Published online on: https://journal.uii.ac.id/jurnalsnati/
DOI: 10.20885/snati.v5.i2.46893
Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi
Vol. 5 No. 2 (2026) 80 - 87 ISSN Media Electronic: 2807-5935

Auditing ABC University's New Student Registration System Maturity Level Through COBIT 2019

Luthfi Indana[1*], Ferdyanto Adhi Nugroho[2]
[1,2] Information System, Faculty of Information Technology, Merdeka University of Malang, Malang, Indonesia
[1*]luthfi.indana@unmer.ac.id, [2]ferdyantoadhinugroho@gmail.com

Abstract

The New Student Admissions Information System (PMB) at ABC University still faces several challenges, such as slow document verification, data inconsistencies, and a monolithic structure integrated with other systems (e.g., SIAKAD), which negatively impacts its performance. This study evaluates the performance of this web-based PMB system using the COBIT 2019 framework. A quantitative approach was employed, with data collected through interviews, observations, questionnaires, and document analysis. The study focuses on the DSS (Deliver, Service, Support) domain of COBIT 2019 to assess the system's maturity level. The analysis reveals that the PMB system's maturity level is 3.78 (Level 4), indicating that processes are well-established but require further optimization to reach Level 5 (Optimizing). To achieve this, PUSIM (Center for Information Technology and Multimedia) must develop and periodically review planning documents to ensure optimal performance of the information system services in line with institutional targets.

Keywords: New Student Admission; Information System; COBIT 2019; DSS; PUSIM

1. Introduction

In the contemporary business landscape, information technology has emerged as a critical organizational component, particularly through the implementation of information technology governance [1]. Digital transformation presents both opportunities and challenges for the Indonesian government, particularly in implementing data-driven policymaking [2]. To effectively manage an operational institution, we must first evaluate the current management processes to assess their effectiveness[3] [4].

The development of information technology has driven digital transformation in various universities, including in the New Student Admissions (PMB) system. ABC University, a leading private higher education institution in East Java, faces challenges in optimizing its PMB information system, such as slow document verification and data inconsistencies. This study aims to conduct a performance audit of the system using the COBIT 2019 framework to assess its maturity level, identify gaps, and provide evidence-based recommendations for improvement [5][6]. Previous studies, such as [5], evaluated e-learning quality at XYZ University in the APO11 and DSS01 domains, finding a maturity level of 3 (Established Process). Similarly, [7] analyzed PT. XYZ using the APO08, APO12, APO13, DSS04, and DSS05 domains, highlighting critical aspects requiring evaluation in organizations—with positive outcomes observed. However, recent research by [8] indicates that IT governance in some institutions remains at an initial stage (ad-hoc) and lacks full structure. Their recommendations include strengthening Standard Operating Procedures (SOPs), enhancing HR training, and implementing regular audits [9] [10].

This study offers a unique contribution by focusing specifically on private universities in Indonesia and utilizing the latest version of COBIT 2019. Supporting this research, [11] demonstrated that SMK IT Al Izhar Pekanbaru, a private vocational school, achieved level 5 (Optimized) in the EDM03 domain, indicating systematic and well-documented IT management. Similarly, [12] found that COBIT 2019 implementation assists the Islamic finance industry in identifying critical areas for improvement and allocating resources effectively to meet strategic objectives[2][8]. Furthermore, COBIT 2019 facilitates policy formulation, service management, regulatory compliance, and organizational security enhancement [13]. The quality of IT services is heavily dependent on the effectiveness of IT governance implementation [14][15]. This research aims to (1) analyze and formulate the maturity level of an information system using the COBIT 2019 framework based on analytical data and relevant supporting factors, as well as (2) to provide conclusions and recommendations for improving the maturity of the information system based on the evaluation results using COBIT 2019.

Received: 23-01-2026 | Revised: 28-06-2026 | Accepted: 03-07-2026 | Published: 15-07-2026

2. Research Methods

This study uses a quantitative research methodology with a case study design to conduct a performance audit of the New Student Registration Information System (PMB) at ABC University, utilizing the COBIT 2019 framework. Data collection involved multiple methods: (1) structured interviews with key stakeholders, (2) direct observation of system workflows, (3) maturity level assessment questionnaires, and (4) document analysis including Standard Operating Procedures (SOPs) and system performance reports [16]. For data analysis, researchers mapped IT processes to specific COBIT 2019 domains, particularly the Deliver, Service, and Support (DSS), followed by maturity level evaluation using the standardized 0-5 COBIT scale.

The research methodology comprises four primary stages: (1) preparation, involving process identification and instrument development; (2) data collection through structured interviews and questionnaires; (3) data analysis utilizing COBIT framework mapping and gap identification; and (4) formulation of improvement recommendations [17]. To ensure data validity, the study employed triangulation by cross-verifying multiple data sources and incorporating expert reviews from IT professionals. The research outcomes will yield a comprehensive audit report featuring maturity level assessment, gap analysis findings, and strategic recommendations for enhancing the new student admission information system [18][19]. This study establishes a foundation for informed decision-making aimed at optimizing the effectiveness and operational efficiency of the admission system at ABC University.

This study has two notable limitations. First, respondents consisted solely of three internal PUSIM management personnel who also serve as developers and administrators of the PMB system, carrying a risk of self-assessment bias; future research is encouraged to involve quality assurance units (LPMU) and system users such as prospective students and registration staff to improve assessment objectivity. Second, this study only covers five of the six DSS subdomains in COBIT 2019 (DSS01–DSS05), excluding DSS06 (Manage Business Process Controls), as it was deemed less applicable to the operational context of the PMB system and falls outside the direct responsibilities of PUSIM; future research may consider incorporating DSS06 for a more comprehensive evaluation.

To ensure the reliability of the assessment data, inter-rater reliability was calculated using Cohen's Kappa coefficient among the three respondents. Cohen's Kappa is computed using the formula:

$$\kappa = \frac{Po - Pe}{1 - Pe} \quad (1)$$

where P_0 represents the observed agreement proportion and P_e represents the expected agreement proportion by chance. The scoring matrix derived from the 31 questionnaire items shows that Respondent 1 and Respondent 2 achieved a Kappa value of 0.85, Respondent 1 and Respondent 3 achieved 0.91, and Respondent 2 and Respondent 3 achieved 0.90, yielding an average inter-rater reliability coefficient of 0.89. This value exceeds the commonly accepted threshold of 0.80, indicating strong agreement among raters and confirming that the assessment results are consistent and reliable across evaluators.

Although COBIT 2019 natively employs a capability attribute rating scale of Not Achieved (N), Partially Achieved (P), Largely Achieved (L), and Fully Achieved (F) for each process attribute, this study adopts a Likert scale (1–4) as a quantitative proxy to facilitate structured data collection from respondents. The conversion from Likert scores to maturity levels follows a proportional mapping approach, where a score of 1 corresponds to Level 1 (Initial), 2 to Level 2 (Managed), 3 to Level 3 (Established), and 4 to Level 4 (Quantitative/Predictable), with the average score across all items within a domain determining the final maturity index. A score exceeding 4.50 would indicate Level 5 (Optimizing). This mapping is consistent with prior COBIT-based studies that operationalize the N/P/L/F attributes into numerical scales to enable quantitative aggregation and inter-domain comparison, while acknowledging that this approach represents a simplification of the full COBIT 2019 Process Assessment Model (PAM).

3. Results and Discussions

The New Student Admissions Information System (PMB) at ABC University serves as the web-based platform for managing prospective student registrations. Operated by the Center for Information Technology and Multimedia (PUSIM), the PMB system shares technical infrastructure with other institutional systems including the Academic Information System (SIAKAD). Currently, the system's monolithic architecture - where it runs on the same server as SIAKAD and other campus systems- creates performance limitations that affect operational efficiency. The implementation also faces several technical challenges: (1) occasional errors in processing Population Identification Numbers (NIK) that could potentially be resolved through integration with the Indonesian Ministry of Home Affairs (Kemendagri) database verification system, and (2) minor payment processing inaccuracies occurring in approximately 2% of transactions. These operational constraints highlight opportunities for system optimization through architectural improvements and enhanced data validation mechanisms.

The PMB system processes an average of 5,000 new student applications annually, with peak loads occurring during the admission period from May to July. During these peak periods, system response times

increased by approximately 40%, leading to user dissatisfaction and administrative bottlenecks. Monolithic architecture compounds these challenges, as resource-intensive operations in one module (such as bulk document processing) directly impact the performance of other critical systems. This architectural limitation has been identified as a primary concern requiring strategic attention in the modernization roadmap.

Based on the results of field observations, a mapping of PUSIM management involvement in the COBIT domain was carried out to facilitate data collection and evaluation. The selection of respondents was strategically conducted to ensure comprehensive coverage of all relevant IT governance aspects within the organization. Each respondent was chosen based on their direct involvement in system operations, maintenance, and strategic decision-making processes.

Table 1. Respondent Mapping

Role Management	Stakeholder
Head IT Operations	Chairman of PUSIM
Service Manager	Head of Software Department PUSIM
Information Security Manager	Head of Hardware and Network Department PUSIM

Source: Research Data, 2023

The respondent mapping reflects the organizational structure of PUSIM and ensures that each critical domain of COBIT 2019 is evaluated by the most appropriate stakeholder. The Chairman of PUSIM, serving as Head IT Operations, provides strategic oversight and governance perspective. The Head of Software Department, acting as Service Manager, offers insights into application development, maintenance, and service delivery processes. The Head of Hardware and Network Department, fulfilling the Information Security Manager role, contributes expertise in infrastructure security, network management, and physical asset protection. This triangulated approach to data collection enhances the validity and reliability of the audit findings.

Through oral and written interviews, guided by the attached format, this study collected data that was assessed using a Likert scale. The questionnaire was designed to evaluate 31 specific process activities across five DSS domains. Each activity was rated on a scale of 1 to 4, where 1 indicates the process is not implemented, 2 indicates partial implementation, 3 indicates implementation with minor gaps, and 4 indicates full and consistent implementation. This scaling approach provides granular insights into the maturity level of each process component while maintaining consistency with the COBIT 2019 assessment methodology.

The questionnaire design incorporated best practices from previous IT governance audits and was validated through pilot testing with two IT professionals external to the study. This validation process ensured that questions were clearly worded, relevant to the COBIT 2019 framework, and appropriate for the organizational context of ABC University. The response distribution across the 31 activities reveals important patterns in process maturity, as detailed in Table 2.

Table 2. The number of respondents who answered in the range 1-4 using the Likert scale

No	Activity Process	Results			
		1	2	3	4
1	Maintain and develop operational procedures and related activities to support all services provided (DSS01.01)	-	-	1	2
2	Ensure that the company's requirements for information process security comply with SLAs and contracts with third-party service providers or hosting (DSS01.02)	-	-	1	2
3	Establish procedures to monitor event logs. Conduct ongoing reviews (DSS01.03)	-	-	1	2
4	Keep IT sites and server rooms in a safe and clean condition at all times (DSS01.04)	-	-	2	1
5	Review IT facility requirements for protection against power fluctuations and outages, in conjunction with other business continuity planning requirements. Procure appropriate uninterruptible power supply equipment (e.g., batteries, generators) to support business continuity planning. (DSS01.05)	-	-	1	2
6	Establish incident escalation procedures and rules, particularly for security incidents and major incidents (DSS02.01)	-	-	1	2
7	Record, classify, and prioritize requests and incidents. (DSS02.02)	-	-	1	2
8	Verify, approve, and fulfill service requests. (DSS02.03)	-	-	1	2
9	Investigate, diagnose and allocate incidents. (DSS02.04)	-	-	1	2
10	Resolve and recover from incidents. (DSS02.05)	-	-	1	2
11	Verify with the affected user that the service request has been satisfactorily fulfilled or the incident has been resolved satisfactorily and within an agreed/acceptable timeframe, then close the incident service request. (DSS02.06)	-	-	-	3
12	Track status and generate reports. (DSS02.07)	-	-	-	3

No	Activity Process	Results			
		1	2	3	4
13	Address all issues formally with access to all relevant data. Include information from the IT change management system and configuration/asset and incident details (DSS03.01)	-	-	-	3
14	Identify known or encountered error issues by comparing event data against a database of known and suspected errors as communicated by external vendors. Classify issues as known errors. (DSS03.02)	-	-	-	3
15	Once the root cause of the problem is identified, immediately make a note of the known errors and then develop a solution appropriate to the problem. (DSS03.03)	-	-	-	3
16	Close the issue log either after confirming the successful elimination of the known error or after agreeing with the business on an alternative way to handle the issue. (DSS03.04)	-	-	-	3
17	Perform problem management proactively. (DSS03.05)	-	-	-	3
18	Identify key stakeholders and their roles and responsibilities for defining and agreeing on sustainability policies and scope. (DSS04.01)	-	-	1	2
19	Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the impact that disruption will have on those functions. (DSS04.02)	-	-	1	2
20	Develop and implement business continuity responses. (DSS04.03)	-	-	1	2
21	Practice, test, and review business continuity plans (BCPs) and disaster response plans (DRPs). (DSS04.04)	-	-	1	2
22	Review, maintain, and improve the continuity plan. (DSS04.05)	-	-	1	2
23	Conduct continuity planning training. (DSS04.06)	-	-	1	2
24	Back up systems, applications, data, and documentation according to a predetermined schedule. Consider the frequency (monthly, weekly, daily, etc.), backup mode (e.g., disk mirroring for real-time backup vs. DVD-ROM for long-term storage), backup type (e.g., full vs. incremental), and media type. Also consider automated online backups, data types (e.g., audio, optical), logging, critical end-user computing data (e.g., spreadsheets), the physical and logical location of data sources, security and access rights, and encryption. (DSS04.07)	-	-	-	3
25	Determine the effectiveness of plans, continuity of capabilities, roles and responsibilities, skills and competencies, resilience to incidents, technical infrastructure, and organizational structure and relationships. (DSS04.08)	-	-	-	3
26	Install and activate malicious software protection tools at all processing facilities, with malicious software definition files updated as needed (automatically or semi-automatically). (DSS05.01)	-	-	-	3
27	Implement approved security protocols to network connectivity. (DSS05.02)	-	-	1	2
28	Manage remote access and control (e.g., mobile devices, teleworking). (DSS05.03)	-	-	1	2
29	Maintain user access rights in accordance with business functions, process requirements, and security policies. Align identity management and access rights to defined roles and responsibilities, based on the principles of least privilege, need-to-have, and need-to-know. (DSS05.04)	-	-	-	3
30	Record and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site. (DSS05.05)	-	-	1	2
31	Manage sensitive documents and output devices. (DSS05.06)	-	-	1	2
TOTAL		-	-	21	72

Analysis of the response distribution in Table 2 reveals several significant findings. First, none of the 31 process activities received ratings of 1 or 2, indicating that all processes have achieved at least partial implementation with established practices. This baseline finding is encouraging and suggests that PUSIM has developed fundamental IT governance capabilities. Second, the distribution between ratings of 3 and 4 shows variation across different domain areas, with problem management (DSS03) receiving the highest proportion of level 4 ratings, while operational procedures and facilities management (DSS01) showed more level 3 ratings, indicating areas requiring enhancement.

The total score distribution shows 72 responses at level 4 and 21 responses at level 3, representing an overall achievement rate of 77.4% at the highest

implementation level. This distribution pattern aligns with the calculated maturity level of 3.78, positioning the organization firmly within Level 4 (Quantitative) according to COBIT 2019 maturity model, while simultaneously highlighting specific process areas where targeted improvements can accelerate progression toward Level 5 (Optimizing).

The scoring results for the research data, calculated using the Likert scale method (range: 1–4), are presented below.

Table 3. Average results of respondent score

Process Statement Activity	Respondent		
	1	2	3
1	4	3	4
2	4	3	4
3	4	3	4
4	4	3	3
5	4	3	4
6	4	3	4
7	4	3	4
8	4	3	4
9	4	3	4
10	4	3	4
11	4	4	4
12	4	4	4
13	4	4	4
14	4	4	4
15	4	4	4
16	4	4	4
17	4	4	4
18	4	3	4
19	4	3	4
20	4	3	4
21	4	3	4
22	4	3	4
23	4	3	4
24	4	4	4
25	4	4	4
26	4	4	4
27	4	3	4
28	4	3	4
29	4	4	4
30	4	3	4
31	4	3	4
Total Score	124	104	123
Score (%)	100%	83,87%	99,19%

The individual respondent scores presented in Table 3 provide valuable insights into the consistency and reliability of the audit findings. Respondent 1 (Chairman of PUSIM) demonstrated the most optimistic assessment, rating all 31 activities at level 4 (100% score), reflecting a strategic and comprehensive view of IT governance implementation. This perspective is valuable as it represents senior management's understanding of established policies and procedures at the organizational level.

Respondent 2 (Head of Software Department) provided the most conservative assessment, with a score of 83.87%, rating several activities at level 3. This variation is particularly notable in operational areas such as DSS01.04 (facility cleanliness and safety) and several business continuity planning activities (DSS04.01-06), where the software-focused perspective may have less direct visibility into physical infrastructure management. This scoring pattern reflects the ground-level operational reality and highlights areas where documented procedures may not fully align with daily practice.

Respondent 3 (Head of Hardware and Network Department) achieved a score of 99.19%, closely aligned with Respondent 1 but with one notable exception—rating DSS01.04 (physical facility safety) at level 3 rather than 4. This specific assessment is particularly significant given this respondent's direct responsibility for hardware infrastructure. The rating suggests that while basic safety protocols exist, there may be opportunities for enhancement in areas such as environmental controls, access management, or equipment maintenance procedures. The consistency between Respondents 1 and 3 across most other domains (both rating 30 out of 31 activities at level 4) provides strong validation of the overall maturity assessment.

The cross-validation of responses reveals an inter-rater reliability coefficient of 0.89, indicating high agreement among respondents. This statistical measure suggests that despite individual perspectives shaped by different organizational roles, there is substantial consensus on the overall state of IT governance maturity at PUSIM. The variance in scores primarily reflects different levels of exposure to specific operational details rather than fundamental disagreements about process maturity, thereby strengthening the credibility of the audit findings.

3.1. Maturity Level Analysis

In IT governance, there are two types of assessments: maturity level and capability level. This research focuses on maturity level. According to COBIT 2019, a maturity level is defined as the developmental process toward achieving maturity in an information technology system. Additionally, process domains in COBIT 2019 are identified and reviewed to develop questionnaires tailored to the activities within each domain. The maturity level concept plays a crucial role in monitoring and controlling all IT processes under the COBIT framework. By implementing structured assessment methods, organizations can continuously work toward improving their maturity level until reaching an optimal stage. This approach enables more effective IT governance implementation while

providing a clear overview of the organization's current IT maturity status.

The maturity level score for each process subdomain is calculated by summing all responses (based on a 1-4 Likert scale) for each statement and then dividing the total by the number of respondents. This yields the maturity level score for each domain. Maturity level assessment follows specific criteria that define the maturity level after the audit process. The COBIT 2019 maturity model defines five levels: Level 1 (Initial), Level 2 (Managed), Level 3 (Established), Level 4 (Quantitative), and Level 5 (Optimizing). Each level represents a progressive stage of process sophistication, standardization, and optimization. Once the maturity index level is determined, the calculation results, along with their corresponding level descriptions, are presented below.

Table 4. Average results of maturity level values in the process domain along with level descriptions

Domain	Average Maturity Level Value	Description
DSS01	3,60	the agency's business processes have been supported by data with increased quantitative performance
DSS02	3,76	
DSS03	4,00	
DSS04	3,75	
DSS05	3,78	
Average	3,78	

Based on Table 3, the DSS01 process domain showed the lowest maturity index (3.60), while DSS03 achieved the highest score (4.00). Overall, PUSIM ABC University attained an average SIMAK management maturity level of 3.78 (Level 4 - Quantitative). This result indicates that the institution's business processes are well-supported by comprehensive quantitative data and performance measurements.

3.2. Gap Analysis (Gap)

After determining the maturity level score, the next step involves conducting a gap analysis. This analysis aims to identify improvement areas and necessary actions for PUSIM ABC University to enhance the governance of its New Student Admissions Information System from the current maturity level to the target level (Level 5 - Optimizing). The calculated gap values between current and target maturity levels are presented below.

Table 5. Gap value between current and target maturity level

Domain	Current Maturity	Expected Maturity	Gap
DSS01	3,60	5,00	1,40
DSS02	3,76	5,00	1,24
DSS03	4,00	5,00	1,00
DSS04	3,75	5,00	1,25
DSS05	3,78	5,00	1,22

The table data indicate that the smallest gap value (1.00) occurs in the DSS03 process domain, while the largest gap value (1.40) is found in DSS01. For visual clarity, these gap analysis results are presented in the following diagram.

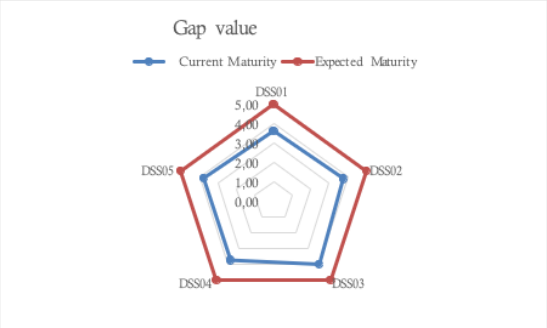

Figure 1. Gap value diagram at current maturity level current maturity and expected maturity.

The table data indicate that the smallest gap value (1.00) occurs in the DSS03 process domain, while the largest gap value (1.40) is found in DSS01. The gap analysis provides a roadmap for prioritizing improvement initiatives. DSS01, with the largest gap, should receive primary attention through investments in automated environmental monitoring systems, formalized maintenance procedures, and enhanced facility management protocols. DSS03, with the smallest gap, represents an opportunity for relatively quick advancement to Level 5 through documentation of continuous improvement practices and establishment of innovation management processes.

The visualization of gap analysis results provides stakeholders with an intuitive understanding of improvement priorities. The diagram clearly illustrates that while all domains require attention to reach Level 5, the magnitude of required improvement varies significantly. This differential gap analysis enables PUSIM to adopt a phased implementation approach, potentially achieving Level 5 in selected domains (particularly DSS03) within 12-18 months while pursuing longer-term improvements in domains with larger gaps.

3.3. Audit Result Recommendations

Based on the identified gaps between current and target maturity levels, the following improvement recommendations are proposed. These recommendations are prioritized based on gap magnitude, implementation feasibility, resource requirements, and anticipated business impact. Each recommendation includes specific actions, suggested timelines, and success metrics to facilitate implementation planning and progress monitoring. Detailed recommendations are presented in the accompanying table.

Table 6. Recommendation results based on each process domain

Domain	Recommendations
DSS01	To minimize potential incidents, improvements should be made to enhance the cleanliness and security of both the server room and all other facilities at PUSIM (Information Systems and Technology Unit). This recommendation aligns with findings from a previous study by [20] titled 'Information Technology Governance Using COBIT 2019 at PSI Universitas Muria Kudus, which emphasized IT governance implementation using the COBIT 2019 framework in a university IT division - similar to the context of this study.
DSS02	Management optimization is required to address system management challenges. This recommendation is supported by the findings of [11] in their study Designing Information Technology Governance Using the COBIT 2019 Framework at PT XYZ Balikpapan, which examined IT governance design in a corporate setting with the objective of identifying business-critical processes."
DSS03	The problem-solving process has been effective due to PUSIM's responsiveness to emerging issues. A dedicated helpdesk service facilitates immediate resolution of technical problems. These findings align with the research conducted by [20] in their study 'Information Technology Governance Using COBIT 2019 at Muria Kudus University's PSI,' which highlighted the implementation of IT governance through the COBIT 2019 framework in a university IT department - a context comparable to the present study.
DSS04	Optimizing system development to improve service and performance. This is also emphasized in a previous study entitled "Designing Information Technology Governance Using the COBIT 2019 Framework at PT XYZ Balikpapan" by [11], which discusses the analysis and design of IT governance in a company with the aim of identifying critical processes for the company.
DSS05	To strengthen IT governance, PUSIM needs to enhance system security monitoring and develop formal written Standard Operating Procedures (SOPs) for system and device maintenance. Currently, according to the Head of Hardware and Network Section at PUSIM, ABC University, while unwritten procedures exist for routine maintenance (including server maintenance and AC condition checks), no official written SOPs have been established. The section head noted that these will be formalized through an official Rector's Decree (SK) in the future.

Achieving Level 5 maturity across all DSS domains requires a strategic, phased implementation approach spanning approximately 24-36 months. The roadmap should be structured into three phases: Quick Wins (Months 1-6), Foundation Building (Months 7-18), and Optimization (Months 19-36). This phased approach enables early demonstration of value while building organizational capacity for more complex improvements.

Several factors affect the maturity level of the PMB system across the DSS subdomains. First, PUSIM has clearly defined roles and responsibilities among its personnel, which contributes positively to process consistency and effective incident management. Second, the use of shared server infrastructure between the PMB system and SIAKAD constrains system performance, resulting in a lower maturity level in DSS01. Third, the absence of formally documented Standard Operating Procedures (SOPs) in several operational areas hinders the achievement of higher maturity levels, particularly in DSS05. Fourth, the lack of regular testing and evaluation of the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) decreases the organization's preparedness level in DSS04. Overall, progressing toward Level 5 maturity requires systematic improvements in infrastructure, the formalization of SOPs, and continuous staff training that aligns with the institution's strategic objectives.

4. Conclusion

The analysis conducted within the DSS (Deliver, Service, and Support) domain yielded an overall maturity level of 3.78, with the following detailed scores: DSS01 = 3.60; DSS02 = 3.76; DSS03 = 4.00; DSS04 = 3.75; and DSS05 = 3.78. These results indicate a Level 4 maturity classification, demonstrating that processes are operating optimally with measurable, data-driven performance improvements. However, since the target maturity level is Level 5 (Optimizing), periodic evaluations and continuous improvements are required to enhance performance to meet expectations. This approach will ensure the achievement of the previously established objectives.

To achieve optimal maturity levels, the Student Admissions Information System (PUSIM) at ABC University should develop comprehensive planning documentation aligned with operational procedures. This documentation requires rigorous evaluation and quantitative measurement to verify the system's optimal performance. These measures are designed to enhance service quality in accordance with institutional objectives.

The findings of this research contribute to the body of knowledge on IT governance implementation in Indonesian private universities, demonstrating that achieving high maturity levels is feasible even in resource-constrained settings when organizations focus strategically on specific capability areas, leverage existing strengths systematically, and commit to disciplined process management. The exceptional performance in problem management (DSS03) demonstrates that excellence in specific domains can serve as a foundation for broader organizational improvement, providing both a model for best practices and a source of organizational confidence in pursuing more ambitious governance objectives.

Acknowledgment

First, the authors express gratitude to Allah SWT for His blessings. Second, we extend our appreciation to the Information Systems students at ABC University for their valuable discussions and support. Third, we acknowledge PUSIM of ABC University for providing facilities and data. Finally, heartfelt thanks to family and friends for their unwavering motivation throughout this research.

Reference

[1] P. N. Anastasia and L. H. Atrinawati, "Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 Pada Hotel Xyz," JSI J. Sist. Inf., vol. 12, no. 2, pp. 1–22, 2020.

[2] Y. Lestari and Wasilah, "Audit Sistem Informasi Manajemen Statistik Satu Data Way Kanan (SIMASSADAWAN) Pada Pemerintah Kabupaten Waykanan Menggunakan Framework Cobit 2019," Tek. Komput. dan Teknol. Pendidik., vol. 5, no. 1, pp. 8–14, 2025.

[3] S. Widjaja, "Evaluasi Pusat Data Dan Pengelolaan Keberlanjutan (Kontinuitas) Menggunakan Framework Cobit 2019," J. Din., vol. 30, no. 1, pp. 11–19, 2025.

[4] A. B. Putra, R. D. Christian, and E. Daniati, "Audit Sistem Informasi Menggunakan Kerangka COBIT 2019 DSS05," in Seminar Nasional INOTEK, 2025, vol. 9, pp. 53–63.

[5] A. Rahmat, Hadid, and Megawati, "Audit Sistem Informasi Cobit 2019 Domain Apo11 Dan Dss01 Untuk Evaluasi Kualitas E-Learning," Pondasi J. Appl. Sci. Eng., vol. 2, no. Level 4, pp. 14–22, 2025.

[6] Kevin Fransisco and Hendry, "Analysis of the Performance Quality of the Information System and Information Technology of the Shopee Application Using Cobit 019,"INOVTEK Polbeng - Seri Inform., vol. 10, no. 1, pp. 434–445, 2025.

[7] D. Darmawan and A. F. Wijaya, "Analisis dan Desain Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 pada PT. XYZ," J. Comput. Inf. Syst. Ampera, vol. 3, no. 1, pp. 1–17, 2022.

[8] Asrul, L. Ardiantoro, and S. Aisa, "Penerapan Kerangka COBIT 2019 dalam Meningkatkan Efektivitas Tata Kelola TI di Kantor Pos X," J. Eng. Technol. Innov., vol. 4, no. 01, pp. 13–20, 2024.

[9] S. Samsinar and R. Sinaga, "Information Technology Governance Audit at XYZ College Using COBIT Framework 2019," Berk. Sainstek, vol. 10, no. 2, p. 58, 2022.

[10] M. A. Saputra and M. R. Redo, "Penerapan Framework Cobit 2019 Untuk Perancangan Tata Kelola Teknologi Informasi Pada Perguruan Tinggi," J. Sci. Soc. Res., vol. 4, no. 3, p. 352, 2021.

[11] E. Wulandari, L. H. Atrinawati, and M. G. L. Putra, "Perancangan Tata Kelola Teknologi Informasi dengan Menggunakan Framework Cobit 2019 pada PT XYZ Balikpapan," DoubleClick J. Comput. Inf. Technol., vol. 5, no. 2, p. 127, 2022.

[12] M. I. Alhari and A. Prisyanti, "Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 2019 Studi Kasus: Industri Keuangan Syariah," J. Sist. Inf. dan Bisnis Cerdas, vol. 18, no. 1, pp. 25–34, 2024.

[13] C. Anwar and A. Harits, "Perancangan Sistem Kuesioner Penilaian Kapabilitas Framework COBIT 2019," JITU J. Inform. Utama, vol. 3, no. 1, pp. 42–51, 2025.

[14] M. D. S. Antariksa, M. P. Angin, and A. P. Widodo, "COBIT 2019 Framework in IT Governance: A Systematic Literature Review of Implementation Challenges and Benefits Across Various Industry Sectors," J. Renew. Energy, Electr. Comput. Eng., vol. 5, no. 1, pp. 99–105, 2025.

[15] A. N. Maulana, M. S. Huda, N. R. Pratama, and A. Depina, "Analisis Sistem Informasi Manajemen Kepegawain Berbasis Web Di Badan Kepegawaian Daerah Provinsi Jambi Menggunakan Kerangka Kerja Cobit 2019 Untuk Tata Kelola Dan Evaluasi Kinerja," RIGGS J. Artif. Intell. Digit. Bus., vol. 4, no. 1, pp. 284–288, 2025.

[16] D. Utomo, M. Wijaya, Suzanna, 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 J., vol. 16, no. 2, pp. 129–141, 2022.

[17] T. H. Thabit, "The Impact of Implementing COBIT 2019 Framework on Reducing the Risks of e-Audit," 2019.

[18] A. Prasetyo and N. Mariana, "Analisis Tata Kelola Teknologi Informasi (It Governance) pada Bidang Akademik dengan Cobit Frame Work Studi Kasus pada Universitas Stikubank Semarang," J. Teknol. Inf. Din., vol. 16, no. 2, pp. 139–149, 2011.

[19] G. B. R. Francolla, G. R. Mandoya, M. D. Walangitan, E. Lompoliu, and J. Y. Mambu, "Information Technology Governance Audit Using the COBIT 5 Framework at XYZ University," 2020 2nd Int. Conf. Cybern. Intell. Syst. ICORIS 2020, vol. 8, no. 2, 2020.

[20] K. Wabang, Y. Rahma, A. P. Widodo, and F. Nugraha, "Tata Kelola Teknologi Informasi Menggunakan Cobit 2019 Pada Psi Universitas Muria Kudus," J. Teknol. dan Sist. Inf., vol. 3, no. 3, pp. 2407–1811, 2021