**Scientific Journal of Informatics**
Vol. 13, No. 1, February 2026
p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

# Unveiling IT Governance Effectiveness in e-Puskesmas Using COBIT 2019

**Sumardiono[1*], Supardi[2], Suci Lailla Fitriani[3], Wiwit Priyadi[4], Norhafizah Ismail[5], Riska Suryani[6]**
[1,3]Information System Department, Bina Insani University, Indonesia
[2]Department of Accounting, Bina Insani University, Indonesia
[4]Department of Software Engineer, Bina Insani University, Indonesia
[5]Department of Information and Communication Technology, Politeknik Mersing, Johor, Malaysia
[6]Department of Information System, Harapan Bangsa University, Indonesia

**Abstract.**
**Purpose:** This study aims to evaluate the effectiveness of IT governance implementation in the e-Puskesmas system at Pengasinan Community Health Center, Bekasi City, using the COBIT 2019 framework. The research focuses on identifying the capability level and governance gaps to ensure risk management and IT service delivery align with institutional objectives.
**Methods:** The study employs a mixed-method approach combining qualitative interviews and quantitative questionnaires. Two COBIT 2019 domains—APO12 (Managed Risk) and DSS02 (Managed Service Requests and Incidents)—were analyzed using capability level measurements and GAP analysis to determine performance alignment with governance standards.
**Result:** The findings reveal that e-Puskesmas achieved a high capability level, with 96.88% for APO12 and 90.47% for DSS02. Despite this success, several weaknesses were identified, including delays in patient registration, data confidentiality issues, and service disruptions. The study provides strategic recommendations to enhance user training, strengthen data security, and implement continuous risk management.
**Novelty:** This research presents one of the first applications of COBIT 2019 in evaluating IT governance for public healthcare systems in Indonesia. It demonstrates how COBIT can serve as a practical tool for assessing digital health governance maturity, ensuring data integrity, and supporting the sustainable transformation of healthcare services.

**Keywords**: e-Puskesmas, COBIT 2019, IT Governance, Healthcare Audit, Capability Assessment
**Received** November 2025 / **Revised** December 2025 / **Accepted** January 2026



## INTRODUCTION

In the contemporary digital era, computers are necessary for the advancement of modern science and technology. As information and communication technologies (ICTs) advance and diffuse widely in our industries and society [1], The advent of the digital era has led to the widespread use of computers in businesses, government agencies, private organizations, trade or services, and hospitals for tasks like data processing, reporting, and data storage. It will be simple and take a lot of time, as it is very lengthy.

The above are forms of services and use of computers in the digital era, so services are published both for public consumption or restricted access based on the agreement [2]. As more and more computer services are being made available to the general population by government organizations like hospitals and health facilities, these challenges are classifiable into three significant aspects: technological, organizational, and policy and regulation [3]. The technological aspect in question is e-puskesmas, because their role is very important in providing services to the community, including administration, medical records, and other aspects [4].

Nowadays, hospital organizations are affected by digital advances [5]. That healthcare industry handles huge volume of patient's medical record [6], complete history of diagnoses and healthcare data among facilities [7]. Information technology has become integral to the operations of numerous organizations and

*Corresponding author.
Email addresses: sumardiono@binainsani.ac.id (sumardiono)*, sucilaillafitriani@gmail.com (Fitriani), norhafizah@tvet.pmj.edu.my (Ismail), supardi@binainsani (supardi)
DOI: 10.15294/sji.v13i1.35868

companies, driving efficiency and effectiveness in various aspects of business [8], [9], [10]. The success and sustainability of a company and organization today relies heavily on IT, in terms of speed and results that can help improve the effectiveness and efficiency of business processes [11]. These security policies and controls must be effectively implemented in order to value the importance of integrity, confidentially and availability of information to all the stakeholders involved in the business [12]. In addition to conducting an assessment within an information system, considering critical aspects of the cloud, such as service models, deployment models, and involved parties [13]. Electronic Health Record (EHR) systems have revolutionized the healthcare industry by enabling the efficient storage, retrieval, and sharing of patient health information [14]. The implementation of community health center services is using the e-puskesmas system which aims to assist in providing community services in the health sector. With e-Puskesmas, patient recording and data collection is done electronically [15], mainly related to unauthorized access to e-health records when different healthcare service providers maintain records [16], so that the data needed to be used can be immediately processed and informed. Efforts to improve IT services [17], it is necessary to audit governance and services so that in the future there will be no problems. One framework that can be used as an audit standard is framework COBIT 2019 (Control Objective for Information and Related Technology) [18] issued by Information System Audit and Control Association (ISACA) [19]. COBIT (Control Objective for Information Technology) 2019 is a standard and guideline for IT governance and management published by ISACA (Information Systems Audit and Control Association) [20]. Control objectives for information and related technology (COBIT) is a well-known IT governance (ITG) framework that groups IT best practices [21]. COBIT is a collection of documentation and guidelines for implementing Information Technology governance appropriately [22]. COBIT is a framework for the governance and management of information and technology, aimed at the whole enterprise [23]. IT Auditing is the formal, independent, and objective examination of an organization's IT infrastructure to determine whether the activities (e.g., procedures, controls, etc.) involved in gathering, processing, storing, distributing, and using information comply with guidelines, safeguard assets, maintain data integrity, and operate effectively and efficiently to achieve the organization's objectives [24].

Based on the explanation above, this study uses COBIT 2019, looking at IT governance maturity and applying the ten COBIT 2019 design factors, ranging from organizational objectives and risk profiles to IT-related issues, compliance needs, and technology adoption strategies [25]. Looking at the problems in the health center, which is the object of this research, which is more directed at issues regarding IT, IT service risks, and technology adoption strategies, the author uses COBIT 2019, which is said to be easy to use in the domain of an information system evaluation and a domain that focuses on services and risk management from technology adoption.

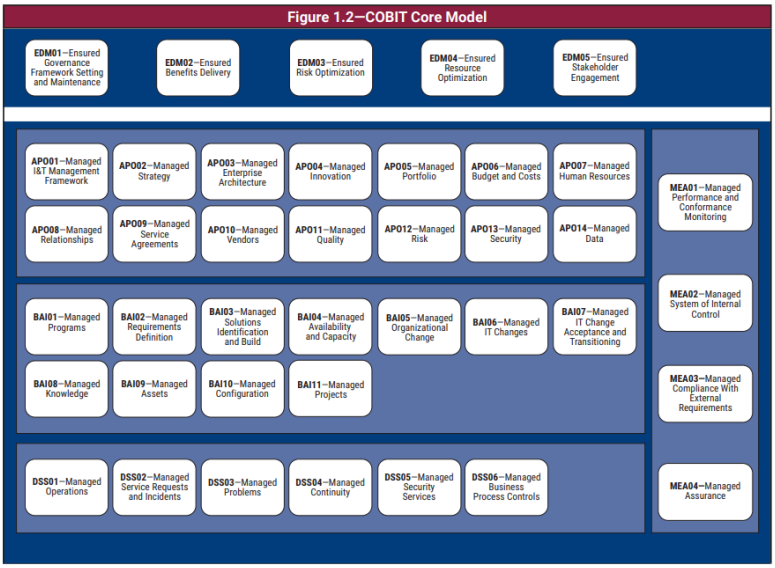

Figure 1. Cobit core model [26]

## METHODS

Nevertheless, there are issues with the Pengasinan Community Health Centre in Bekasi City's e-puskesmas Information System Audit. Fourteen domains—APO14, BAI01—BAI11, DSS01—DSS06, MEA01—MEA04, EDM01—EDM05 are produced by COBIT 2019 utilizing eleven design variables. In this research, several domains from COBIT 2019 were used, such as APO12, DSS02, and GAP Analysis. This research reveals the main themes: 1 standard and 2 domains, namely COBIT 2019 with domains DSS02 (service management) and APO12 (risk management) [27], [28]. By conducting analysis, you can provide recommendations to improve the organization's capabilities to meet the agency's expectations and goals regarding IT governance in supporting its performance [29]. The measuring the level of capability, because measuring the level of maturity is carried out if the measurement of the level of capability [30] is in line with the targets [31], such as APO12, DSS02, and GAP Analysis.

The researcher created a research procedure that is depicted in the Figure 2 below in order to meet the goals of risk management (APO12) [32], management of services and demand (DSS02), and Gap analysis.

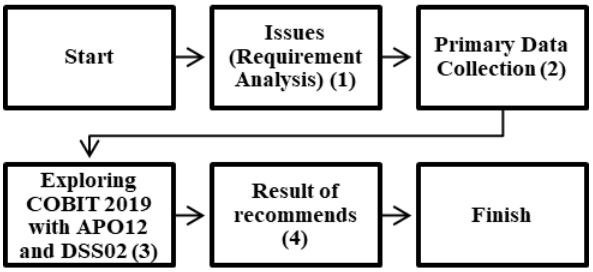


Figure 2. Research stages and workflow

There are 4 stages in conducting research regarding audits at e-Puskesmas in the Pengasinan Community Health Center, Bekasi City. These stages include: 1) Requirement analysis; 2) Data collection; 3) Exploring COBIT 2019; 4) Recommended results.

**Primary Data Collection**

The research results contained a technology governance management design [33] factors. The data collection was conducted using [34], from the interviews and the observations [35] in community health centres that are involved in using e-puskesmas. The qualitative method is carried out by observing and interviewing related parties, namely registration staff and health workers who use information technology. In the meanwhile, questionnaires are used to gather data for the quantitative [36], [37] approach. The sample was selected using a random sampling method through online surveys [38] to obtain quantitative data.

**Capability Index Formula**

Maturity level is used to control information technology processes using the COBIT framework with information on assessment/scoring methods [39]. In the IS audit process, maturity/capability is a part of the stage will be conducted of IT processes [40]. The results obtained by respondents will create a mapping of the position of each system process in the capability assessment model. The results of the questionnaire calculations and the achievement of the capability level, on the current and expected conditions [41]. In the IS audit process, maturity/capability is a part of the stage will be conducted of IT processes [40]

$$Capability\ Index\ (CI) = \frac{\sum Yes\ (Y)}{\sum Indicators} \quad (1)$$

$$Achievement\ (A) = IC\ x\ 100\% \quad (2)$$

The results of the questionnaire calculations and the achievement of the capability level, on the current and expected conditions [41].

Table 1. Capability level

| Level | Interpretation | Score Range (%) |
|---|---|---|
| 1 | Not Achieved | 0 – 15 |
| 2 | Partially Achieved | 16 – 50 |
| 3 | Largely Achieved | 51 – 85 |
| 4 | Fully Achieved | 86 – 100 |

To advance to the next level of capability assessment, one must have a Fully (4) rating or more than 85 percent [42].

## RESULT AND DISCUSSION

### Result

As with the data findings in the introduction above, several data collection techniques were used, such as observation and interviews [43], [44]. A detailed analysis of the requirements and functionalities of the platform is conducted through stakeholder consultations, interviews, and surveys [45]. The audit will focus on the following IT-related issues:

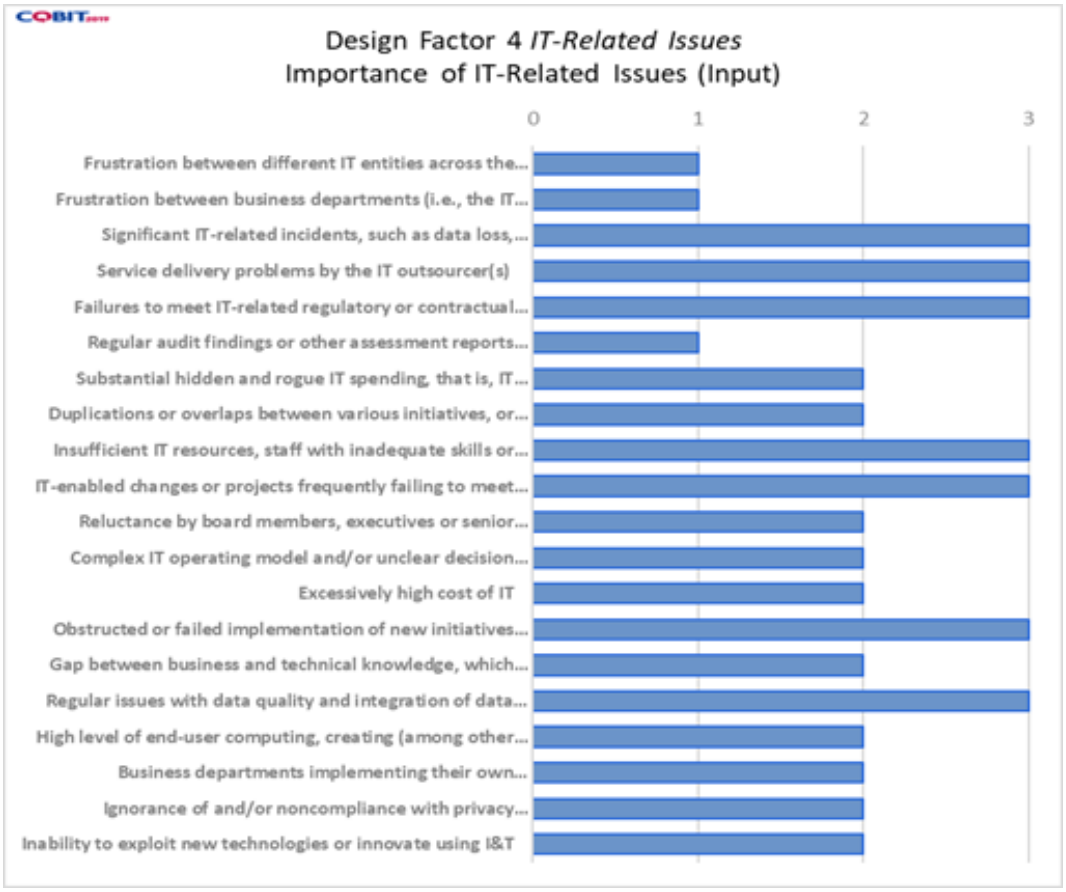


Figure 3. Design factor IT related issues

Figure 3 is the fourth stage in the factor design, which shows the results that three IT-related problems are not problematic, ten are in the problematic category, and seven are serious problems. COBIT 2019 refers to these, collectively, as design factors, which the enterprise must consider in tailoring its governance systems to realize the most value from its use of I&T [46]. The IT problems that will be discussed in this research are serious problems, namely data loss, security breaches, project failures and application errors, provision of services by IT service providers, failure to fulfill regulatory or contractual requirements related to IT, IT resources that are insufficient, staff with inadequate skills, or staff fatigue/dissatisfaction, IT-enabled changes or projects often fail to meet business needs and are delivered late or over budget, delayed or failed implementation of new initiatives or innovations caused by architecture and systems in today's IT, and routine issues with data quality and data integration across multiple sources.

The results obtained by respondents will create a mapping of the position of each system process in the capability assessment model. In Exploring COBIT 2019, researchers present the design factor results as in Figure 4 Design Factor Results.

Figure 4. Design factor results

In Figure 4 above is the result of the stages of factor design, where each domain has a different value. The COBIT 2019 process is determined through the measurement of design factors [47]. However, with the existing problems and observations made by visiting the observation site, the focus for assessing the level of capability is the DSS02 and APO12 domains.

Table 2. APO12 activity level 1 capability

| Activities | Σ Yes | No |
|---|---|---|
| Using the e-puskesmas system can identify and reduce risks | 20 | 0 |
| Level Results | 100% (*Fully*) | |

The activity from APO12, "Using the e-puskesmas system can identify and reduce risks," had 20 respondents who selected "yes," as shown in table 2, meaning that the level 1 capability result was "Fully".

Table 3. APO12 activity level 2 capability

| Activities | Σ Yes | No |
|---|---|---|
| The use of the e-puskesmas system can establish and maintain methods for data analysis | 19 | 1 |
| Using the e-puskesmas system can record data related to existing risks | 19 | 1 |
| Using the e-puskesmas system can identify support personnel, related applications and facilities | 19 | 1 |
| The use of the e-puskesmas system can collect current risk scenarios by category and functional | 18 | 2 |
| Level Results | 93.75% (*Fully*) | |

The APO12 "Activity Level 2 Capability" is explained in table 3, where users may make sure that e-puskesmas can be handled appropriately. Based on their search results, the respondents received a result of 93.75%, or "Fully."

Table 4. APO12 calculation results

| Process | | Score |
|---|---|---|
| APO12 Level 1 | | 100% |
| APO12 Level 2 | | 93.75% |
| Capability Level Results | Total | 193.75% |
| | Average | 96.88% |

The results of calculating APO12 are shown in Table 4, where the final score of 96.88% indicates a noteworthy level of success.

Table 5. DSS02 activity level 1 capability

| Activities | Σ Yes | No |
|---|---|---|
| The use of the e-puskesmas system can provide timely responses to the community and restore normal services | 17 | 3 |
| Level Results | 85% (*Largely*) | |

Table 6. DSS02 activity level 2 capability

| **Activities** | Σ **Yes** | **No** |
|---|---|---|
| IT use can log all service requests and incidents | 19 | 1 |
| Service requests on the e-puskesmas system can be activated and classified | 19 | 1 |
| To make a service request, verification of rights is required | 19 | 1 |
| Obtain financial and functional approval or signing in using the e-puskesmas system | 17 | 3 |
| The use of IT can identify and explain possible causes of incidents in applications to find a solution | 18 | 2 |
| Investigate if problems occur with the e-puskesmas system | 17 | 3 |
| More expertise is needed in using the e-puskesmas system to be able to assign incidents to specialist functions | 18 | 2 |
| E-puskesmas services can select and implement temporary/permanent solutions | 19 | 1 |
| Supports in recording whether the solution is used for resolution in the e-puskesmas system | 20 | 0 |
| The e-puskesmas system service can carry out recovery actions | 19 | 1 |
| Document future resolution of knowledge source incidents in the e-puskesmas system | 19 | 1 |
| In using the e-puskesmas system, verification with affected users is required that service requests have been fulfilled satisfactorily | 20 | 0 |
| The use of IT can cover service requests and incidents | 17 | 3 |
| Monitor handling procedures to progress towards resolution or settlement in the e-puskesmas system | 19 | 1 |
| Level Results | 92.85% (*Fully*) | |

Table 7. DSS02 activity level 3 capability

| Activities | Σ Yes | No |
|---|---|---|
| The use of IT can determine incidents and service request classifications based on priority schemes as well as criteria for registration issues | 19 | 1 |
| Determine incident models for known errors to enable efficient and effective resolution of the e-puskesmas system | 19 | 1 |
| Determine the service request model according to the type of service request to enable independent and efficient service for e-puskesmas system requests | 17 | 3 |
| When using the e-puskesmas system, you can establish incident escalation rules and procedures, especially for major incidents and security incidents related to data on the e-puskesmas system. | 19 | 1 |
| Using IT can find out about incidents and requests on the e-puskesmas system | 19 | 1 |
| The use of the e-puskesmas system can fulfill requests by carrying out selected request procedures | 19 | 1 |
| Identifying stakeholder information and their needs in the form of data or reports in the e-puskesmas system | 19 | 1 |
| Level Results | 93.57% (*Fully*) | |

Table 8. DSS02 calculation results

| Process | | Score |
|---|---|---|
| DSS02 Level 1 | | 85% |
| DSS02 Level 2 | | 92.85% |
| DSS02 Level 3 | | 93.57% |
| Capability Level Results | Total | 271.42% |
| | Average | 90.47% |

Table 8 presents the results of DSS02 level 3 calculations, achieving a final result of 90.47%, indicating a substantial level of accomplishment.

Table 9. GAP analysis results

| Domain | Current Capability Value (as-is) | Expected Capability Value (to-be) | GAP |
|---|---|---|---|
| APO12 | 1 | 4 | 3 |
| DSS02 | 2 | 4 | 2 |

The APO12 domain has a gap of three, while the DSS02 domain has a gap of two, according to the results in the table above. This indicates that the actions taken inside the DSS02 and APO12 domains have been in line with their corresponding domain functions.

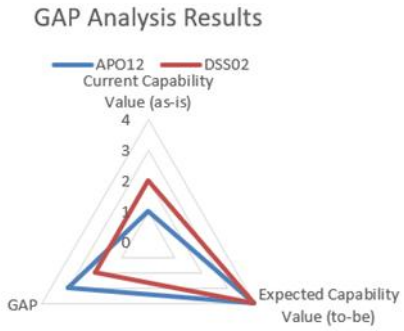


Figure 5. Radar chart GAP analysis

**Discussion**

Analytical interpretation of achieved capability levels for APO12 and DSS02, states that:

1. APO12 (Managing Risk): This domain shows that the use of the e-health center system can identify and reduce risks, which is stated to be very well achieved (fully achieved). This occurs at APO12 level 1, and APO level 2 states that the risk level of using the e-health center system if constrained can be handled well by being recorded by the registration service officer as a form of support and responsibility by officers related to the facilities of the institution, with a very good level of achievement (fully achieved), so that at APO12 level 1-2 it is declared Managed.
2. DSS02 (Service Management): This domain shows that the management service of the e-health center system in the form of system use can provide timely responses to the community and restore normal services is stated as Mostly achieved, because this system service is more helpful in registering patients to obtain poly services at the health center, this statement is at DSS02 level 1, at DSS02 level 2 regarding identification if there are system constraints and their solutions, and this statement is achieved well (fully achieved), because the occurrence of system errors can be overcome with a manual system in the form of recording using formulas, and at DSS02 level 3, if there are constraints as at level 2 or greater than level 2 such as security systems, with the existence of manuals or SOPs implemented by the health center, that this result is achieved very well, so that at DSS02 levels 1-3 it is stated as Established.

**IS Audit Results Findings**

As a result of the SI audit that was carried out in the previous stages, several findings regarding the SI were found, including the following:

Table 10. Results Findings

| No | Findings | Impacts |
|---|---|---|
| 1 | Automatic Medical Record Number Retrieval Process | Patient identity data is missing, which slows down the medical records industry's operation if the data is still missing. |
| 2 | Patient Registration Process | Patients were waiting in line to register for consultation and diagnostic. |
| 3 | Storage of Patient Identity and Treatment History | Patient history data is no longer confidential due to data theft or disclosure. |
| 4 | System Services | Work in all fields is slowed down, and less reliable data is the outcome. |

From Table 10 of the findings, recommendation analysis results were made referring to these findings, including:1. Socialization of the rules for using technology; 2. training for technology users to maintain the good quality of official technical services; 3. Ensure system security in protecting patient data from irresponsible parties; 4. Risk management in the e-puskesmas system to minimize disruptions and incidents and be able to handle risks; 5. Carry out identification, collection, and analysis of data related to the performance of the e-puskesmas system process as evidence for reporting to management.

**Synthesis of Results Review**

This study shows that the e-Puskesmas IT governance at Pengasinan Community Health Center has achieved a high level of capability—96.88% in risk management (APO12) and 90.47% in service handling (DSS02). However, several problems are still encountered in the field, such as patient registration queues, data security vulnerabilities, and service disruptions. This indicates that although the system has high

capabilities, its implementation is still not optimal in meeting the real needs of users. Therefore, this study emphasizes that the success of IT governance is not only measured by numbers but also by the system's ability to solve daily problems at the service location. Recommendations include user training, strengthening data security, and increasing service responsiveness.

## CONCLUSION

This study obtained results by evaluating the IT governance of e-Puskesmas at Pengasinan Community Health Center, Bekasi, using the COBIT 2019 framework. The audit results showed a high level of IT capability of 96.88% for risk management (APO12) and 90.47% for service handling (DSS02), indicating that the IT governance process has been running effectively. However, several operational challenges were still found, such as patient registration queues, data security vulnerabilities, and technical disruptions. To overcome these, this study recommends several strategic steps, including improving user training, strengthening data security, and implementing sustainable risk management. Overall, COBIT 2019 has proven effective as an audit and evaluation tool for IT governance in the health sector, especially for digital-based public service systems such as e-Puskesmas. As for the next research, an information system audit will be conducted still using the COBIT 2019 Framework with the APO13 (Managed Security) domain to focus on cybersecurity and BAI06 (Managed IT Changes) to assess the system's adaptability to technological changes so as to expand the scope of the evaluation, especially in services to the community at the community health center.

## REFERENCES


[1] S. Chung and J. Chung, "The Korean approach to Industry 4.0: the 4th Industrial Revolution from regional perspectives," *European Planning Studies*, vol. 29, no. 9, pp. 1690–1707, 2021, doi: 10.1080/09654313.2021.1959645.

[2] Falahah and A. F. Santoso, "Design of Data Interchange Regulation for Regional ICT Office," *International Journal on Informatics Visualization*, vol. 6, no. 2, pp. 335–342, 2022, doi: 10.30630/joiv.6.1.546.

[3] D. S. Sayogo, S. B. C. Yuli, and W. Wiyono, "The Determinants of Smart Public Library Roles in Promoting Open Government in Indonesia," *International Information and Library Review*, vol. 0, no. 0, pp. 1–16, 2021, doi: 10.1080/10572317.2021.1936380.

[4] L. M. Haryanto and W. Setyonugroho, "Analysis of Management Information System Implementation at Pratama 24 Hour Clinic Firdaus," *Jurnal Aisyah: Jurnal Ilmu Kesehatan (JIKA)*, vol. 9, no. 1, pp. 52–66, 2023, doi: 10.30604/jika.v9i1.2373.

[5] O. Rachid, B. Hanan, and M. Fatima, "Ten years of Hospital Information Systems: A taxonomy attempt," *Procedia Computer Science*, vol. 239, pp. 1401–1408, 2024, doi: 10.1016/j.procs.2024.06.312.

[6] M. Kiruthika, A. Kumar, L. Krishnasamy, and V. Sarveshwaran, "Investigation on Preserving Privacy of Electronic Medical Record using Split Learning," *Procedia Computer Science*, vol. 233, no. April, pp. 614–622, 2024, doi: 10.1016/j.procs.2024.03.251.

[7] M. Ali and I. Miguel, "ScienceDirect ScienceDirect Cloud-Based Framework for Data Exchange to Enhance Global Cloud-Based Framework for Data Exchange to Enhance Global Healthcare Healthcare," *Procedia Computer Science*, vol. 241, no. 2023, pp. 570–575, 2024, doi: 10.1016/j.procs.2024.08.082.

[8] W. A. Prabowo, "Developing Compliant Audit Information System for Information Security Index: A Study on Enhancing Institutional and Organizational Audits Using Web-based Technology and ISO 25010:2011 Total Quality of Use Evaluation," *International Journal on Informatics Visualization*, vol. 8, no. 1, pp. 343–351, 2024, doi: 10.62527/joiv.8.1.1845.

[9] B. Arora and Z. Rahman, "Technology Analysis & Strategic Management Information technology investment strategies : a review and synthesis of the literature," vol. 7325, no. May, 2016, doi: 10.1080/09537325.2016.1181742.

[10] A. C. Y. Jeong, S. T. Lee, C. Y. Jeong, S. T. Lee, J. Lim, and C. Y. Jeong, "Information Security Breaches and IT Security Investments: Impacts on Competitors," *Information & Management*, 2018, doi: 10.1016/j.im.2018.11.003.

[11] A. Maritsa, U. Hanifah Salsabila, M. Wafiq, P. Rahma Anindya, and M. Azhar Ma'shum, "The Influence of Technology in the World of Education," *Al-Mutharahah: Jurnal Penelitian dan Kajian Sosial Keagamaan*, vol. 18, no. 2, pp. 91–100, 2021, doi: 10.46781/al-mutharahah.v18i2.303.

[12] L. Almeida and A. Respício, "Decision support for selecting information security controls," *Journal of Decision Systems*, vol. 27, no. May, pp. 173–180, 2018, doi: 10.1080/12460125.2018.1468177.
[13] T. Ali, M. Al-Khalidi, and R. Al-Zaidi, "Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review," *Journal of Computer Information Systems*, vol. 00, no. 00, pp. 1–28, 2024, doi: 10.1080/08874417.2024.2329985.
[14] A. Folasole, O. S. Adegboye, O. I. Ekuewa, and P. E. Eshua, "Security, Privacy Challenges and Available Countermeasures in Electronic Health Record Systems: A Review," *European Journal of Electrical Engineering and Computer Science*, vol. 7, no. 6, pp. 27–33, Nov. 2023, doi: 10.24018/ejece.2023.7.6.561.
[15] S. F. N. Tarigan and T. S. Maksum, "Utilization of E-Puskesmas Information System Services Using the Pieces Method," *Jambura Health and Sport Journal*, vol. 4, no. 1, pp. 29–36, 2022, doi: 10.37311/jhsj.v4i1.13446.
[16] G. Lax, R. Nardone, and A. Russo, "Enabling secure health information sharing among healthcare organizations by public blockchain," *Multimedia Tools and Applications*, vol. 83, no. 24, pp. 64795–64811, Jan. 2024, doi: 10.1007/s11042-024-18181-4.
[17] S. D. Putra, H. Herman, and A. Yudhana, "Academic Information System Governance Audit Using the Cobit 2019 Framework," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, no. 3, pp. 467–474, 2023, doi: 10.25126/jtiik.20231036361.
[18] J. Felicia, J. F. Andry, F. Adikara, D. Y. Bernanda, and K. Christianto, "Leveraging COBIT 2019 to Measure the Accounting Software Implementation in High Schools for Better Transparency," *Journal of Computer Science*, vol. 20, no. 2, pp. 218–228, 2024, doi: 10.3844/JCSSP.2024.218.228.
[19] D. K. Jamal and A. Kusumawati, "Information System Audit Using COBIT 2019 Framework in Construction Companies," *Quest Journals*, vol. 9, no. 4, pp. 20–29, 2023.
[20] E. Aflakhah and B. Soewito, "Assessing Information Security Using COBIT 2019 And ISO 27001:2013," *Journal of System and Management Sciences*, vol. 14, no. 3, pp. 127–145, 2024, doi: 10.33168/jsms.2024.0308.
[21] H. Bouayad, L. Benabbou, and A. Berrado, "Aligning information technology and supply chain: An approach to map SCOR to COBIT," *International Journal of Information System Modeling and Design*, vol. 12, no. 3, pp. 1–26, 2021, doi: 10.4018/IJISMD.2021070101.
[22] M. Rizki and E. Novianto, "Auditing Artificial Intelligence Using COBIT 2019," *Jurnal Sistem Informasi dan Informatika (JUSIFOR)*, vol. 2, no. 1, pp. 1–7, 2023, doi: 10.33379/jusifor.v2i1.1847.
[23] COBIT 2019, *Governance and Management Objectives*. 2019.
[24] Angel R. Otero, *Information Technology Control and Audit-Fifth Edition*. CRC Press, Taylor & Francis Group, 2019.
[25] G. M. W. Tangka and E. Lompoliu, "Information Technology Governance Using the COBIT 2019 Framework at PT. Pelindo TPK Bitung," *International Journal of Engineering, Science and InformationTechnology Volume*, vol. 9, no. 2, pp. 355–367, 2023, doi: 10.31154/cogito.v9i2.577.355-367.
[26] ISACA, *COBIT 2019 Framework - Introduction and Methodology*. 2019.
[27] A. Zilziana, M. Noor, A. P. Widodo, and K. Adi, "Evaluation of Information Technology Governance Using Cobit 2019 on Domain DSS ( Deliver , Service , Support ) at PT XYZ," *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, vol. 5, no. 2, pp. 15611–15618, 2019.
[28] B. Putra, M. Jazman, F. N. Salisah, K. Kampar, M. Cobit, and D. A. N. Itil, "it governance audit at the kampar regency library and archives department using cobit 2019 and itil 4 audit tata kelola ti di dinas perpustakaan dan kearsipan," *Jurnal Teknik Informatika (JUTIF)*, vol. 3, no. 6, pp. 1591–1600, 2022, doi: //doi.org/10.20884/1.jutif.2022.3.6.406.
[29] T. Nurul Annisa and H. Sulastri, "Analysis of Information Technology Governance of the Tasikmalaya City Manpower Service Using Framework COBIT 2019," *International Journal of Applied Information Systems and Informatics (JAISI)*, vol. 1, no. 1, pp. 1–7, 2023, doi: 10.37058/jaisi.v1i1.8989.
[30] F. X. Adrian and G. Wang, "Measure the Level Capability IT Governance in Effectiveness Internal Control for Cybersecurity Using the Cobit 2019 in Organization: Banking Company," *Journal of Theoretical and Applied Information Technology*, vol. 101, no. 5, pp. 1710–1723, 2023.

[31] J. Beato and M. I. Fianty, "COBIT 2019 Framework: Evaluating Knowledge and Quality Management Capabilities in a Printing Machine Distributor," *Journal of Information Systems and Informatics*, vol. 6, no. 1, pp. 1–12, 2024, doi: 10.51519/journalisi.v6i1.638.
[32] J. N. Utamajaya, S. H. Supangat, F. L. Gaol, and B. Ranti, "Hotel Information System Management Audit Using COBIT 2019 - APO12," in *2023 2nd International Conference for Innovation in Technology, INOCON 2023*, BINUS University, BINUS Graduate Program School of Information System, Jakarta, Indonesia: Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/INOCON57975.2023.10101245.
[33] R. A. Nugraha and R. Syaidah, "Smart Campus Governance Design for XYZ Polytechnic Based on COBIT 2019," *International Journal on Informatics Visualization*, vol. 6, no. 3, pp. 718–725, 2022, doi: 10.30630/joiv.6.3.1257.
[34] Y. Liu and C. Li, "Insights into Talent Cultivation in Big Data Management and Application Major Based on Recruitment Information," *Procedia Computer Science*, vol. 242, pp. 568–575, 2024, doi: 10.1016/j.procs.2024.08.107.
[35] D. Riehle, A. Wolters, and K. Müller, "Adopting Artificial Intelligence in a Decision Support System — Learnings from Comment Moderation Systems," *Submitted and currently under review at the 18th International Conference on Wirtschaftsinformatik*, vol. 239, no. 2023, pp. 1847–1855, 2023, doi: 10.1016/j.procs.2024.06.366.
[36] Bulya and U. Pribadi, "Community Acceptance of SIKESAL : An UTAUT Model Approach in E-Government Services in Jambi City," *Scientific Journal of Informatics*, vol. 11, no. 3, pp. 661–680, 2024, doi: 10.15294/sji.v11i3.7511.
[37] R. G. Utomo and R. Yasirandi, "Securing Digital Wallet Loyalty : Unveiling the Impact of Privacy and Security," *Scientific Journal of Informatics*, vol. 11, no. 2, pp. 287–302, 2024, doi: 10.15294/sji.v11i2.2423.
[38] S. A. Nuswantoro, M. Ulfi, and M. Rafli, "Identification of Factors Influencing the Use of QRIS Using TAM and UTAUT 2 Methods," *Scientific Journal of Informatics*, vol. 11, no. 2, pp. 451–466, 2024, doi: 10.15294/sji.v11i2.3562.
[39] Purwadi and H. Santoso, "Comparison of Information Technology Governance Maturity Levels Based on COBIT 2019 at PT Kereta Commuter Indonesia in 2023 and 2024," *Jurnal Teknik Informatika (JUTIF)*, vol. 6, no. 5, pp. 2962–2974, 2025, doi: 10.52436/1.jutif.2025.6.5.5200.
[40] H. Nugroho, "A Review on Information System Audit Using COBIT Framework," *IJAIT (International Journal of Applied Information Technology)*, vol. 03, no. 02, p. 46, 2020, doi: 10.25124/ijait.v3i02.2114.
[41] L. G. Toyner and S. Sfenrianto, "Information System Security Evaluation Using Cobit 5 Framework," *Journal of Information System Management (JOISM)*, vol. 4, no. 2, pp. 147–157, 2023, doi: 10.24076/joism.2023v4i2.992.
[42] E. M. Lompoliu, G. B. R. F. Francolla, G. R. Mandoya, and M. D. Walangitan, "Information Technology Governance Analysis Using The COBIT 2019 Framework at XYZ Institution," *CogITo Smart Journal*, vol. 8, no. 2, pp. 346–358, 2022, doi: 10.31154/cogito.v8i2.427.346-358.
[43] M. M. M. S. Sumardiono, "Design of Futsal Match Message Application With Waterfall," *INFOTECH: Jurnal Informatika & Teknologi*, vol. 2, pp. 25–32, 2021, doi: 10.37373/infotech.v2i1.107.
[44] S. Sumardiono and Marfu'ah, "Design and Development of a Letter Archival Information System using the Waterfall Model," *Gema Wiralodra*, vol. 12, no. 2, pp. 269–278, 2021, doi: 10.31943/gemawiralodra.v12i2.192.
[45] A. Shinde, V. Mane, N. Ambulgekar, and Z. Ansari, "Renewable Energy Trading Platform using Blockchain," *Procedia Computer Science*, vol. 233, pp. 243–253, 2024, doi: 10.1016/j.procs.2024.03.214.
[46] F. CA. Abdul Rafeq, CISA, CGEIT, "COBIT Design Factors: A Dynamic Approach to Tailoring Governance in the Era of Digital Disruption," ISACA. Accessed: Sep. 26, 2024. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2019/cobit-design-factors
[47] 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, 2023, doi: 10.34288/jri.v5i4.212.