Jurnal E-Komtek
Vol. 10, No. 1. (2026) pp. 338-346
https://jurnal.politeknik-kebumen.ac.id/index.php/E-KOMTEK
p-ISSN : 2580-3719 e-ISSN : 2622-3066

Evaluation of Internal Control on the Siakad Application at Politeknik Kesehatan Bhakti Setya Indonesia Using Cobit 2019

Adi Cahyo Kuswijayanto[1], Suhirman[2], Joko Sutopo[3], Muhammad Senoaji Wibowo[4]

[1,2,3]Department of Information Technology Magister, Universitas Teknologi Yogyakarta, Indonesia, 55285
[4]Politeknik Kesehatan Bhakti Setya Indonesia, Indonesia,

asasuke77adi@gmail.com

https://doi.org/10.37339/e-komtek.v10i1.3010

Published by Politeknik Piksi Ganesha Indonesia

Artikel Info
Submitted:
23-01-2026
Revised:
05-06-2026
Accepted:
06-06-2026
Online first :
30-06-2026

Abstract

The digitalization of higher education has made Academic Information Systems (SIAKAD) essential assets requiring effective IT internal controls. This study evaluates the capability level of internal controls in the SIAKAD application at Poltekkes Bhakti Setya Indonesia (BSI) using the COBIT 2019 framework and identifies improvement opportunities. Data were collected through in-depth interviews with six key respondents, including IT management, SIAKAD operators, and the Head of Academic Affairs, supported by institutional documents. The assessment focused on five COBIT 2019 processes: APO12, DSS01, DSS05, BAI10, and MEA02. The results indicate that most processes remain at Capability Level 1 (Performed Process), while DSS01 achieved Level 2 (Managed Process). The largest capability gap was identified in MEA02, which remains at Level 0 (Incomplete Process), whereas APO12, DSS05, and BAI10 each showed a gap of two levels. These findings provide practical recommendations to strengthen IT governance and achieve Capability Level 3 (Established Process) through standardized procedures and continuous internal monitoring.

Keywords: Internal Control, SIAKAD, IT Governance, COBIT 2019, Capability Level

Abstrak

Digitalisasi pendidikan tinggi menjadikan Sistem Informasi Akademik (SIAKAD) sebagai aset penting yang memerlukan pengendalian internal teknologi informasi yang efektif. Penelitian ini bertujuan mengevaluasi tingkat kapabilitas pengendalian internal pada aplikasi SIAKAD di Poltekkes Bhakti Setya Indonesia (BSI) menggunakan kerangka kerja COBIT 2019 serta mengidentifikasi kesenjangan untuk menyusun rekomendasi perbaikan. Data dikumpulkan melalui wawancara mendalam dengan enam responden kunci yang terdiri atas pengelola TI, operator SIAKAD, dan Kepala Bagian Akademik, serta didukung oleh dokumen operasional institusi. Penilaian difokuskan pada lima proses COBIT 2019, yaitu APO12, DSS01, DSS05, BAI10, dan MEA02. Hasil penelitian menunjukkan bahwa sebagian besar proses berada pada Level 1 (Performed Process), sedangkan DSS01 telah mencapai Level 2 (Managed Process). Kesenjangan terbesar ditemukan pada MEA02 yang masih berada pada Level 0 (Incomplete Process), sementara APO12, DSS05, dan BAI10 memiliki kesenjangan dua level. Temuan ini menghasilkan rekomendasi praktis untuk memperkuat tata kelola TI melalui standarisasi prosedur dan pengawasan internal yang berkelanjutan guna mencapai Level 3 (Established Process).

Kata Kunci: Pengendalian Internal, SIAKAD, Tata Kelola TI, COBIT 2019, Tingkat Kapabilitas

1. Introduction

The rapid development of Information and Communication Technology (ICT) has transformed the operational landscape of higher education. ICT adoption enables institutions to enhance the efficiency and quality of academic services [1]. Poltekkes Bhakti Setya Indonesia (BSI), operating in the health sector, relies on ICT for the Tridharma Perguruan Tinggi (Three Pillars of Higher Education). A critical component is the Academic Information System (SIAKAD), which manages the student lifecycle from registration and curriculum management to grade input and graduation, serving as the primary source of academic data transparency and accuracy [2].

The implementation of effective IT governance has become urgent for organizations aligning strategy with technology. In the education sector, studies have proposed framework harmonization using feature selection and K-Means clustering to produce data-driven governance maturity profiles [3]. In the health sector, institutions such as RSUD ODSK and PT PLN Suluttenggo utilized COBIT 2019 to identify governance priority objectives [4] [5]. Models integrating NIST CSF and COBIT 2019 have been developed for comprehensive information security measurement [6].

The high degree of reliance on SIAKAD demands strong internal IT controls. Internal control consists of policies, procedures, and practices designed to ensure business objectives are achieved and operational risks can be prevented, detected, and corrected [7]. Failure to manage internal controls exposes the institution to risks including data leakage, system errors affecting academic records, and operational inefficiencies. COBIT 2019 is a globally recognized framework for governance and management of information and technology [8], offering domains, objectives, and practices to help organizations achieve business goals through the effective and controlled use of IT [9].

Despite the critical role of SIAKAD, no formal evaluation of IT internal controls has been conducted at Poltekkes BSI. This research gap—the absence of an empirical capability assessment for IT internal control in health-focused higher education using COBIT 2019—provides the primary motivation for this study. This research has three objectives: (1) assess the capability level of internal control within SIAKAD against relevant COBIT 2019 processes; (2) identify gaps between the current condition and the target capability level; and (3) provide practical recommendations to enhance internal control effectiveness and IT governance at Poltekkes BSI.

2. Method

This research employs a descriptive qualitative approach with a case study method to evaluate internal control on SIAKAD at Poltekkes BSI. The COBIT 2019 framework is applied to five IT management processes selected based on direct alignment with SIAKAD operational risks: APO12 (Manage Risk), addressing organizational risk management **[10]**; DSS01 (Manage Operations), covering routine IT activities; DSS05 (Manage Security Services), guaranteeing academic data security **[11]**; BAI10 (Manage Configuration), addressing system change integrity; and MEA02 (Monitor, Evaluate, and Assess the System of Internal Control), as the oversight mechanism for all other processes.

Data were collected through triangulation comprising: (1) in-depth semi-structured interviews with six key respondents—two IT management staff, two SIAKAD operators, one Head of Academic Affairs, and one internal quality auditor—selected purposively based on direct involvement with SIAKAD; and (2) document review of official operational policies, SOPs, and incident logs related to SIAKAD.

Analysis proceeded through three stages. First, As-Is Assessment mapped interview and document evidence against Base Practices of each COBIT 2019 process: Level 0 (no evidence), Level 1 (ad-hoc performance), Level 2 (planned and monitored), Level 3 (defined, documented, standard process). Second, Gap Analysis compared As-Is results with the target Level 3 (Established Process). Third, improvement recommendations were formulated to close identified gaps.

3. Results and Discussion

3.1 Existing Process Capability Level (As-Is Assessment)

This assessment measures the level of internal control implementation in SIAKAD processes at Poltekkes BSI based on the COBIT 2019 Process Capability Model. Capability levels were determined by assessing Base Practices fulfillment, validated through interviews and document verification. Results are presented in **Table 1.**

Table 1. Existing SIAKAD Process Capability Levels

No.	COBIT 2019 Process	Process Description	Existing Capability Level
1	APO12	Manage Risk	Level 1 (Performed Process)
2	DSS01	Manage Operations	Level 2 (Managed Process)
3	DSS05	Manage Security Services	Level 1 (Performed Process)
4	BAI10	Manage Configuration	Level 1 (Performed Process)
5	MEA02	Monitor, Evaluate, and Assess System of Internal Control	Level 0 (Incomplete Process)

As shown in **Table 1,** most SIAKAD management processes are at Level 1 (Performed Process). Basic control functions are carried out ad-hoc but lack formally managed procedures. Only DSS01 achieved Level 2 (Managed Process). The most critical finding is MEA02 at Level 0 (Incomplete Process), indicating the complete absence of formal internal control monitoring. This pattern is consistent with similar studies in health-sector institutions, where operational processes tend to reach Level 1–2 while oversight functions remain underdeveloped **[13] [14]**.

Figure 1. Gap Analysis Capability Level COBIT 2019 - SIAKAD Poltekkes BSI

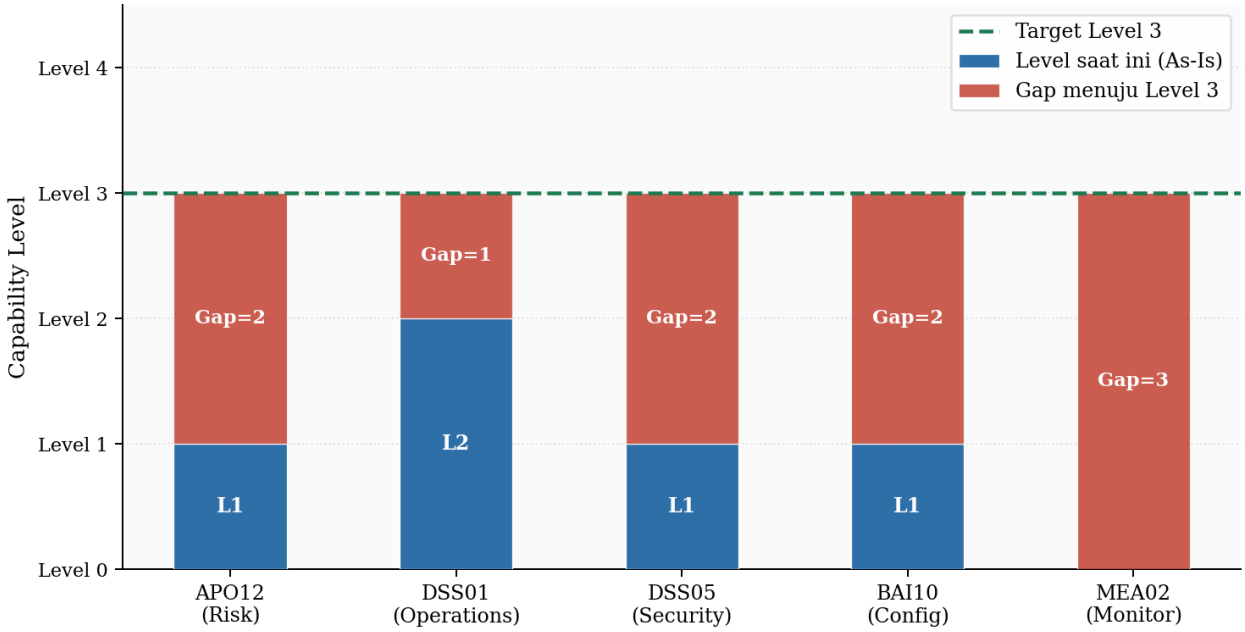

Figure 1. Gap Analysis Capability Level COBIT 2019 – SIAKAD Poltekkes BSI

3.2 Capability Gap Analysis

The Target Capability Level (To-Be) for all processes is set at **Level 3 (Established Process)**, representing Poltekkes BSI's need for defined, documented, and structured processes. The gap is calculated by comparing the target with the existing level, as shown in **Table 2.**

Table 2. SIAKAD Process Capability Gap Analysis

No.	COBIT 2019 Process	Target Level (To-Be)	Existing Level (As-Is)	Gap
1	APO12	Level 3	Level 1	2
2	DSS01	Level 3	Level 2	1
3	DSS05	Level 3	Level 1	2
4	BAI10	Level 3	Level 1	2
5	MEA02	Level 3	Level 0	3 (Critical)

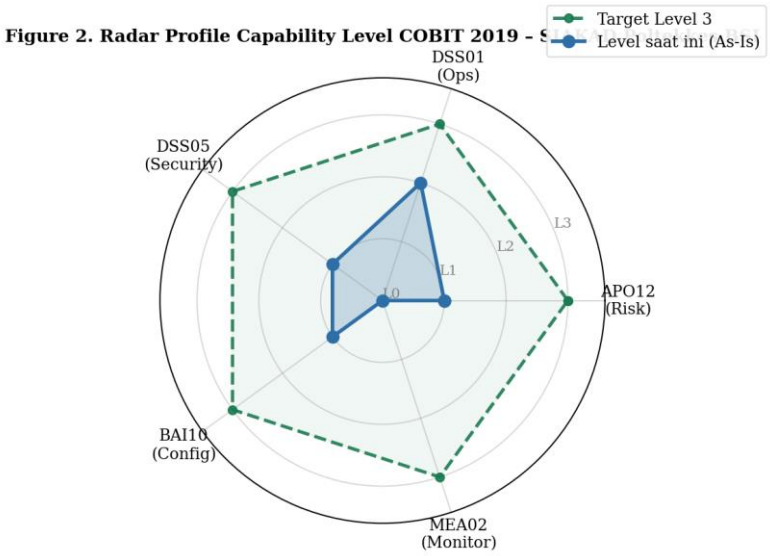

Figure 2. Radar Profile Capability Level COBIT 2019 – SIAKAD Poltekkes BSI

3.3 Discussion

3.3.1 Interpretation of Capability Levels and Implications

The research results show that SIAKAD internal control is dominated by Level 1 (Performed Process) with a critical Level 0 in MEA02. This indicates IT activities are performed but rely on individual efforts without formally managed procedures, making the system susceptible to human error and threatening academic data integrity. The absence of defined Process Attributes (PA 2.1–PA 3.1) prevents Poltekkes BSI from guaranteeing SIAKAD operates according to approved procedures, hindering achievement of Alignment and Value Delivery business goals. Comparable findings were reported by Tangka et al. [1] at PT PLN Suluttenggo and Wulyatiningsih & Mambu [2] at RSUD ODSK, confirming that health-sector institutions share common structural barriers to IT governance maturity.

3.3.2 Critical Gap: Oversight Foundation (MEA02, Gap = 3)

MEA02 at Level 0 is the most significant gap. As the mechanism verifying the effectiveness of all other control processes, its absence means Poltekkes BSI cannot validate whether Level 1

and Level 2 processes are actually effective, and there is no separation between self-assessment and operational functions—a fundamental internal control principle. To reach Level 3, the institution must establish an internal audit and monitoring function supported by management-endorsed policies.

3.3.3 Significant Gaps: Risk, Security, and Configuration (APO12, DSS05, BAI10, Gap = 2)

APO12 (Manage Risk): Risks are not identified proactively. The institution is reactive after incidents rather than maintaining a formal risk register for preventive action.

DSS05 (Manage Security Services): SIAKAD security remains basic. The absence of defined Role-Based Access Control (RBAC) procedures and routine vulnerability testing increases potential for data leakage and manipulation.

BAI10 (Manage Configuration): System changes are made without formal Change Management controls, violating system integrity principles.

3.4 Improvement Recommendations to Achieve Level 3

Recommendations are focused on fulfilling missing Process Attributes to advance each process toward Level 3. **Table 3** presents specific actions with implementation priorities, as also illustrated in **Figure 3.**

Table 3. Improvement Recommendations per COBIT 2019 Process

Process	Gap	Key Recommendation	Priority
MEA02	3	Implement IT Compliance Function: Establish a unit responsible for self-assessment and reporting IT performance to top management periodically.	Immediate (0–3 months)
APO12	2	Formalize Risk Management: Draft and ratify an IT Risk Management Policy; create a Risk Register reviewed quarterly.	Short-term (3–6 months)
DSS05	2	Implement Access Control and Testing: Implement RBAC matrix and mandate annual penetration testing on SIAKAD.	Short-term (3–6 months)
BAI10	2	Implement Change Management: Establish formal procedures (submission, approval, testing, documentation) for all SIAKAD modifications.	Short-term (3–6 months)
DSS01	1	Operational Standardization: Document, communicate, and consistently implement all operational procedures including backup and Disaster Recovery.	Medium-term (6–12 months)

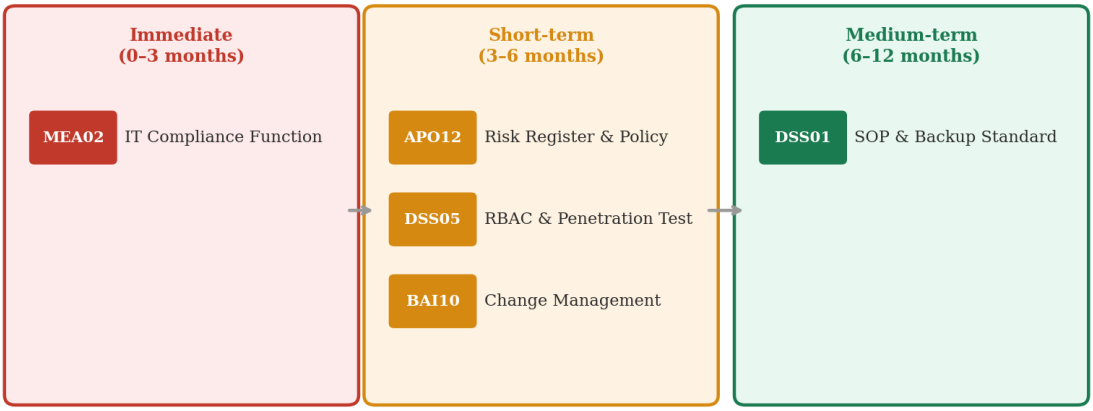

Figure 3. Implementation Roadmap – Improvement Recommendations

3.5 Managerial and Research Implications

The findings require Poltekkes BSI to immediately shift its IT management focus from executing tasks (performed) to managing and defining processes (established). This transition requires strong top management support for resource allocation, training, and documentation formalization. Scientifically, this research confirms the relevance of COBIT 2019 as an effective diagnostic tool for measuring IT internal control in health higher education academic systems, where no comparable empirical model previously existed.

4. Conclusion

Based on the internal control evaluation on the SIAKAD application at Poltekkes Bhakti Setya Indonesia using COBIT 2019, the overall IT management process capability is dominated by Level 1 (Performed Process). The most critical gap (Gap = 3) was identified in MEA02 (Level 0), indicating the complete absence of formal internal control oversight. Significant gaps (Gap = 2) were found in APO12, DSS05, and BAI10, indicating high vulnerability to operational and security risks. To achieve Level 3 (Established Process), Poltekkes BSI must prioritize formalization and documentation of procedures and build a sustainable internal oversight function to guarantee academic data integrity.

This study is limited to five COBIT 2019 processes and a single institution. Capability assessment relies on qualitative evidence subject to respondent bias. Future studies could evaluate the effectiveness of these recommendations through longitudinal assessment, or expand the scope to include APO13 or BAI06 for a more comprehensive governance picture.

Acknowledgement

The authors express gratitude to God Almighty for His grace in allowing this research to be completed successfully. The authors also thank the management of Poltekkes Bhakti Setya Indonesia for their cooperation and participation as research subjects.

References

[1] G. M. W. Tangka, C. Lumingkewas, and E. Lompoliu, "IT Governance Maturity Assessment at PT PLN Suluttenggo Using COBIT 2019," International Journal of Engineering, Science and Information Technology, vol. 5, no. 2, pp. 195–203, 2025.

[2] T. Wulyatiningsih and J. Y. Mambu, "IT Governance Maturity and Business Alignment: A COBIT 2019 Evaluation at RSUD ODSK," International Journal of Engineering, Science and Information Technology, vol. 5, no. 2, pp. 248–255, 2025.

[3] R. Setyadi and A. A. Rahman, "Enhancing IT Governance Based on Risk and Security Analysis in a Private School: A COBIT 2019 Approach," JOIV: International Journal on Informatics Visualization, vol. 9, no. 5, pp. 2148–2156, 2025.

[4] K. M. AL-Qatanani, "The impact of implementing information technology governance based on the COBIT-2019 framework on institutional performance," Edelweiss Applied Science and Technology, vol. 9, no. 3, pp. 84–95, 2025.

[5] R. Y. Pratama and S. Umaroh, "An IT Asset Governance Model Design Using COBIT 2019 and ITIL V4 Framework at BKU Itenas," E3S Web of Conferences, vol. 484, p. 02006, 2024.

[6] M. Fadya and D. N. Utama, "Towards Secure Information Systems: Developing and Implementing an Information Security Evaluation Model Using NIST CSF and COBIT 2019," TEM Journal, vol. 14, no. 1, pp. 182–191, 2025.

[7] S.-Y. Huang, T. Wang, Y.-T. Huang, and T.-N. Yeh, "Information security risk items and management practices for mobile payment using non-financial-institution service providers," International Journal of Accounting Information Systems, vol. 53, p. 100684, 2024.

[8] I. Kirpitsas and T. Pachidis, "KIBO, a new hybrid software development method with enhanced information systems auditing capability," Information and Software Technology, vol. 190, p. 107958, 2026.

[9] J. Casamassa, W. Wang, and M. Masialeti, "Generative AI governance for cybersecurity: an integrated approach," Issues in Information Systems, vol. 26, no. 3, pp. 484–493, 2025.

[10] T. R. McIntosh et al., "From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models," Computers & Security, vol. 144, p. 103964, 2024.

[11] J. C. Radjulan, A. Iriani, and J. Tambotoh, "Evaluation IT Governance Computer Network at Central Bureau of Statistics (BPS) Maluku Province Using COBIT 2019 DSS01 and DSS05 Domains," Barekeng, vol. 18, no. 4, pp. 2779–2794, 2024.

[12] L. Pietersen and R. J. Rudman, "Data-related risks for the use of machine learning in retail customer demand forecasting," South African Journal of Business Management, vol. 56, no. 1, p. a4766, 2025.

[13] Faradillah, Ermatita, and D. P. Rini, "Enhancing Governance Maturity Assessment in Higher Education Institutions Through Data-Driven Feature Selection and Clustering Techniques," Ingénierie des Systèmes d'Information, vol. 30, no. 10, pp. 2773–2783, 2025.

[14] R. Amalia and T. Handayani, "Evaluasi Tata Kelola Teknologi Informasi Menggunakan COBIT 2019 pada Domain APO12 (Manage Risk)," Jurnal Sistem Informasi, 2021.

[15] ISACA, COBIT 2019 Framework: Introduction and Methodology. Schaumburg, IL: ISACA, 2018.
[16] Jogiyanto, Sistem Informasi Keputusan. Yogyakarta: Andi Offset, 2005.
[18] A. Kristanto, Perancangan Sistem Informasi dan Aplikasinya. Yogyakarta: Gava Media, 2008.
[19] H. T. Sukmana et al., "A Framework of IT Governance Implementation Assessment Using COBIT 2019 in Educational Institution," Telkomnika, vol. 18, no. 2, pp. 1015–1026, 2020.
[20] P. Weill and J. W. Ross, IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Harvard Business School Press, 2004.
[21] COSO, Internal Control—Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission, 2013.