels.

2. METHODS

This research adopts the COBIT 2019 framework to assess IT governance process capability within the organization. The methodology begins with structured interviews to identify key issues, followed by mapping enterprise goals and alignment goals aligned with the institution’s vision and mission. Subsequently, the 10 Design Factors are analyzed using the COBIT 2019 Design Toolkit to determine high-priority domains within the COBIT Core Model. These selected domains are used as focal points for capability assessment, with relevant respondents identified through RACI diagram mapping. Data were collected via questionnaires and analyzed using the Guttman Scale to quantify the actual capability level of each IT process. The results were then compared to the target level through gap analysis, which formed the basis for making recommendations of mitigation suggestions for improved governance and associated risk strategies.

3. RESULTS AND DISCUSSION

3.1. Mapping Enterprise Goals and Alignment Goals to IT Related Goals

Through interviews and document analysis, organizational goals were identified and a mapping table was developed to align them with relevant enterprise goals. the results obtained from mapping the company's vision and mission to COBIT Enterprise Goals are EG05 Customer-oriented Service Culture, EG10 Staff Skills, Motivation, and Productivity and EG02 Managing Business Risks.

Table 1. Mapping Enterprise Goals (EG) to Alignment Goals (AG)

Enterprise Goals	Alignment Goals	Relation
EG05	AG05, AG12	Primary
EG10	AG12	Primary
EG12	AG12	Primary

The mapping results from enterprise goals to alignment goals show results AG05 (Delivery of I&T Services in Line with Business Requirements), AG12 (Competent and Motivated Staff with Mutual Understanding of Technology and Business Innovation), and AG02 (Managed I&T Related Risk).

3.2. Defining the Scope of the Governance System

This stage is a process in determining the scope of the governance system by considering the 10 Design Factors analyzed using the Design Toolkit. The determination of this stage was carried out through document analysis and interviews with the IT Unit Manager at Wilujeng Hospital.

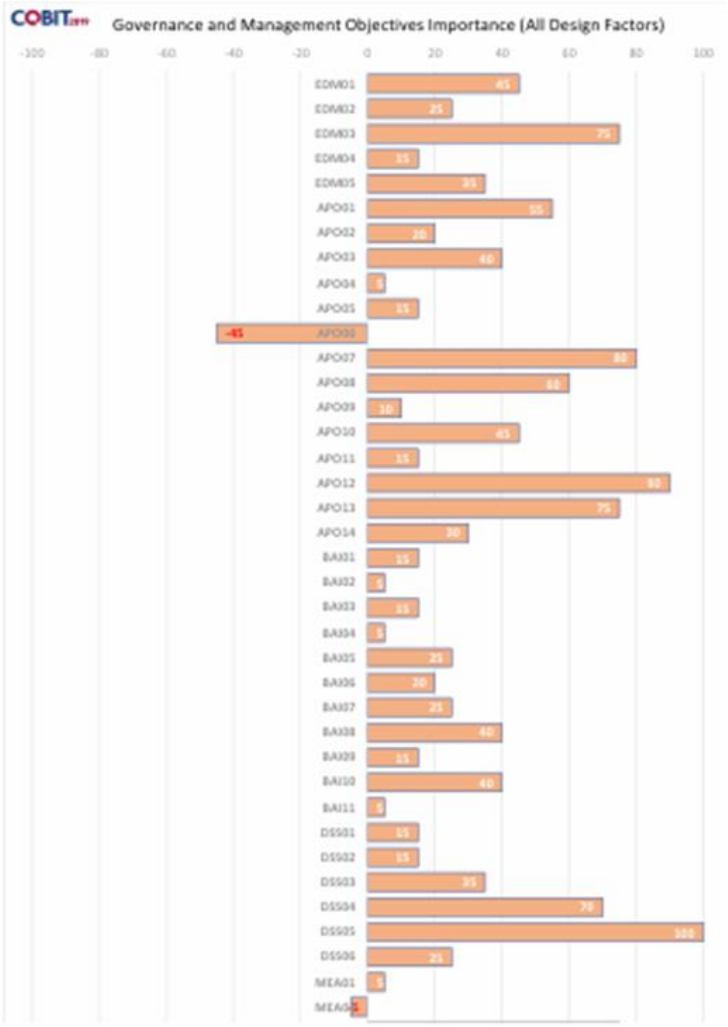

Figure 1. Result 10 Design Factor

Based on the analysis of COBIT 2019 design factors, this study identifies three key domains as the primary focus for Capability Level assessment: DSS05 (Manage Security Services), APO07 (Manage Human Resources), and APO12 (Manage Risk). These domains were selected due to their high importance and critical role in supporting IT governance at Wilujeng Hospital. DSS05 focuses on protecting information systems through effective security services, including access control, threat monitoring, and incident response. APO07 addresses the planning, development, and management of IT human resources to ensure the availability of skilled and competent personnel. APO12 emphasizes proactive risk management by identifying

and mitigating IT-related risks to maintain operational continuity and align IT practices with organizational objectives. These domains form the foundation for evaluating current capability levels and developing targeted recommendations.

3.3. Determining Respondents

This research uses a RACI Chart based on the COBIT 2019 framework to analyze roles and responsibilities in IT management in hospitals. Although the RACI Chart ideally involves several roles, in this study interviews were conducted with one main respondent, the IT Unit Manager, who has comprehensive insight into the implementation of IT governance and can provide perspectives on the roles of other parties involved. And one other respondent from the HR Unit because the APO07 domain involves Human Resources. The IT Unit Manager has primary responsibility for managing IT resources (APO07), so can provide insight into competencies, training, and HR management in IT. The IT Unit Manager also plays a role in IT risk management (APO12), including identification, mitigation, and risk handling strategies related to hospital information systems. From an information security perspective (DSS05), the IT Unit Manager has knowledge of security policy implementation, security incident management, and controls implemented in hospital information systems.

3.4. Risk Management Assessment Using Capability Level Process Analysis

3.4.1. DSS05

The Capability Level 1 assessment for the DSS05 domain was based on an evaluation by the IT Unit Manager at Wilujeng Hospital to measure the implementation of processes according to COBIT 2019 standards. The assessment focused on Level 1 indicators (Performed Process), indicating that processes are carried out, although lacking structured control or documentation.

Table 2. Capability Level Calculation Result DSS05 Level 1

Process	Level	Activity	Yes	No	Score
DSS05	1	1	X		1
	1	2	X		1
	1	3	X		1
	1	4	X		1
	Total				4
	Capability Level				100%

$$CC = \frac{\sum CLa}{\sum Po} \; X \; 100\%$$

$$CC = \frac{4}{4} \; X \; 100\%$$

$$CC = \; 100\%$$

Based on the calculation results, the DSS05 Level 1 process capability achieved a score of 100%, allowing the assessment to proceed to Level 2.

Table 3. Capability Level Calculation Result DSS05 Level 2

Process	Level	Activity	Yes	No	Score
DSS05.01	2	1	X		1
		2	X		1
DSS05.02	2	1	X		1
		2	X		1
		3	X		1
		4	X		1
DSS05.03	2	1	X		1
		2		X	0
		3		X	0
		4	X		1
		5		X	0
		6	X		1
		7		X	0
		8		X	0
		9		X	0
DSS05.04	2	1	X		1
DSS05.05	2	1		X	0
		2	X		1
		3		X	0
		4	X		1
DSS05.06	2	1	X		1
		2	X		1
DSS05.07	2	1		X	0
		2	X		1
		3	X		1
		4		X	0
		Total			16
		Capability Level			100%

$$CC = \frac{\sum CLa}{\sum Po} X\ 100\%$$

$$CC = \frac{4}{4} X\ 100\%$$

$$CC = 100\%$$

Based on calculations, the DSS05 Level 2 process capability at Wilujeng Hospital obtained a value of 61.5% (Largely Achieved), so it was declared that it had not yet met the requirements for level 2 and concluded that it was still at Level 1.

3.4.2. APO07

The calculation of the Capability Level in the APO07 domain was carried out based on the responses of the IT Unit Manager as well as through additional interviews with HR representatives, so that we may assess IT HR management implementation in the hospital from operational as also calculated aspects, even though full documentation was lacking.

Table 4. Capability Level Calculation Result APO07 Level 1 Respondent 1

Process	Level	Activity	Yes	No	Score
DSS05	1	1	X		1
	1	2	X		1
	1	3	X		1
	1	4	X		1
Total					4
Capability Level					100%

$$CC = \frac{\sum CLa}{\sum Po} X\ 100\%$$

$$CC = \frac{4}{4} X\ 100\%$$

$$CC = 100\%$$

Based on the calculation results, APO07 Level 1 process capability achieved a score of 100%, allowing the assessment to proceed to Level 2.

Table 5. Capability Level Calculation Result APO07 Level 1 Respondent 2

Process	Level	Activity	Yes	No	Score
APO07	1	1	X		1
	1	2	X		1
	1	3	X		1
	1	4	X		1
Total					4
Capability Level					100%

$$CC = \frac{\sum CLa}{\sum Po} X\ 100\%$$

$$CC = \frac{4}{4} X\ 100\%$$

$$CC = 100\%$$

Based on the calculation results, APO07 Level 1 process capability achieved a score of 100%, allowing the assessment to proceed to Level 2.

Table 6. Result of Capability Level 1 Calculation Recapitulation APO07

Process	Respondent	Total Activity Score	Total Activity	Capability Value
APO07	R1	4	4	100%
	R2	4	4	100%
Total		8	8	
Result		8	8	100%

$$CLi = \frac{Rn + Rn + Rn \ldots}{\sum R}$$

$$CLi = \frac{100 + 100}{2}\ \%$$

$$CLi = \frac{200}{\sum R}\%$$

$$CLi = 100\%$$

Based on the calculation, the APO07 - Managed Human Resources process at Capability Level 1 at Wilujeng Hospital reaches 100% (Fully Achieved), so it is declared successful and can proceed to the calculation of Capability Level 2.

Table 7. Capability Level Calculation Result APO07 Level 2 Respondent 1

Process	Level	Activity	Yes	No	Score
APO07.01	2	1	X		1
		2	X		1
		3	X		1
APO07.02		1	X		1
		2	X		1
		3	X		1
APO07.03		1	X		1
		2		X	0
APO07.04		1	X		1
		2	X		1
		3	X		1
		4	X		1
APO07.05		1	X		1
APO07.06		1	X		1
		2	X		1
		3	X		1
		4	X		1
		5	X		1
		Total			16
		Capability Level			100%

$$CC = \frac{\sum CLa}{\sum Po} \; X \; 100\%$$

$$CC = \frac{17}{18} \; X \; 100\%$$

$$CC = \; 94{,}44\%$$

Based on the calculation results, it was found that APO07 Level 2 process capability has a value of 94,44%.

Table 8. Capability Level Calculation Result APO07 Level 2 Respondent 2

Process	Level	Activity	Yes	No	Score
APO07.01	2	1		X	0
		2	X		1
		3		X	0
APO07.02	2	1	X		1
		2		X	0
		3	X		1
APO07.03	2	1	X		1
		2		X	0
APO07.04	2	1	X		1
		2	X		1
		3	X		1
		4	X		1
APO07.05	2	1	X		1
APO07.06	2	1	X		1
		2	X		1
		3		X	0
		4	X		1
		5		X	0
		Total			16
		Capability Level			100%

$$CC = \frac{\sum CLa}{\sum Po} X\ 100\%$$

$$CC = \frac{12}{18} X\ 100\%$$

$$CC = 66{,}66\%$$

Based on the calculation results, it was found that APO07 Level 2 process capability has a value of 66,66%.

Table 9. Result of Capability Level 1 Calculation Recapitulation APO07

Process	Respondent	Total Activity Score	Total Activity	Capability Value
	R1	17	18	94.44%
	R2	12	18	66.66%
Total		29	36	161.1%
Result				80.55%

$$CLi = \frac{Rn + Rn + Rn \ldots}{\sum R}$$

$$CLi = \frac{94{,}44 + 66{,}66}{2}\ \%$$

$$CLi = \frac{161{,}1}{2}\%$$

$$CLi = 80{,}55\%$$

Based on calculations, the APO07 - Managed Human Resources process at Capability Level 2 at Wilujeng Hospital reaches 80.55% (Largely Achieved), so it has not met the requirements to be declared Level 2, remains at Level 1, and does not proceed to Capability Level 3.

3.4.3. APO12

Calculation of Capability Level 1 in the APO12 domain Managed Risk domain is based on responses from the IT Unit Manager as the main respondent. IT Unit as the main respondent.

Table 10. Capability Level Calculation Result APO12 Level 1 Respondent 1

Process	Level	Activity	Yes	No	Score
APO12	1	1	X		1
	1	2	X		1
	1	3	X		1
	1	4	X		1
Total					4
Capability Level					100%

$$CC = \frac{\sum CLa}{\sum Po}\ X\ 100\%$$

$$CC = \frac{4}{4}\ X\ 100\%$$

$$CC = 100\%$$

Table 11. Capability Level Calculation Result APO12 Level 1 Respondent 2

Process	Level	Activity	Yes	No	Score
APO12	1	1	X		1
	1	2	X		1
	1	3	X		1
	1	4	X		1
Total					4
Capability Level					100%

$$CC = \frac{\sum CLa}{\sum Po} X\ 100\%$$

$$CC = \frac{4}{4} X\ 100\%$$

$$CC = 100\%$$

Based on the calculation results, it was found that APO12 Level 1 process capability in respondent 1 and respondent 2 has a value of 100%.

Table 12. Result of Capability Level 1 Calculation Recapitulation APO12

Process	Respondent	Total Activity Score	Total Activity	Capability Value
	R1	4	4	100%
	R2	4	4	100%
Total		8	8	200%
Result				100%

$$CLi = \frac{Rn + Rn + Rn \ldots}{\sum R}$$

$$CLi = \frac{100 + 100}{2}\ \%$$

$$CLi = \frac{200}{2}\%$$

$$CLi = 100\%$$

Based on the calculation, the APO12 - Managed Risk process at Capability Level 1 at Wilujeng Hospital reaches 100% (Fully Achieved), so it is declared successfully achieved and can proceed to the calculation of Capability Level 2.

Table 13. Capability Level Calculation Result APO12 Level 2 Respondent 1

Process	Level	Activity	Yes	No	Score
APO12.01	2	1	X		1
	2	2	X		1
APO12.03	2	1	X		1
	2	2	X		1
	2	3		X	0
APO12-05	2	1	X		1
		Total			16
		Capability Level			100%

$$CC = \frac{\sum CLa}{\sum Po} X\ 100\%$$

$$CC = \frac{5}{6} X\ 100\%$$

$$CC = 83{,}33\ \%$$

Based on the calculation results, it was found that APO12 Level 2 process capability has a value of 83,33%.

Table 14. Capability Level Calculation Result APO12 Level 2 Respondent 2

Process	Level	Activity	Yes	No	Score
APO12.01	2	1	X		1
	2	2		X	0
APO12.03	2	1		X	0
	2	2	X		1
	2	3		X	0
APO12-05	2	1		X	0
		Total			2
		Capability Level			100%

$$CC = \frac{\sum CLa}{\sum Po} X\ 100\%$$

$$CC = \frac{2}{6} X\ 100\%$$

$$CC = 33.33\%$$

Based on the calculation results, it was found that APO12 Level 2 process capability has a value of 33.33%.

Table 15. Result of Capability Level 2 Calculation Recapitulation APO12

Process	Respondent	Total Activity Score	Total Activity	Capability Value
	R1	5	6	83.33%
	R2	2	6	33.33%
Total		7	12	116.66%
Result				58.33%

$$CLi = \frac{83{,}33 + 33{,}33}{2}$$

$$CLi = \frac{116{,}66}{2}\ \%$$

$$CLi = 58{,}33\%$$

Based on calculations, the APO12 - Managed Risk process at Capability Level 2 at Wilujeng Hospital reaches 58.33% (Largely Achieved), so it has not met the requirements to be declared Level 2, remains at Level 1, and cannot be continued to Capability Level 3.

3.5. Gap Analysis

A gap analysis was conducted to compare the current IT governance capability level (As-Is) with the expected level (To-Be), aiming to identify gaps and areas for improvement to develop more effective enhancement strategies aligned with business needs and established standards.

Table 6. Result of Gap Analysis

Proccess	Capability Level		
	As-is	*To-be*	*Gap*
DSS05	1	4	3
APO07	1	4	3
APO12	1	4	3

3.6. Recommendation

After the gap analysis between the current (As-Is) and expected (To-Be) capability conditions, improvement recommendations are made to improve IT governance to align with organizational needs and COBIT 2019 standards, as well as support the achievement of business objectives and improvement of IT risk management capabilities.

Table 6. Result of Gap Analysis

Proccess	Recomendation
DSS05	Wilujeng Hospital needs to develop a security policy that includes procedures for handling security incidents, access control, and protection of patient data and hospital information systems.
	Wilujeng Hospital needs to organize periodic training on cyber security, access policies, and procedures for handling security threats.
	Wilujeng Hospital lacks the human resources that have expertise for data security. Several solutions that can be applied involve working with an IT security service provider (MSSP) in order to assist in monitoring, detecting, and in handling security threats in such a manner. Another solution that one can apply is to optimize existing human resources through providing intensive training along with certification in the field of data security, such as Certified Information Systems Security Professional (CISSP) or Certified Ethical Hacker (CEH). For managing data security, hospitals can utilize cloud-based security services like Cloud Access Security Broker (CASB) if internal resources are limited. Hospitals can also forgo a large security staff inside or forming a data security staff using outsourcing or part-time staff..
APO07	Wilujeng Hospital needs to carry out technical training and certification for IT staff to improve their skills in managing hospital information systems
	Hospitals need to develop a performance assessment mechanism based on Key Performance Indicators (KPI) to measure the effectiveness and productivity of IT HR.
APO12	Wilujeng Hospital needs to create an IT risk management policy document that includes methods of identification, analysis, mitigation and ongoing risk monitoring.
	Wilujeng Hospital needs to identify risks to information systems and IT infrastructure. For example, by using standard methods such as Risk Assessment Matrix or Failure Mode and Effect Analysis to analyze the impact and likelihood of risks that can prevent the Hospital from achieving its goals.
	Wilujeng Hospital needs to increase awareness and carry out periodic socialization and training to all employees regarding the importance of IT risk management.

4. CONCLUSION

Based on the results of analysis and calculation, the three domains-DSS05 (Manage Security Services), APO07 (Manage Human Resources), and APO12 (Manage Risk)-are all at Level 1. This indicates that the processes in the three domains are still reactive, less structured, and not well documented, posing a high risk to data security and the overall effectiveness of IT management. To improve capability, hospitals need to develop more systematic policies, strengthen IT HR competencies through training and certification, and provide adequate human resources. In addition, strengthening inter-unit coordination, implementing KPI-based performance evaluation, and career development programs are also needed so that IT management can optimally support the hospital's operational and strategic needs.

REFERENCES

[1] D. Kurnianty Jamal and A. Kusumawati, "Information System Audit Using COBIT 2019 Framework in Construction Companies," 2023. [Online]. Available: www.questjournals.org

[2] "Auditing Cyber Incident Response and Recovery 2 nd Edition Global Practice Guide Aligns with the Global Internal Audit Standards."

[3] M. H. A. Syahputra and R. Sutomo, "Analysis of IT Performance on Management HR of Equity Firm Using COBIT 5," *Journal of Information Systems and Informatics*, vol. 5, no. 2, pp. 650–664, May 2023, doi: 10.51519/journalisi.v5i2.494.

[4] S. Salim and A. H. Muhammad, "Security Infrastructure Service and Information Security Management Capability Audit to Improve System Security in Preventing Cyber Attacks using COBIT 2019," *G-Tech: Jurnal Teknologi Terapan*, vol. 9, no. 1, pp. 400–409, Jan. 2025, doi: 10.70609/gtech.v9i1.6319.

[5] "Auditing Network and Communications Management 2 nd Edition Global Practice Guide Aligns with the Global Internal Audit Standards."

[6] A. Viamianni, R. Mulyana, and F. Dewi, "COBIT 2019 INFORMATION SECURITY FOCUS AREA IMPLEMENTATION FOR REINSURCO DIGITAL TRANSFORMATION," *JIKO (Jurnal Informatika dan Komputer)*, vol. 6, no. 2, Aug. 2023, doi: 10.33387/jiko.v6i2.6366.

[7] E. Enrique and M. I. Fianty, "Enhancing Risk Management in an IT Service Company: A COBIT 2019 Framework Approach," *Jurnal Riset Informatika*, vol. 5, no. 4, pp. 499–506, Sep. 2023, doi: 10.34288/jri.v5i4.212.

[8] M. I. Fianty and M. Brian, "Leveraging COBIT 2019 Framework to Implement IT Governance in Business Process Outsourcing Company," *Journal of Information Systems and Informatics*, vol. 5, no. 2, pp. 568–579, May 2023, doi: 10.51519/journalisi.v5i2.492.

[9] R. N. Christiadi and R. Sutomo, "Measurement of IT Security Governance Capabilities Using COBIT 2019 at Indonesian Business Sector," *G-Tech: Jurnal Teknologi Terapan*, vol. 7, no. 4, pp. 1498–1508, Oct. 2023, doi: 10.33379/gtech.v7i4.3170.

[10] A. Oktaviana, K. Adi, and B. Warsito, "Adopting COBIT 2019 for the Evaluation of Information Technology Risk Management in a Startup Company," *International Journal of Innovative Science and Research Technology (IJISRT)*, pp. 1613–1621, Jul. 2024, doi: 10.38124/ijisrt/ijisrt24jun1542.

[11] E. Nachrowi, Yani Nurhadryani, and Heru Sukoco, "Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 4, no. 4, pp. 764–774, 2020, doi: 10.29207/resti.v4i4.2265.