Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Strategic IT Governance: Utilizing COBIT 2019 Framework to Mitigate Data Backup Failures in Industrial Operations

Daffa Kaisha Pratama Chandra[1], Melissa Indah Fianty[2]
daffa.kaisha@student.umn.ac.id, melissa.indah@umn.ac.id*
[1,2] Information Systems Study Program, Faculty of Engineering & Informatics, Multimedia Nusantara University

Article Information

Submitted : 5 Apr 2024
Reviewed : 29 Apr 2024
Accepted : 30 Jun 2024

Keywords

Capability Level, COBIT 2019, IT Audit

Abstract

The development of information technology today has had a significant impact on various aspects of human life, including in the industrial sector. One example is the integration of information technology in company operations to use it as a supporting tool for sending data and information which is the main reference for organizational management in decision making. To measure the level of capability of the IT system used, companies can use the COBIT 2019 framework, which not only helps in assessing the suitability of IT systems, but also provides recommendations for solutions to problems faced by the company. For example, research results show that problems related to data backup failures have been identified in Domain DSS01, with recommended solutions such as implementing policies related to information security from outsourced employees, establishing internal management processes, setting up timely incident tickets, and implementing recommendations to overcome non-compliance.

A. Introduction

To survive in today's digital era, every company or organization needs to think about ways to keep their business running amidst the massive onslaught of technology. One way is by utilizing Information Technology or Information Systems (IT/SI) [1]. The investment costs and risks are large in the use of IT/IS in companies so that the use of IT/SI can increase the efficiency and effectiveness of existing business processes. To ensure whether the IT/IS investment implemented in a company is in line with the company's business objectives or not, a technique called IT Governance can be used [2]. Without good IT governance in the company, it will be very difficult to assess how effective the company is in implementing IT [3]. Even though someone has already regulated the IT/IS system, it does not rule out the possibility of risks occurring that could hamper the company's business processes.

One of the risks that can occur within the scope of technology utilization is the occurrence of backup or data backup failure incidents [4]. Therefore, companies need to think about a strategy so that data backup failures can be avoided [5]. If we refer to data published by databoks.katadata.co.id, the second biggest risk experienced by companies globally in 2022 is business disruption [6].

The risk of business interruption ranks second in terms of the greatest risk that may be experienced in a company [6]. The risk of data backup failure can be categorized as business disruption if data backup failure occurs repeatedly, disrupting the business processes of the company that experiences it [7]. The problem in question is a data backup failure at the Indonesian branch company. The data that companies most often fail to back up is manufacturing data.

The results of interviews at the company show differences between the company's Information Technology (IT) mission and objectives with a focus on the effectiveness and optimality of technology support, while business objectives emphasize asset security. The main problem arises in manufacturing data backup which can hamper the transformer sales process if not addressed immediately. To overcome this problem, the company plans to measure the level of IT/IS governance capabilities using the COBIT framework. The results of these measurements are expected to be a guide for the IT and sales divisions to align the company's mission and goals regarding data backup.

Frameworks commonly used for IT governance include COBIT (Control objectives for Information and Related Technology), and CMMI (Capacity Maturity Model Integrated) [8]. Each framework mentioned above has its own use. The COBIT framework focuses on evaluating the performance of IT application to business processes in a company [9]. The CMMI framework is used to evaluate the quality of applications used by a company [10].

IT governance is divided into five main components: IT strategy alignment, the value that IT can provide, IT risk management, performance measurement, and IT resource management [11]. Based on the four frameworks mentioned previously, the COBIT framework is the most comprehensive framework for use in measuring IT governance in a company [12] [13].

The framework that will be used in this research is the COBIT 2019 framework. The selection of the COBIT 2019 framework is based on the focus of COBIT 2019, which focuses on aligning business objectives with the use of IT in

companies that are not yet aligned so that it affects the company's business processes [14] [15]. Apart from that, the COBIT 2019 framework can also provide recommendations, solutions and guidelines for problems experienced by companies [14] [16]. In this research, a company's capability level will be measured to determine the company's ability to implement IT processes [17]. Measuring the level of company capability was carried out because it was in accordance with previous research which also measured the level of capability of a company/organization using the COBIT 2019 framework [18][19][20][21].

Therefore, with the problems that have been found, an audit will be carried out to evaluate IT governance in the company. This research will use COBIT 2019 as an audit framework that measures capability levels and issues recommendations for completion as output from the audit carried out in this research. So that the results of the evaluation and recommendations provided will have a good impact on the company in implementing IS/IT and existing business processes.

B. Research methods

In this research, qualitative methods were used, the data used for this research was obtained from a literature review, the results of interviews with the company and the results of audit observations. The audit activity plan that will be carried out at the company in this research is depicted as in the picture below.

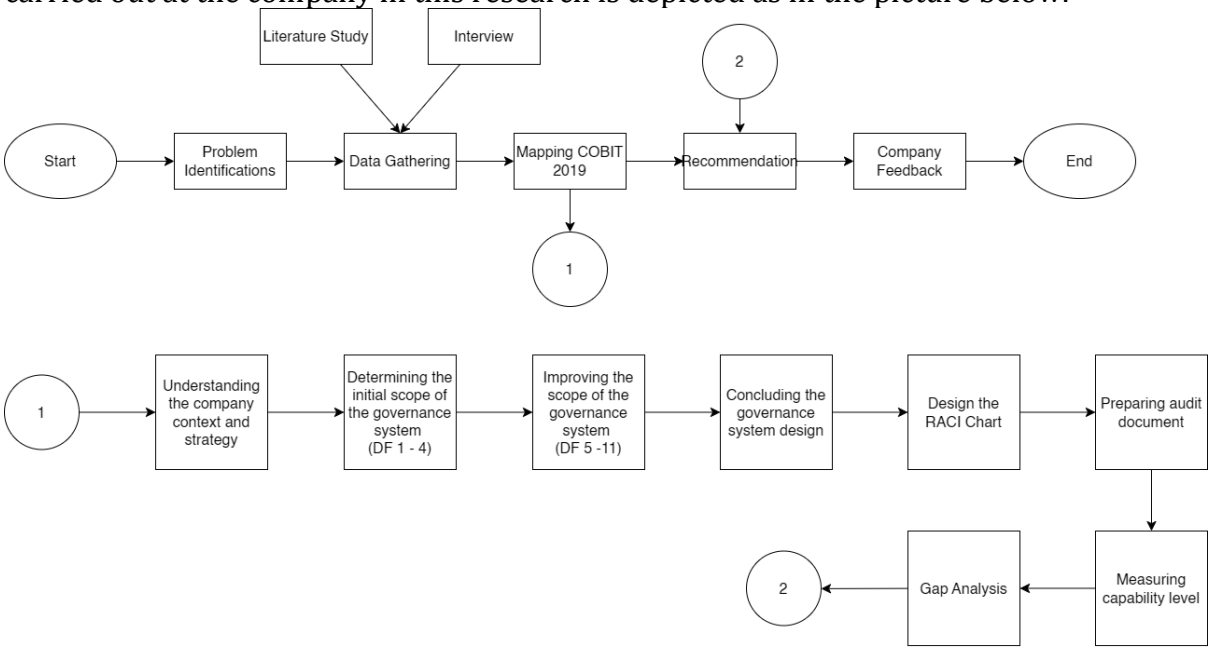

Figure 1. Research Flow [22] [23]

Figure 1 shows the research flow with the following explanation:

1. **Identification of problems**
   The problem identification process aims to identify the obstacles faced by companies that encourage them to implement IT governance using COBIT 2019. To obtain information, interviews were conducted with company IT staff.
2. **Data collection**

At this literature study stage, learning is carried out through books, journals and articles related to this research topic. The journals, books and articles reviewed will be used as references that can help this research. Through this literature review, the principles related to the COBIT 2019 framework used in this research can be identified.

3. **COBIT Mapping 2019**
   The COBIT 2019 process goal mapping stage was carried out to determine the process goals that will be measured. Goal mapping will use the COBIT 2019 Design Toolkit as a tool to determine relevant COBIT 2019 process goals that will be evaluated within the company. This process aims to determine the basis for measuring process objectives in accordance with the COBIT 2019 framework.
4. **Recommendation**
   From the evaluation results obtained using the COBIT 2019 framework, this research will provide recommendations to companies to overcome and resolve problems and increase the level of company capability.
5. **Company feedback**
   At this stage, as a result of the recommendations that have been given, the company will provide feedback by first reviewing whether the recommendations given are appropriate and can help the company to resolve existing problems.

C. Results and Discussion

Identification of problems

At this stage, problems occurring in the company will be identified by collecting data to determine the next stage, namely COBIT 2019 mapping.

Data collection

At this stage, data collection is divided into 2 stages, namely literature study and interviews. The literature study stage is carried out by reading and understanding books, journals and articles related to theory and previous research that are related and used as references in this research. At the interview stage, it will be carried out by interviewing the company, namely Mr. Reggie, as one of the IT divisions at XYZ company. Interviews are conducted to find out the problems that occur in the company and provide an assessment of the audit documents for each objective that has been mapped. From the results of interviews, the problem that often occurs in companies is related to data backup failures.

Mapping COBIT 2019

At this stage, mapping will be carried out using the COBIT 2019 framework based on the results of interviews, namely the problem of data backup failure. From the COBIT framework, mapping will be selected from five domains using the COBIT 2019 Design Toolkit tools. The mapping process is as follows:

a) Understand the company's corporate focus.

b) Determine the initial scope of the governance system by measuring design factors 1-4 to determine the company's strategy, objectives, risk profile and IT problems.
c) Improve the initial scope of the governance system by measuring design factors 5-11 to determine threats, compliance, IT role, IT sources, implementation methods, technology used, and company size.
d) Concluding the governance system design and obtaining COBIT 2019 objectives.
e) Determine respondents to assess audit documents using the RACI Chart regarding COBIT 2019 objectives from the results of design factor mapping.
f) Measuring the level of capability from the objectives obtained.
g) Analyze the gap between the current capability level and the target capability level.

The summary results of the design factors that have been carried out are as follows.

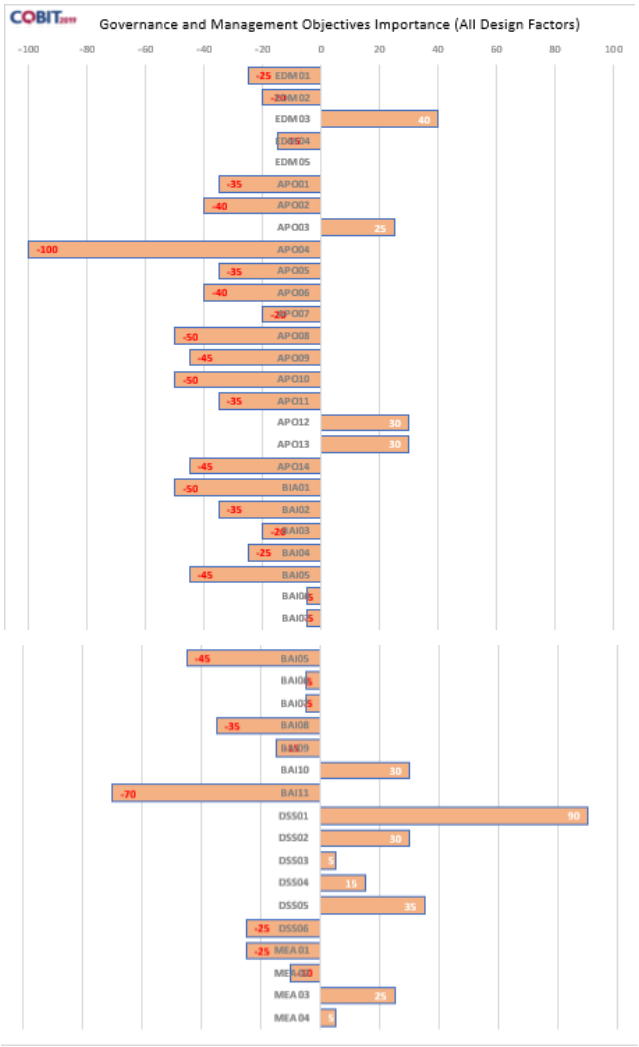

Figure 2. Factor Design Summary

Figure 2 displays the results of all design factors that have been measured, providing information about the domains that companies must prioritize for

improvement. All domains are assessed on a scale from the lowest, namely -100 to the highest, namely 100. Although all processes will be assessed, not all of them are considered important or given priority. Determining the level of ability that is prioritized is a Domain that has a score of 85 or more. Domains that score 85 or more on the design Factor are DSS01.

RACI Chart

RACI is an abbreviation for Responsible, Accountable, Consulted, and Informed [24] [24]. RACI Chart is one of the tools used in decision making and helps company/organization management to identify the roles and responsibilities of each employee in the company/organization [25] [26].

Table 1. RACI Chart Objective DSS01

No	Activity	IT Deputy Manager	EPC Business Unit
1	DSS01.1: Perform operational procedures.	R	R
2	DSS01.2: Manage outsourced I&T services.	R	R
3	DSS01.3: Monitor I&T infrastructure.	R	A/C
4	DSS01.4: Manage the environment.	R	A/C
5	DSS01.5: Manage facilities.	R	A/C

Table 1 shows the roles and responsibilities of the roles responsible for the DSS01 domain, namely IT Deputy Manager and EPC Business Unit, in the audited company. Individuals who have the R (responsible) role will be respondents in the audit document report, while individuals who have the A (Accountable) / C (Consulted) role are the people responsible for the success of this domain.

Process Assessment Profile and Capability Level Achievement

The first thing to do is conduct interviews and distribute questionnaires to Auditees. After distributing a questionnaire to determine the level of capability in the company, the following results were obtained with the details listed in table 2. Table 2 describes the condition of the company's current level of capability, which is in the DSS01 – Manage Operation domain.

Table 2. Conclusion of Audit Results

Summary Results								
Process ID	Process Description	Process Purpose	Achieved Capability Level					
			1	2	3	4	5	
DSS01	Manage Operations	Deliver I&T operational product and service outcomes as planned.	F	F	L			

Table 3 contains an explanation of the assessments that must be passed in order to proceed to the next capability level, namely with an average of >85% for each level. Based on table 3.1, it can be concluded that the company has a capability level at level 3 with an average score of 76.7% which is at level L, namely largely achieved, so it cannot continue to assess the capability level to the next level and must stop at level 3.

Table 3. Scoring scale

Scale	Identity
< 15%	(N) Not Achieved

15% - 50%	(P) Partially Achieved
50% - 85%	(L) Largely Achieved
> 85%	(F) Fully Achieved

The DSS01 process in COBIT 2019 is the process of coordinating and implementing the operational procedure activities required to provide internal and outsourced IT services, including the implementation of previously established standard operating procedures and necessary monitoring activities [26]. The following are the results of measuring the level of capability in the DSS01 process.

Table 4. DSS01 Capability Measurement

Process Name DSS01	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Rating by Criteria	F	F	F	L		
Rating by Percentage	100%	100%	85.20%	76.68%		
Capability Reach				3		

In table 4, it can be concluded that the DSS01 process reached level 3 with a percentage of 76.68% in the criteria, namely L (largely achieved). After the DSS01 objective calculation process was carried out, the results of measuring the level of capability were obtained. Based on the findings, a gap analysis will be carried out from the results of measuring the current level of capability (current maturity level) with the target level of expected capability (expected maturity level) . This gap analysis is used to determine the comparison of the current capability level and the target capability level in order to identify processes that need to be improved and improved.

Table 5 will explain the company's maturity level and the expectations it should achieve.

Table 5. Gap Analysis

Gap analysis			
Process	**Current Maturity Level**	**Expect Maturity Level**	**Gap**
DSS01	3	4	1

Table 5 shows the results of the gap analysis between the results of measuring the current capability level (current maturity level) which is worth 4 and the expected capability level target (expected maturity level) which is worth 3, so the calculated gap is 1.

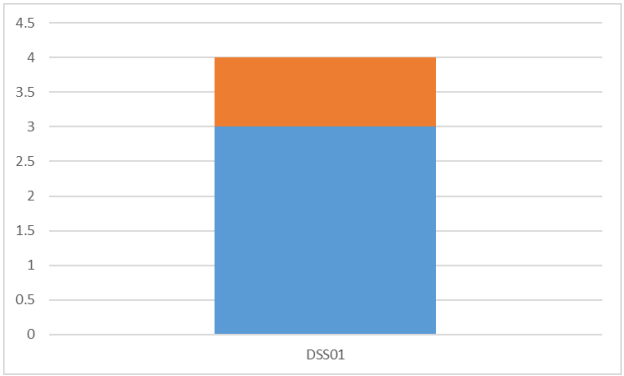

Figure 3. Gap Analysis

Figure 3 shows a graph comparing the results and targets of the company's DSS01 domain capability levels. Based on the results of objective assessments that have been carried out previously, there are several findings from activities that have a score of ≤ 50. These findings are used to evaluate the company's IT governance performance and as a reference for improvement. These results help determine the impact the company experienced.

Table 6. DSS01 Findings and Impact

Process	Activity	Findings	Impact
DSS01.02 - 1	Ensure that company requirements regarding information process security comply with contracts and SLAs with third parties that organize or provide services.	Some information process security does not comply with contracts and SLAs.	Sensitive or confidential business data may be exposed or become vulnerable to access by unauthorized parties.
DSS01.03 - 5	Ensure incident tickets are generated timely when detection of specified thresholds.	There was a delay in creating an incident ticket.	Can hamper handling of data backup failures.
DSS01.05 - 5	Ensure that physical wiring and labeling (data and telephone) are arranged, organized and well documented.	Physical wiring and labeling are not well structured or organized	Difficulty in tracking, managing, and maintaining certain cables.

Table 6 shows the findings and impacts of processes DSS01.02, DSS01.03, and DSS01.05 related to third-party contracts, incident ticket delays, and cable labeling.

Recommendation

Based on the results of measuring the level of capability and the findings and impacts that have been carried out, recommendations will then be given, namely recommendations for improvement and recommendations for increasing the level of capability level in accordance with the COBIT 2019 guidelines to improve several activities that still have a score of ≤ 50 and increase the level of capability level of the company.

Improvement Recommendations

Recommendations for improvement are used to improve activities that still have a score of ≤ 50 in accordance with the findings and impacts contained in table 3. Recommendations for improvement are given for objective DSS01.

Table 7. DSS01 Improvement Recommendations

Process	Activity	Recommendation
DSS01.02	Ensure that company requirements regarding information process security comply with contracts and SLAs with third parties that organize or provide services.	Develop and implement comprehensive data security policies and procedures. Assess security risks regularly and implement data security controls regularly.
DSS01.03	Ensure incident tickets are created in a timely manner while monitoring	Improve monitoring processes and use appropriate technology. improving

	identified deviations from specified thresholds.	communication, defining roles and responsibilities on the team. then develop procedures for handling incidents that occur.
DSS01.05	Ensure that physical cabling and labeling (data and telephone) is arranged and well organized. Document wiring and conduit structures (e.g. building floor plans and wiring diagrams).	Develop physical wiring and labeling policies and procedures. And develop controls to mitigate risks that could occur in infrastructure, followed by carrying out infrastructure improvements.

Table 7 shows the recommendations from the DSS01.02 process to Ensure that enterprise requirements regarding information process security comply with contracts and SLAs with third parties that host or provide services. The recommendation given is that companies can develop and implement comprehensive data security policies and procedures and implement data security controls periodically.

Recommendations for Increasing Capability Levels

Recommendations for increasing the level of capability are used to improve the activities of processes that are still at level 3, so that by providing recommendations it is hoped that they can help the company to improve activities and increase the level of capability. Apart from that, through these recommendations it is also hoped that IT use can be aligned with business activities in the company, so that company goals can be achieved.

Table 8. DSS01 Level 3 Improvement Recommendations

Process	Recommendation
DSS01.02	• Create regulations and procedures related to data security that cover various things. • Carry out work records and adjustments by complying with contracts with third parties or service providers. • Create internal IT management processes and appoint people to oversee them. Create procedures and policies to prevent company information from being disseminated widely.
DSS01.03	• Record violations and the conditions of the incident. • Ensure incident tickets are created in a timely manner while monitoring identified deviations from specified thresholds.
DSS01.04	• Determine insurance policy requirements for emergency measures and plans. • Assess existing emergency measures and plans to ensure compliance with insurance policy requirements. • Create reports detailing assessment results and recommendations to address points of non-compliance. • Implement recommendations that have been made and follow up to ensure that points of non-compliance have been resolved.
DSS01.5	• Develop physical wiring, labeling policies and procedures, and controls to mitigate risks that could occur in infrastructure.

Table 8 shows recommendations for increasing the level of capability level 3 of the DSS01 objective. Managed Operations. The recommendations given include that companies implement several policies related to the security of company

information from outsourced employees, create an internal management process, ensure incident tickets are made on time and implement recommendations that have been made to ensure points of non-compliance can be resolved.

D. Conclusion

From the results of the research that has been carried out, the DSS01 capability level is obtained at level 4. The expected capability level is at level 3, it can be concluded that there is a gap of 1 level from the current capability level. The recommendations given to increase capability levels are implementing policies related to company information security from outsourced employees, creating internal management processes, ensuring incident tickets are made on time and implementing recommendations that have been made to ensure points of non-compliance can be resolved. Further research can be carried out to evaluate how mature Information Technology (IT) governance, especially database servers, is in manufacturing companies using the COBIT 2019 framework. It is hoped that the results of this research can become a reference for similar studies in the future or to combine with other frameworks. in broader research.

E. Acknowledgement

This research was realized with guidance provided by supervisors from Multimedia Nusantara University, who provided direction and support to researchers in the process of carrying out this research.

F. References

[1] D. Tinus and J. Setiawan, "Implementation IT Governance Using COBIT 5 Framework at PT. XYZ (Persero)," *IJNMT Int. J. NEW MEDIA Technol.*, vol. 9, no. 2, pp. 56–68, 2022, [Online]. Available: https://ejournals.umn.ac.id/index.php/IJNMT/article/view/2739

[2] D. A. Sudarnoto, W. Wella, and R. I. Desanti, "COBIT 5: How Capable PT GTI Governing Innovation, Human Resource, and Knowledge Aspect?," *Ultim. InfoSys J. Ilmu Sist. Inf.*, pp. 108–114, Apr. 2022, doi: 10.31937/si.v12i2.2400.

[3] C. Lumingkewas, J. Y. Mambu, and A. Wahyudi, "Identification of IT Governance Capability Level of COBIT 2019 at The KOMINFO City of Bitung, North Sulawesi," *TeIKa*, vol. 13, no. 01, pp. 1–15, Apr. 2023, doi: 10.36342/teika.v13i01.3064.

[4] A. N. Ramadhani, T. Theresiawati, and S. Sarika, "Analisis Manajemen Risiko Pada Sistem Informasi Kimia Farma Employee Self Technology," *Bit (Fakultas Teknol. Inf. Univ. Budi Luhur)*, vol. 20, no. 1, p. 38, Apr. 2023, doi: 10.36080/bit.v20i1.2127.

[5] Khrisna Aprianto, Endroyono, and S. M. S. Nugroho, "Analisis Manajemen Risiko SPBE Menggunakan COBIT 5 For Risk dan ISO 31000:2018 di Kabupaten Magetan," *J. IPTEK-KOM (Jurnal Ilmu Pengetah. dan Teknol. Komunikasi)*, vol. 23, no. 2, pp. 107–123, 2021.

[6] A. M. Syuhada, "Apa Risiko Bisnis Terbesar Global pada 2022?" https://databoks.katadata.co.id/datapublish/2022/01/21/apa-risiko-bisnis-terbesar-global-pada-2022 (accessed Oct. 03, 2023).

[7] H. Wang and B. Ran, "Network governance and collaborative governance: a thematic analysis on their similarities, differences, and entanglements," *Public Manag. Rev.*, vol. 25, no. 6, pp. 1187–1211, Jun. 2023, doi: 10.1080/14719037.2021.2011389.

[8] H. Ibrahim and B. Abdessamad, "A Built-in Criteria Analysis for Best IT Governance Framework," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 10, 2019, doi: 10.14569/IJACSA.2019.0101026.

[9] A. M. N. Aziz *et al.*, "Audit Sistem Informasi Menggunakan Framework Cobit 4.1 Pada E-Learning Ars University," *JISAMAR (Journal Inf. Syst. Applied, Manag. Account. Researh)*, vol. 4, no. 3, 2020, [Online]. Available: https://journal.stmikjayakarta.ac.id/index.php/jisamar/article/view/253

[10] D. Made Novita, I. Made Sukarsa, and I. Ketut Adi Purnawan, "Mengetahui Tingkat Kematangan Aplikasi pada Start up IT Menggunakan Metode CMMI dan TMMi," *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, p. 1, Apr. 2019, doi: 10.24843/JIM.2019.v07.i01.p01.

[11] S. C. I. Simatupang and M. I. Fianty, "Assessment of Capability Levels and Improvement Recommendations Using COBIT 2019 for the IT Consulting Industry," *G-Tech J. Teknol. Terap.*, vol. 7, no. 4, pp. 1391–13400, Oct. 2023, doi: 10.33379/gtech.v7i4.3141.

[12] R. D. Handayani and R. A. Aziz, "Framework Information Technology Infrastructure Library (Itil V3) : Audit Teknologi Informasi Sistem Informasi Akademik (Siakad) Perguruan Tinggi," *Explor. J. Sist. Inf. dan Telemat.*, vol. 11, no. 1, p. 29, Jun. 2020, doi: 10.36448/jsit.v11i1.1456.

[13] A. Algiffary, M. Izman Herdiansyah, and Yesi Novaria Kunang, "Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework COBIT 2019 Pada RSUD Palembang BARI," *J. Appl. Comput. Sci. Technol.*, vol. 4, no. 1, pp. 19–26, Jun. 2023, doi: 10.52158/jacost.v4i1.505.

[14] N. Baisholan, K. E. Kubayev, and T. S. Baisholanov, "Modern Tools For Information Security Systems," *PHYSICO-MATHEMATICAL Ser.*, vol. 335, no. 1, pp. 14–18, Feb. 2021, doi: 10.32014/2021.2518-1726.2.

[15] 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, May 2023, doi: 10.34010/jtk3ti.v9i1.9672.

[16] B. V. Tulus and A. R. Tanaamah, "Design of Information Technology Governance in Educational Institutions Using COBIT 2019 Framework," *J. Inf. Syst. Informatics*, vol. 5, no. 1, pp. 31–43, Feb. 2023, doi: 10.51519/journalisi.v5i1.408.

[17] A. S. Sukamto, 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, Aug. 2021, doi: 10.26418/jp.v7i2.47859.

[18] A. A. Mariatama, L. H. Atrinawati, and M. G. L. Putra, "Perancangan Tata Kelola Teknologi Informasi Dengan Menggunakan Framework Cobit 2019 Pada Pt Jwt Global Logistics Indonesia," *J. Sist. Inf. dan Inform.*, vol. 5, no. 1, pp. 19–29, Feb. 2022, doi: 10.47080/simika.v5i1.1423.

[19] A. M. Syuhada, "Kajian Perbandingan Cobit 5 dengan Cobit 2019 sebagai

Framework Audit Tata Kelola Teknologi Informasi," *Syntax Lit.; J. Ilm. Indones.*, vol. 6, no. 1, 2021, doi: 10.36418/syntax-literate.v6i1.2082.

[20] R. A. Nugraha and R. Syaidah, "Smart Campus Governance Design for XYZ Polytechnic Based on COBIT 2019," *JOIV Int. J. Informatics Vis.*, vol. 6, no. 3, p. 718, Sep. 2022, doi: 10.30630/joiv.6.3.1257.

[21] D. Utomo, M. Wijaya, S. Suzanna, E. Efendi, and N. T. M. Sagala, "Leveraging COBIT 2019 to Implement IT Governance in SME Context: A Case Study of Higher Education in Campus A," *CommIT (Communication Inf. Technol. J.*, vol. 16, no. 2, pp. 129–141, Jun. 2022, doi: 10.21512/commit.v16i2.8172.

[22] G. I. Belo, L. H. Atrinawati, and Y. T. Wiranti, "Perancangan Tata Kelola Teknologi Informasi menggunakan COBIT 2019 pada PT Telekomunikasi Indonesia Regional VI Kalimantan," *J. Sist. Inf. dan Ilmu Komput. Prima (JUSIKOM Prima)*, vol. 4, no. 1, 2020, [Online]. Available: http://jurnal.unprimdn.ac.id/index.php/JUSIKOM/article/view/1202

[23] D. Putra and M. I. Fianty, "Capability Level Measurement of Information Systems Using COBIT 5 Framework in Garment Company," *J. Inf. Syst. Informatics*, vol. 5, no. 1, pp. 333–346, Mar. 2023, doi: 10.51519/journalisi.v5i1.454.

[24] M. R. Boyce, M. C. Asprilla, B. van Loenen, A. McClelland, and A. Rojhani, "How do local-level authorities engage in epidemic and pandemic preparedness activities and coordinate with higher levels of government? Survey results from 33 cities," *PLOS Glob. Public Heal.*, vol. 2, no. 10, p. e0000650, Oct. 2022, doi: 10.1371/journal.pgph.0000650.

[25] A. Wijaya, N. Putra, A. Sunyoto, and A. Nasiri, "Perencanaan Audit Tata Kelola Teknologi Informasi Laboratorium Kalibrasi Menggunakan COBIT 2019 (Studi Kasus: Laboratorium Kalibrasi BSML Regional II)," *J. Fasilkom*, vol. 10, no. 3, 2020.

[26] O. T. Poetry, R. Fauzi, and R. Mulyana, "Perancangan Tata Kelola Teknologi Informasi Untuk Transformasi Digital di Industri Perbankan Menggunakan Framework Cobit 2019 Dengan Domain Deliver, Service And Support: Studi Kasus Bank Xyz," *e-Proceeding Eng.*, vol. 8, no. 5, 2021, [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/15776