**Business Management**
Vol. 5 No 3 Agustus 2026
*p-ISSN:2828-7606, e-ISSN:2828-8203*
*Link: https://ejournal.mandalanursa.org/index.php/Bisnis*

# IT Governance Capability Assessment Using COBIT 2019 DSS Domain: A Case of DKI Jakarta Education Office

**Yasmin Arafah Hakim[1], Zaldy Adrianto[2]**
[1,2]Universitas Padjadjaran, Indonesia

**Article Info**

***Article history:***
Accepted: 18 July 2026
Publish: 1 Agustus

***Keywords:***
*IT Governance;*
*COBIT 2019;*
*DSS Domain;*
*Capability Level;*
*Process Assessment Model;*

**Abstract**

*As a provider of digital education services, the DKI Jakarta Provincial Education Office requires effective information technology (IT) governance to support the implementation of the Electronic-Based Government System (SPBE). However, the current SPBE evaluation does not assess the capability of IT processes at the operational level. Therefore, this study aims to: (1) assess the capability level of information technology governance within the Deliver, Service, and Support (DSS) domain using the COBIT 2019 framework, (2) analyze the gap between the current capability level (as-is) and the target capability level (to-be), (3) identify weaknesses in information technology service processes based on the capability assessment and gap analysis, and (4) formulate recommendations to improve information technology service governance. A qualitative approach with a case study method was employed. Data were collected through interviews, observations, and document analysis involving five informants selected using purposive sampling based on the RACI chart. The data were analyzed using the Process Assessment Model (PAM) to determine the capability level of each DSS process. The results indicate that DSS01, DSS04, DSS05, and DSS06 achieved Capability Level 3 (Established Process), while DSS02 and DSS03 achieved Capability Level 2 (Managed Process). Gap analysis revealed that all DSS processes remain below the target Capability Level 4 (Predictable Process), primarily due to the absence of quantitative process performance measurement, inadequate operational documentation, and insufficient monitoring and control mechanisms. The identified capability gaps reveal weaknesses in IT service processes, including the absence of standardized incident and problem management procedures, limited quantitative performance measurement, inadequate process control mechanisms, and incomplete operational documentation. Based on these findings, this study recommends developing Standard Operating Procedures (SOPs), establishing Key Performance Indicators (KPIs), and strengthening monitoring, control, and cross-unit coordination mechanisms to improve the quality of IT service governance. The findings also demonstrate that COBIT 2019 complements SPBE evaluation by providing a detailed operational-level capability assessment that supports continuous improvement of digital public services.*



***Corresponding Author:***
**Yasmin Arafah Hakim**
Universitas Padjadjaran, Indonesia
Email Correspondent: yasmin22005@mail.unpad.ac.id

## 1. INTRODUCTION

The rapid development of information technology (IT) has significantly changed the way public sector organizations deliver services and manage administrative processes.

Governments increasingly rely on digital technologies to improve service quality, enhance operational efficiency, and support evidence-based decision-making through digital governance initiatives [18]. In Indonesia, this transformation is implemented through the Electronic Based Government System (SPBE) as a national framework for digital governance [8]. As one of Indonesia's leading provinces in digital transformation, DKI Jakarta has consistently demonstrated a high level of digital readiness, reflected in its Information and Communication Technology (ICT) Development Index.

Despite this achievement, high digital readiness does not necessarily indicate effective governance of operational IT services. The implementation of SPBE primarily evaluates digital governance from an institutional and policy perspective, focusing on organizational readiness, digital transformation, and governance maturity. However, SPBE evaluation does not specifically assess the capability of operational IT processes responsible for ensuring service availability, incident management, service continuity, security, and operational controls. Consequently, organizations with strong digital infrastructure may still experience operational weaknesses that cannot be identified through macro-level SPBE evaluation alone [15].

This issue is particularly relevant to the DKI Jakarta Provincial Education Office, which manages various digital education services, including the New Student Admission System (PPDB), educational administration services, and integrated educational data management. These digital services require reliable IT operations, effective incident handling, business continuity, and information security to ensure uninterrupted public service delivery. Therefore, evaluating operational IT governance capability becomes essential for maintaining service quality and organizational performance [14].

Previous studies on information technology governance have widely applied framework such as ITIL, ISO/IEC 27001, and COBIT to evaluate IT governance in public sector organizations [3]. These studies generally focus on service management, security aspects, or governance structures. Most of these studies emphasize governance maturity, information security management, or IT service management. However, relatively few studies have specifically assessed the capability level of operational IT processes using the COBIT 2019 framework, particularly within the Deliver, Service, and Support (DSS) domain in the public education sector. In addition, most prior studies generally focus on measuring existing governance conditions without systematically identifying capability gaps and formulating improvement recommendations based on target capability levels [20]. Furthermore, prior studies tend to emphasize general governance evaluation rather than systematically analyzing the gap between current (as-is) and expected (to-be) capability levels.

Based on these limitations, this study proposes an assessment approach using the COBIT 2019 framework with a specific focus on the Deliver, Service, and Support (DSS) domain, which covers six operational processes: Managed Operations (DSS01), Managed Service Requests and Incidents (DSS02), Managed Problems (DSS03), Managed Continuity (DSS04), Managed Security Services (DSS05), and Managed Business Process Controls (DSS06). (ISACA, 2018). This domain emphasizes operational service management, including incident handling, service continuity, and system security, which are critical for ensuring the effectiveness of IT-base public services [13]. Capability assessment was conducted using the Process Assessment Model (PAM), which adopts the ISO/IEC 33020 capability measurement framework, enabling each process to be evaluated based on Process Attributes and Capability Levels ranging from Level 0 to Level 5. [6].

The target capability level in this study was established at Capability Level 4 (Predictable Process). This level was selected because the DKI Jakarta Provincial Education Office has implemented an Information Security Management System (ISMS) based on

ISO/IEC 27001:2022 and has documented operational procedures for most IT service processes. Therefore, the organization is expected not only to perform standardized processes (Level 3) but also to manage and control those processes through measurable performance indicators, quantitative monitoring, and continuous evaluation consistent with the characteristics of Capability Level 4.

In addition to evaluating operational IT governance capability within the DSS domain, this study contributes methodologically by explicitly describing the capability assessment process using the COBIT 2019. Unlike SPBE evaluation, which primarily measures institutional digital governance maturity, this study evaluates the capability of operational IT processes and identifies capability gaps together with structured improvement recommendations. Accordingly, this study aims to assess the capability level of IT governance processes within the DSS domain using the COBIT 2019 framework, analyze the gap between current capability level (as-is) and the target capability level (to-be), identify weaknesses in information technology service processes based on the capability assessment and gap analysis, and formulate recommendations to improve operational IT governance at the DKI Jakarta Provincial Education Office.

## 2. RESEARCH METHOD

This study employed a qualitative approach with a case study design to evaluate information technology (IT) governance at the DKI Jakarta Provincial Education Office. The assessment focused on the Deliver, Service, and Support (DSS) domain of the COBIT 2019 framework, which comprises six management objectives: DSS01 (Managed Operations), DSS02 (Managed Service Requests and Incidents), DSS03 (Managed Problems), DSS04 (Managed Continuity), DSS05 (Managed Security Services), and DSS06 (Managed Business Process Controls) [7]. A qualitative case study was selected to obtain an in-depth understanding of operational IT governance practices within their real organizational context.

Data were collected through primary and secondary sources. Primary data were obtained through semi-structured interviews with relevant stakeholders involved in managing information technology services, while secondary data were collected through document analysis to support data validity through triangulation. Five informants were selected using purposive sampling based on the RACI (Responsible, Accountable, Consulted, Informed) Chart, ensuring that each informant represented roles directly involved in the DSS management objectives. During the field study, some personnel represented multiple roles in the RACI matrix; therefore, one informant represented more than one RACI role while ensuring that all RACI responsibilities remained represented. Data collection continued until data saturation was achieved, indicated by the absence of new themes, codes, or meaningful information relevant to the research objectives [1].

The collected data were analyzed using the interactive analysis model proposed by [12], consisting of data condensation, data display, and conclusion drawing/verification. To improve the credibility of the findings, triangulation was conducted by comparing information obtained from interviews, observations, and organizational documents. The triangulation process was used to confirm the consistency of evidence before determining the capability assessment results [19].

The capability assessment was conducted using the COBIT 2019 Process Assessment Model (PAM), which adopts the capability measurement framework defined in ISO/IEC 33020. Each DSS process was evaluated through the corresponding Process Attributes (PA) at every capability level. Assessment evidence obtained from interviews, observations, and document analysis was compared with the criteria specified for each Process Attribute. The achievement of every attribute was rated using four categories: Not Achieved (N), Partially

Achieved (P), Largely Achieved (L), and Fully Achieved (F) [6]. The overall capability level was then determined progressively, where a process could advance to the next capability level only after satisfying the required Process Attributes at the preceding level. Finally, a gap analysis was performed by comparing the current capability level (*as-is*) with the target capability level (*to-be*) to identify capability gaps and formulate improvement recommendations.

## 3. RESULTS AND DISCUSSION

The DKI Jakarta Provincial Education Office is a regional government agency responsible for education services in the province of DKI Jakarta under the coordination of the Governor through the Regional Secretary in accordance with (Peraturan Gubernur DKI Jakarta No.57/2022). Within its structure, the Center for Education Data and Information Technology (Pusdatin Pendidikan) is responsible for managing IT services, supports digital education systems, and coordinating with the Jakarta Communication, Informatics and Statistics Office (Diskominfotik) as the SPBE infrastructure provider and with the Population and Civil Registration Office (Dukcapil) for student-data integration, in line with Presidential Regulation No. 39/2019 on One Data Indonesia and Governor Regulation of the Special Capital Region of Jakarta Number 11 of 2018 concerning Guidelines for Cryptography Administration for Information Security .

The capability assessment identified different levels of process capability across the six DSS management objectives. The following section presents the capability assessment results, followed by the gap analysis and discussion of the factors influencing the achievement of each capability level.

### 3.1 Capability Level of the DSS Processes

Capability levels were determined by comparing evidence obtained from interviews, observations, and document analysis against the process attributes (PA) required at each level of the COBIT 2019 Process Capability Model. Each attribute was rated on the Not Achieved (N), Partially Achieved (P), Largely Achieved (L), Fully Achieved (F) scale before the overall capability level was concluded [6]. Table 1 summarizes the capability assessment results.

**Table 1. Recapitulation of Capability Level per DSS Process**

| Domain | PA1.1 | PA2.1 | PA2.2 | PA3.1 | PA3.2 | PA4.1 | Capability Level |
|---|---|---|---|---|---|---|---|
| DSS01 Managed Operations | F | F | L | L | L | P | Level 3 (Established) |
| DSS02 Managed Service Requests & Incidents | F | L | L | P | P | P | Level 2 (Managed) |
| DSS03 Managed Problems | F | L | L | P | P | P | Level 2 (Managed) |
| DSS04 Managed Continuity | F | L | L | L | L | P | Level 3 (Established) |
| DSS05 Managed Security Services | F | F | L | L | L | P | Level 3 (Established) |
| DSS06 Managed Business Process Controls | F | F | L | L | L | P | Level 3 (Established) |

DSS01 (Managed Operations) achieved capability level 3 (Established Process), indicating that operational IT activities have been standardized, documented, and implemented consistently across the organization. Operational procedures are supported by the Information Security Management System (ISMS) based on ISO/IEC 27001:2022, with clearly defined responsibilities and coordination mechanisms. However, the organization has not yet implemented quantitative performance measurement through Key Performance Indicators (KPIs), and operational monitoring is still primarily based on

periodic evaluations and user reports. Consequently, the requirements of PA4.1 (Process Measurement) and PA4.2 (Process Control) have not been fulfilled, preventing progression to Capability Level 4.

DSS02 (Managed Service Requests and Incidents) and DSS03 (Managed Problems) both achieved capability level 2 (Managed Process). The assessment indicates that service requests, incident handling, and problem management activities have been implemented through structured operational practices, including ticket recording, classification, prioritization, escalation, and corrective actions. However, both processes remain largely dependent on operational experience rather than formally standardized procedures. The assessment identified the absence of documented Standard Operating Procedures (SOPs), inconsistent implementation of incident and problem management processes, limited documentation of incident resolution and problem analysis, and the lack of standardized Root Cause Analysis (RCA). Consequently, the requirements of PA3.1 (Process Definition) and PA3.2 (Process Deployment) were only Partially Achieved, preventing both processes from progressing to Capability Level 3 (Established Process).

DSS04 (Managed Continuity) achieved capability level 3. Service continuity is supported through scheduled database backups, distributed microservice architecture, and coordination with Diskominfotik for infrastructure availability. These practices demonstrate that continuity processes have been defined and consistently implemented. However, continuity performance is not yet evaluated using measurable indicators such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Consequently, PA4.1 and PA4.2 remain only partially achieved.

DSS05 (Managed Security Services) achieved capability level 3. Information security controls, including firewall protection, role-based access control, secure coding practices, and server activity monitoring, have been implemented consistently under the Information Security Management System (ISO/IEC 27001:2022). Despite these strengths, security performance has not yet been evaluated using measurable security indicators or quantitative monitoring mechanisms. Therefore, the process has not fulfilled the requirements for Capability Level 4.

DSS06 (Managed Business Process Controls) achieved capability level 3. Business process controls are implemented through layered validation mechanisms, segregation of duties, user acceptance testing, and mandatory approval procedures before system implementation. These controls ensure consistent operational governance and support reliable service delivery. Nevertheless, the effectiveness of these controls is not yet measured through quantitative performance indicators or formal control metrics. Accordingly, PA4.1 and PA4.2 remain partially fulfilled, preventing advancement to Capability Level 4.

Overall, four processes DSS01, DSS04, DSS05, and DSS06 achieved capability level 3 (Established Process), indicating that procedures are documented, standardized, and applied consistently. In contrast, DSS02 and DSS03 remained at capability level 2 (Managed Process) because process standardization has not been formally documented. Across all six DSS processes, the principal factor limiting progression to level 4 (Predictable Process) is the absence of quantitative process measurement, documented performance indicators, and data-driven process control mechanisms.

### 3.2 Gap Analysis

Capability level 4 (Predictable Process) was established as the target capability level for the DKI Jakarta Education Office, because it reflects its position as a public-service provider with a high dependency on the availability, security, and reliability of information systems, and consistent with the direction of SPBE (Presidential Regulation No. 95/2018)

and the ISO 27001:2022-based Information Security Management System, both of which push organizations toward measurable, data-driven process control. Table 2 presents the gap between the current (as-is) and target (to-be) capability levels for each DSS process.

**Table 2. Gap Analysis of the DSS Domain**

| Domain | As-Is | To-Be | Gap |
|---|---|---|---|
| DSS01 – Managed Operations | 3 | 4 | 1 |
| DSS02 – Managed Service Requests & Incidents | 2 | 4 | 2 |
| DSS03 – Managed Problems | 2 | 4 | 2 |
| DSS04 – Managed Continuity | 3 | 4 | 1 |
| DSS05 – Managed Security Services | 3 | 4 | 1 |
| DSS06 – Managed Business Process Controls | 3 | 4 | 1 |

The gap analysis indicates that all six DSS processes remain below the target capability level. DSS01, DSS04, DSS05, and DSS06 showed a one-level gap, while DSS02 and DSS03 showed a two-level gap. Although most operational processes have been standardized and consistently implemented, the assessment identified several Process Attributes that have not yet been fully achieved. The identified gaps can be grouped into three categories.

First, process standardization weaknesses were observed in DSS02 and DSS03. Although incident handling and problem management activities are performed routinely, neither process is supported by formally documented Standard Operating Procedures (SOPs), standardized Root Cause Analysis (RCA), or consistently deployed operational procedures. Consequently, PA3.1 (Process Definition) and PA3.2 (Process Deployment) were only partially achieved, preventing both processes from reaching Capability Level 3.

Second, process performance measurement weaknesses represent the primary factor preventing all DSS processes from achieving Capability Level 4. The organization has not yet established measurable Key Performance Indicators (KPIs), quantitative Service Level Agreements (SLAs), or performance measurement mechanisms capable of demonstrating process predictability. As a result, PA4.1 (Process Measurement) has not been fulfilled across all assessed DSS processes.

Third, process control weaknesses remain evident because evaluation results have not yet been systematically utilized to control or improve operational performance. For example, DSS04 has not established measurable Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets, while DSS05 and DSS06 do not yet employ KPI-based evaluation mechanisms to measure the effectiveness of security controls and business process controls. Consequently, PA4.2 (Process Control) remains only partially achieved.

These findings demonstrate that the capability gaps are primarily associated with higher-level Process Attributes rather than deficiencies in operational implementation. While most operational activities have already been performed consistently, organizations require measurable performance indicators, quantitative monitoring, and data-driven process control mechanisms to progress toward Capability Level 4.

### 3.3 Discussion

#### 3.3.1 Capability Level and Digital-Based Education Services

The capability assessment indicates that the DKI Jakarta Provincial Education Office has established a relatively mature operational IT governance environment, with four DSS processes achieving Capability Level 3 (Established Process). This demonstrates that operational activities have been formally defined, documented, and consistently

implemented through standardized procedures, clearly assigned responsibilities, and an Information Security Management System (ISMS) aligned with ISO/IEC 27001:2022. Nevertheless, the organization has not yet achieved Capability Level 4 (Predictable Process), as process performance is primarily evaluated through operational monitoring and periodic reviews rather than quantitative performance measurement. The absence of measurable Key Performance Indicators (KPIs) and data-driven process control mechanisms indicates that operational IT services have been implemented effectively; however, strengthening process measurement and control remains essential to improve the predictability, reliability, and sustainability of digital education services.

### 3.3.2 Relationship between Capability Level and the ICT–SPBE Gap

The findings demonstrate that high digital readiness does not necessarily reflect mature operational IT governance. Although DKI Jakarta has a high ICT Development Index and SPBE evaluation score, the capability assessment revealed that two DSS processes remain at Capability Level 2, while none has reached Capability Level 4. This indicates that SPBE primarily evaluates digital governance at the institutional level, whereas COBIT 2019 provides a more detailed assessment of operational IT processes. Consequently, capability assessment offers a deeper understanding of operational IT governance conditions that cannot be fully identified through SPBE evaluation alone.

### 3.3.3 COBIT 2019 as a Complement to SPBE Evaluation

SPBE evaluation focuses on assessing digital government implementation at the organizational level, whereas COBIT 2019 evaluates the capability of operational IT processes through the Process Assessment Model (PAM). In addition to determining the capability level of each DSS process, the assessment identifies Process Attributes that have not yet been achieved, enabling organizations to understand the underlying causes of capability gaps. The assessment revealed several operational weaknesses, including the absence of documented Incident Management procedures, Problem Management standardization, Key Performance Indicators (KPIs), and quantitative process measurement mechanisms. These findings demonstrate that COBIT 2019 complements SPBE evaluation by providing a more detailed assessment of operational IT governance and supporting evidence-based improvement planning.

### 3.3.4 Implications for Education Service Governance

The findings suggest that improving operational IT governance requires measurable process management supported by Key Performance Indicators (KPIs), Service Level Agreements (SLAs), standardized operational procedures, and performance-based monitoring to achieve Capability Level 4 (Predictable Process). These improvements are expected to enhance the reliability and consistency of digital education services while strengthening the implementation of SPBE within the DKI Jakarta Provincial Education Office.

## 3.4 Improvement Recommendations

Based on the capability assessment and gap analysis, all six DSS processes still show a difference between the current (as-is) and target (to-be) capability levels. The recommendations were developed by considering the unmet Process Attributes (PA) identified through the COBIT 2019 Process Assessment Model (PAM), supported by evidence obtained from interviews, observations, document analysis, and COBIT 2019 good practices. The proposed improvements primarily address process standardization, process measurement, and process control to support the achievement of Capability Level 4 (Predictable Process). A summary of the recommendations is presented in Table 3.

**Table 3. Summary of Improvement Recommendations**

| Domain | As-Is → To-Be | Key Improvement Recommendations |
|---|---|---|
| DSS01 – Managed Operations | 3 → 4 | Develop operational KPIs, define service-level SLAs, implement an operational performance monitoring dashboard. |
| DSS02 – Managed Service Requests & Incidents | 2 → 4 | Formalize an Incident Management SOP, define incident classification and priority levels, integrate all incident records into a single ticketing system |
| DSS03 – Managed Problems | 2 → 4 | Formalize a Problem Management SOP, apply Root Cause Analysis (RCA), document problem-resolution outcomes. |
| DSS04 – Managed Continuity | 3 → 4 | Define Recovery Time Objective (RTO) and Recovery Point Objective (RPO) targets, implement backup and recovery performance monitoring. |
| DSS05 – Managed Security Services | 3 → 4 | Establish security KPIs, implement a security monitoring dashboard, establish periodic security incident trend reporting. |
| DSS06 – Managed Business Process Controls | 3 → 4 | Establish business process control KPIs, conduct periodic performance-based control evaluations. |

Overall, the proposed recommendations are intended to address the unmet Process Attributes identified during the capability assessment. For DSS02 and DSS03, priority should be given to establishing standardized Incident Management and Problem Management procedures before implementing quantitative performance measurement. For the remaining DSS processes, improvement efforts should focus on strengthening process measurement and control through KPIs, SLAs, RTO/RPO targets, and performance-based monitoring. Implementing these recommendations is expected to support progression toward Capability Level 4 (Predictable Process) while improving the reliability, consistency, and sustainability of digital education services.

### 3.5 Limitations and Future Research

This study is subject to several limitations. The assessment was conducted only at the DKI Jakarta Provincial Education Office using the COBIT 2019 framework and was limited to the Deliver, Service, and Support (DSS) domain; therefore, the findings represent only the operational aspect of IT governance rather than the overall governance capability across all COBIT 2019 domains. Furthermore, this study focused on capability assessment and the development of improvement recommendations without evaluating their implementation or effectiveness. Future research is encouraged to include other COBIT 2019 domains, such as Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), and Monitor, Evaluate and Assess (MEA), as well as to validate the proposed recommendations through quantitative or mixed-methods approaches involving broader organizational units to provide a more comprehensive evaluation of IT governance.

## 4. CONCLUSION

Based on the findings, four conclusions can be drawn.

1. The capability assessment using the COBIT 2019 Process Assessment Model (PAM) showed that DSS01, DSS04, DSS05, and DSS06 achieved Capability Level 3 (Established Process), while DSS02 and DSS03 achieved Capability Level 2 (Managed Process). These results indicate that most operational IT processes have been standardized and consistently implemented, although improvements in process management and control are still required.

2. Capability gaps remain across all DSS processes compared with the target Capability Level 4 (Predictable Process). DSS01, DSS04, DSS05, and DSS06 each have a one-level gap, whereas DSS02 and DSS03 have a two-level gap. The gaps are primarily associated with unmet Process Attributes related to process measurement and process control.
3. The assessment identified operational IT governance weaknesses not explicitly captured by SPBE evaluation, including the absence of documented Standard Operating Procedures (SOPs) for incident and problem management, the lack of standardized Root Cause Analysis (RCA), limited Key Performance Indicators (KPIs), inadequate quantitative performance measurement, and insufficient data-driven process control mechanisms. These weaknesses explain why several DSS processes have not yet achieved the expected capability level.
4. Based on the capability assessment and gap analysis, this study proposes improvement recommendations to strengthen information technology service governance. The recommendations include developing SOPs, implementing KPIs and Service Level Agreements (SLAs), applying Root Cause Analysis (RCA), establishing Recovery Time Objective (RTO) and Recovery Point Objective (RPO), and strengthening performance monitoring and process control mechanisms to support the achievement of Capability Level 4 (Predictable Process).

The findings indicate that the DKI Jakarta Education Office has established a reasonably sound operational governance of information technology, but still requires strengthening in performance measurement, process control, and continuous improvement to make IT service management more effective in supporting the implementation of the Electronic-Based Government System (SPBE).

## 5. BIBLIOGRAPHY

[1] Ahmed, S. K. (2025). Sample size for saturation in qualitative research: Debates, definitions, and strategies. *Journal of Medicine, Surgery, and Public Health, 5*, Article 100171. https://doi.org/10.1016/j.glmedi.2024.100171

[2] Al Mouf, D., & Sari, F. W. (2025). Audit tata kelola teknologi informasi di PT SMOE Indonesia menggunakan framework COBIT 2019. *Journal of Applied Multimedia and Networking, 8*(2), 47–58. https://doi.org/10.30871/jamn.v8i2.9067

[3] Budiman, A., & Lubis, Y. F. A. (2025). Perbandingan framework COBIT 2019 dan ITIL 4 dalam tata kelola teknologi informasi. *Jurnal Ilmu Komputer dan Teknik Informatika, 1*(2), 52–57. https://doi.org/10.64803/juikti.v1i2.50

[4] Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage Publications.

[5] Gouwnalan, S. K., & Tanaamah, A. R. (2023). The Application of COBIT 2019 Framework in the Evaluation of Information Technology Governance. *Jurnal Teknik Informatika dan Sistem Informasi, 9*(2). https://doi.org/10.28932/jutisi.v9i2.6373

[6] ISACA. (2018). *COBIT® 2019 framework: Governance and management objectives*. ISACA.

[7] ISACA. (2018). *COBIT® 2019 framework: Introduction and methodology*. ISACA.

[8] Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. (2024). *Keputusan Menteri PANRB Nomor 13 Tahun 2024 tentang evaluasi Sistem Pemerintahan Berbasis Elektronik (SPBE).*

[9] Kesuma, I. N. R. W., Hermadi, I., & Nurhadryani, Y. (2023). Evaluasi tata kelola teknologi informasi di Dinas Pertanian Gianyar menggunakan COBIT 2019. *Jurnal Teknologi Informasi dan Ilmu Komputer, 10*(3), 513–522. https://doi.org/10.25126/jtiik.2023106565

[10] Kunio, N. I. H., Utami, E., & Muhammad, A. H. (2022). Audit tata kelola TI berbasis COBIT 2019 di Politeknik XYZ. *Jurnal Ilmiah Universitas Batanghari Jambi, 22*(2), 876. https://doi.org/10.33087/jiubj.v22i2.1994

[11] Kurniawan, A., Friadi, J., Sutjahjo, G., & Desvazulinda, E. (2025). Tata kelola teknologi informasi pada sektor pendidikan dan kesehatan: Penerapan framework COBIT 2019 untuk meningkatkan efektivitas layanan publik. *Zona Komputer: Program Studi Sistem Informasi Universitas Batam, 15*(2). https://doi.org/10.37776/zkomp.v15i2.2044

[12] Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). *Qualitative data analysis: A methods sourcebook* (4th ed.). Sage Publications.

[13] Nugroho, A. P., & Ambarwati, A. (2025). Analisis tata kelola teknologi informasi di PT Garam menggunakan framework COBIT 2019 domain *Deliver, Services & Support*. *Jurnal Tata Kelola dan Kerangka Kerja Teknologi Informasi, 11(1) https://doi.org/10.34010/jtk3ti.v11i1.15782*

[14] Nurhidayat, Nurmandi, A., & Misran. (2024). Evaluation of the challenges of e-government implementation: Analysis of the E-Government Development Index in Indonesia. Jurnal Manajemen Pelayanan Publik, 8(2). https://doi.org/10.24198/jmpp.v8i2.52759

[15] Puspitaningrum, A. C., Fitrani, L. D., & Sintiya, E. S. (2024). Systematic literature review: Implementation COBIT as a best practice of Electronic-Based Government System governance. *SISTEMASI, 13*(1), 335–349. https://doi.org/10.32520/stmsi.v13i1.3639

[16] Prasetyo, T. M. A., & Sitokdana, M. N. N. (2021). Analisis tata kelola pusat data dan informasi Kementerian XYZ menggunakan COBIT 2019. *Journal of Applied Computer Science and Technology (JACOST), 2*(2), 95–107. https://doi.org/10.52158/jacost.v2i2.265

[17] Safitri, A., Syafii, I., & Adi, K. (2021). Measuring the performance of information system governance using framework COBIT 2019. *International Journal of Computer Applications, 174*(31), 23–30. https://doi.org/10.5120/ijca2021921253

[18] Sarwar, M. I., Abbas, Q., Alyas, T., Alzahrani, A., Alghamdi, T., & Alsaawy, Y. (2023). *Digital Transformation of Public Sector Governance With IT Service Management-A Pilot Study. In IEEE Access (*Vol. 11, pp. 6490–6512*). Institute of Electrical and Electronics Engineers Inc*. https://doi.org/10.1109/ACCESS.2023.3237550

[19] Sugiyono. (2022). *Metode penelitian kuantitatif, kualitatif, dan R&D* (2nd ed.). Alfabeta.

[20] Windasari, I. P., Yonanta, M. Y., Himawati, R. Y., & Rochim, A. F. (2022). Audit tata kelola teknologi informasi pada perusahaan menggunakan domain DSS dan MEA kerangka kerja COBIT 2019 (Studi kasus: Fakultas Teknik UNDIP). *Teknik, 43*(1), 67–77. https://doi.org/10.14710/teknik.v43i1.34121