Journal of Information Systems and Informatics
Vol. 7, No. 1, March 2025 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v7i1.972 Published By DRPM-UBD

COBIT 2019 for Enhanced ICT Governance: A Case Study at a Higher Education Institution

Baiq Yulia Fitriyani[1], Alva Hendi Muhammad[2]

[1,2] Masters in Informatics Engineering, AMIKOM University Yogyakarta, Indonesia
Email: [1]baiqyuliafitriyani@students.amikom.ac.id, [2]alva@amikom.ac.id

Abstract

Effective ICT governance is essential for aligning technological resources with institutional objectives, especially in higher education institutions with limited resources. This study evaluates the ICT governance framework at PUSTIK STMIK Lombok using COBIT 2019, focusing on six domains: APO04, APO10, BAI02, DSS01, DSS05, and EDM01. A structured survey was conducted with 189 respondents, including faculty, students, and administrative staff, to assess capability maturity levels and identify governance gaps. The results indicate that all domains achieved Level 3 (Established), reflecting standardized processes but highlighting deficiencies in security resilience, vendor management, and operational change management. A SWOT analysis identified weaknesses such as limited proactive security measures, insufficient stakeholder engagement, and inadequate staff training, while opportunities include government funding and emerging technologies. To address these challenges, a tailored governance framework was developed, incorporating policies, standards, and procedures to enhance security, innovation management, and vendor accountability. The findings underscore the applicability of COBIT 2019 in resource-constrained educational settings and provide practical recommendations to bridge governance gaps. Future research should examine the long-term effects of governance improvements and explore the framework's scalability across similar institutions.

Keywords: ICT Governance, COBIT 2019, Higher Education, Capability Maturity, SWOT Analysis.

1. INTRODUCTION.

In today's digital era, Information and Communication Technology (ICT) plays a crucial role in supporting the strategic objectives of organizations across various sectors. Beyond its traditional function as a support tool, ICT now drives innovation, efficiency, and organizational competitiveness. Effective ICT governance ensures that technology investments align with institutional strategies, enhancing operational performance and ensuring long-term sustainability [1], [2]. PUSTIK STMIK Lombok is responsible for managing ICT infrastructure, ensuring information security, overseeing technology procurement, and maintaining integrated information systems. However, it faces several major challenges, including cybersecurity vulnerabilities, inefficient resource management, and lack of system integration. Additionally, dependency on a single

internet service provider without a backup, budget constraints for implementing advanced security measures, and suboptimal planning in hardware and software procurement hinder the improvement of ICT services in the academic environment [3], [4], [5].

Addressing these challenges necessitates a structured approach to ICT governance. Among the available frameworks, the Control Objectives for Information and Related Technology (COBIT) 2019 framework is particularly well-suited for this purpose. COBIT 2019 offers a comprehensive methodology for ICT governance, integrating principles of strategic alignment, resource optimization, risk management, and performance measurement. The framework has been widely acknowledged for its ability to enhance ICT governance capabilities and align ICT processes with organizational objectives [6], [7]. Recent research underscores the effectiveness of COBIT 2019 in bridging capability gaps and improving ICT governance outcomes across diverse organizational contexts, including educational institutions, public agencies, and private enterprises [8], [9].

The current study seeks to design an ICT governance model for PUSTIK STMIK Lombok using the COBIT 2019 framework. This approach is grounded in a SWOT analysis to identify internal and external factors influencing ICT management. By mapping these factors against COBIT 2019 domains, the study aims to provide actionable recommendations to address existing gaps and optimize ICT service delivery. Previous studies have demonstrated the utility of COBIT 2019 in various domains, such as risk management, security enhancement, and operational continuity [10], [11], [12]. However, there remains a need for tailored frameworks that address the unique challenges faced by educational institutions, particularly in regions with limited ICT resources.

A notable example is the work by [8] who applied the COBIT 2019 framework to evaluate ICT governance at a government office in Pesawaran Regency. Their study highlighted capability gaps in domains such as APO11 (Managed Quality) and DSS02 (Managed Service Levels), demonstrating the value of targeted recommendations to enhance governance outcomes. Similarly, research by [9] identified critical governance processes in a private company, emphasizing the role of alignment goals in achieving strategic objectives. Both studies underscore the flexibility and adaptability of COBIT 2019 in addressing context-specific governance challenges. At PUSTIK STMIK Lombok, the adoption of COBIT 2019 is anticipated to yield significant improvements in ICT governance capabilities. The framework's focus on aligning ICT processes with organizational goals aligns well with the institution's strategic priorities. Additionally, COBIT 2019's capability assessment model provides a robust mechanism for evaluating current performance levels and identifying areas for improvement. By leveraging

the framework's structured approach, this study aims to enhance the reliability, efficiency, and security of ICT services at PUSTIK.

The relevance of ICT governance frameworks extends beyond the immediate challenges faced by PUSTIK STMIK Lombok. In their work, [10] demonstrated the utility of COBIT 2019 in evaluating risk and security management processes at a research institution. Their findings revealed significant capability gaps, with key domains such as APO12 (Managed Risk) and APO13 (Managed Security) achieving suboptimal levels. These results underscore the importance of continuous improvement and iterative evaluation in ICT governance, principles that are central to the COBIT 2019 methodology [12], [13]. Furthermore, Wulandari et al., (2024) explored the application of COBIT 2019 at a regional telecommunications company, identifying 14 critical processes that required immediate attention. Their study provided actionable recommendations to enhance governance capabilities, illustrating the framework's potential to drive organizational change. This aligns with findings by Senggik et al., (2022) who applied COBIT 2019 to assess ICT governance at a regional government office. Their work highlighted the importance of aligning governance objectives with broader institutional goals, a principle that is equally relevant for PUSTIK STMIK Lombok [8], [14]

In the context of higher education, the importance of ICT governance cannot be overstated. Universities and colleges increasingly rely on ICT to support academic, administrative, and research functions. Effective governance frameworks ensure that these systems operate efficiently, securely, and in alignment with institutional objectives. Research by [9] demonstrated the value of COBIT 2019 in enhancing ICT governance at a private university in Indonesia. Their findings emphasized the role of structured governance processes in addressing resource constraints and improving service delivery. Similar insights were provided by [8] who applied COBIT 2019 to evaluate ICT innovation and change management processes at a private enterprise. Their work highlighted the critical role of governance in fostering organizational agility and resilience. This study builds on the rich body of literature surrounding ICT governance and the COBIT 2019 framework. By focusing on PUSTIK STMIK Lombok, it seeks to address a critical gap in the existing research, namely the application of COBIT 2019 in educational settings with limited resources. The findings are expected to contribute valuable insights into the practical implementation of ICT governance frameworks, providing a model that can be adapted to similar institutions.

2. METHODS

This study follows a structured research methodology to evaluate the ICT governance maturity level at PUSTIK STMIK Lombok using the COBIT 2019

framework. Figure 1 illustrates the overall research process, ensuring a systematic approach to data collection and analysis.

2.1. Research Design

The research began with the identification of ICT governance issues at PUSTIK STMIK Lombok and proceeded with a SWOT analysis to determine strengths, weaknesses, opportunities, and threats in ICT management [15]. Subsequently, the COBIT 2019 framework was applied to evaluate the governance capabilities and develop actionable recommendations [8].

2.2. Research Stages

The research was conducted in several key stages:

1. Problem Identification The initial stage involved identifying issues in ICT governance at PUSTIK STMIK Lombok. This was achieved through preliminary interviews and observations of existing ICT processes [16].
2. SWOT Analysis A SWOT analysis was conducted to examine the internal and external factors influencing ICT governance. This analysis informed the selection of relevant COBIT 2019 domains for evaluation [10].
3. Data Collection Data collection was carried out using a structured survey instrument comprising 248 Likert-scale questions. These questions were distributed across six COBIT 2019 domains: APO04 (Managed Innovation), DSS01 (Managed Operations), DSS05 (Managed Security Services), BAI02 (Managed Requirements Definition), EDM01 (Ensured Governance Framework Setting and Maintenance), and APO10 (Managed Vendor Relationships) [11].
4. Data Analysis The collected data were analyzed using descriptive and inferential statistical methods. Gap analysis was performed to compare the current capability levels (as-is) with the desired levels (to-be) for each domain. This stage provided insights into areas requiring improvement and priority [9].
5. Recommendation Formulation Based on the analysis results, tailored recommendations were developed to enhance ICT governance capabilities at PUSTIK STMIK Lombok. These recommendations were guided by the COBIT 2019 framework and SWOT analysis outcomes [17].

2.3. Survey Instrument and Respondents.

The survey instrument utilized a five-point Likert scale designed to measure respondents' perceptions of ICT governance capabilities. The study involved 189 respondents, comprising 20 faculty members, 159 students, 9 administrative staff, and 1 head of PUSTIK. The respondents were purposively selected based on their

involvement in ICT services and management to ensure comprehensive data collection [18], [6],[19].

2.4. Visual Representation

Figure 1, presented as part of this study, illustrates the detailed research methodology, highlighting the sequence from problem identification to validation of findings. This visual representation provides a logical flow of the research process and demonstrates the interconnections between stages [20], [21].

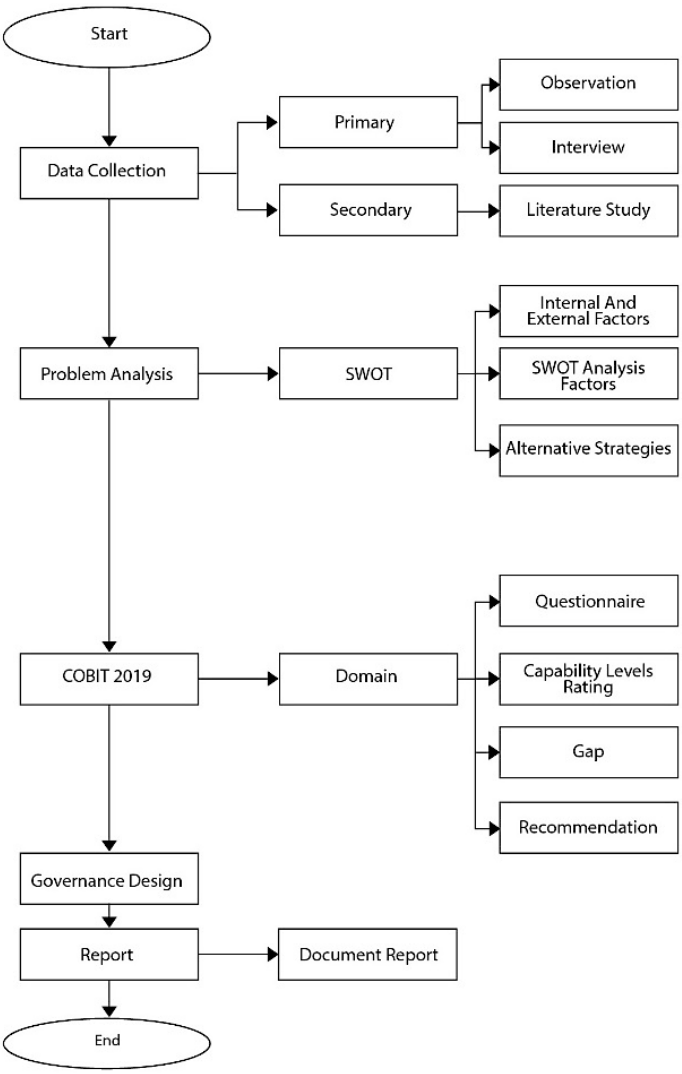

Figure 1. Research Methodology

The revised methodology ensures clarity in the research stages, justifies the selection of frameworks, and provides a structured approach to data collection and analysis. The integration of COBIT 2019 and SWOT analysis enhances the reliability of the findings and the applicability of the governance model in similar institutions.

3. RESULTS AND DISCUSSION

3.1. Overview of Respondents and Data Validation

The study involved a total of 189 respondents, categorized into four stakeholder groups: 20 faculty members, 159 students, 9 administrative staff, and 1 Head of PUSTIK. This comprehensive sampling strategy ensures that the diverse perspectives of all key stakeholders interacting with ICT services at PUSTIK STMIK Lombok are represented. The survey instrument was validated using Cronbach's alpha, which achieved a reliability score above 0.7 for all domains. This confirms that the survey responses were consistent and reliable [5], [20]. The reliability of the instrument strengthens the credibility of the findings and provides a robust basis for subsequent analysis.

3.2. Capability Levels of ICT Governance

Capability levels across six COBIT 2019 domains were assessed to determine the current state of ICT governance. The results, summarized in Table 1, highlight the average scores and corresponding capability levels for each domain. All domains achieved a Level 3 (Established), indicating that processes are standardized and performed consistently across the institution.

Table 1. Capability Levels

Domain	Average Score	Capability Level	Description
APO04	3.87	Level 3	Established
APO10	3.48	Level 3	Established
BAI02	3.31	Level 3	Established
DSS01	3.35	Level 3	Established
DSS05	3.34	Level 3	Established
EDM01	3.43	Level 3	Established

Domains APO04 (Managed Innovation) and APO10 (Managed Vendor Relationships) scored highest, reflecting strong adherence to standardized processes. However, lower scores within certain subdomains indicate room for improvement, particularly in DSS05 (Managed Security Services), which scored an average of 3.34, and DSS01 (Managed Operations) at 3.35. These gaps highlight the need for targeted interventions to strengthen ICT governance capabilities [16]

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

3.3. Gap Analysis

The gap analysis revealed that while processes in all domains are standardized and consistently performed (Level 3), they have not yet reached higher levels such as "Predictable" (Level 4) or "Optimized" (Level 5). For instance, DSS05 requires more robust security measures and proactive monitoring to advance to a predictable capability level. Similarly, DSS01 needs structured mechanisms for managing operational changes and incident escalation to improve service reliability.

3.4. Subdomain-Specific Observations

Figure 2 illustrating average scores for each subdomain provides a clear visualization of strengths and weaknesses within each domain.

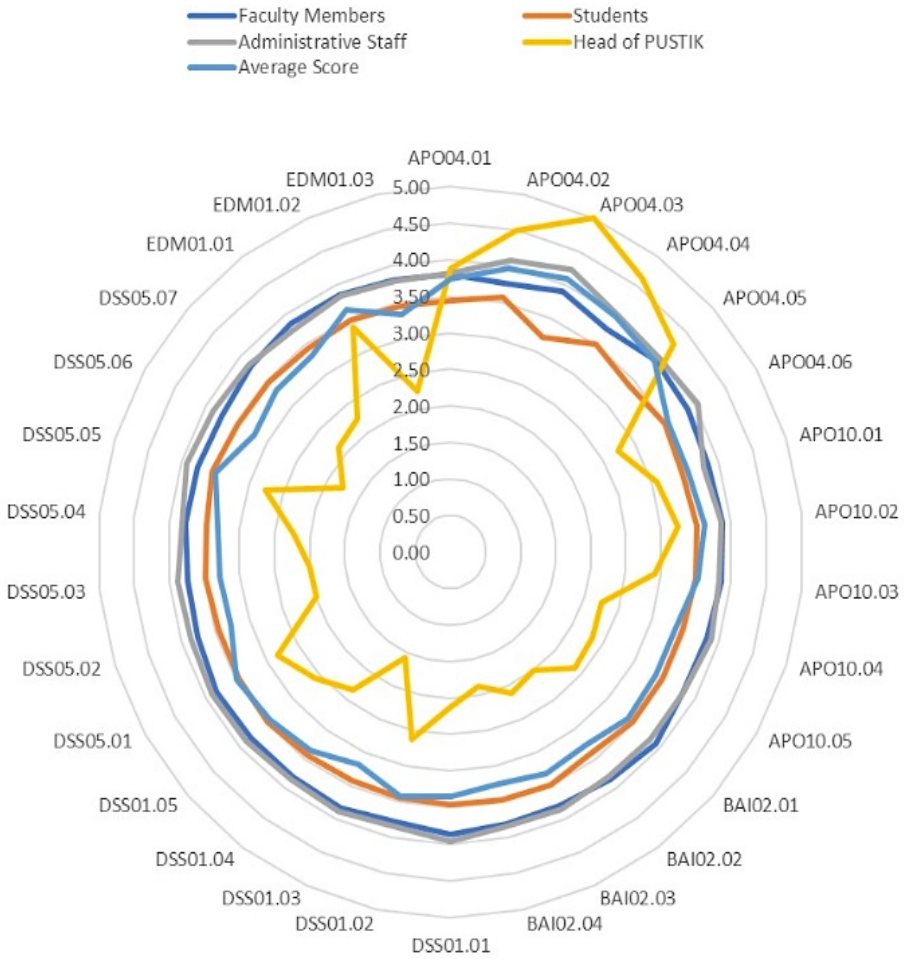

Figure 2. Capability Levels

Detailed analysis of subdomains within each domain provided deeper insights:

1. APO04 - Managed Innovation Subdomains APO04.01 to APO04.06 reflect a strong focus on fostering innovation. The highest score (4.08) was observed in APO04.03, which involves aligning innovation practices with institutional objectives. However, APO04.06, which addresses the formalization of innovation processes, scored lower (3.55), indicating the need for better documentation and monitoring of innovative practices [22].
2. DSS01 - Managed Operations DSS01 subdomains demonstrated variability, with DSS01.04 (Manage Service Desk and Incidents) scoring the highest at 3.58. This suggests that service desk operations are well-managed and responsive. However, DSS01.02 (Manage Operational Change) scored lower (3.27), reflecting challenges in effectively managing and communicating operational changes to stakeholders [9].
3. DSS05 - Managed Security Services DSS05 scored an average of 3.34 across its subdomains, with DSS05.06 (Monitor and Evaluate Security Performance) being the lowest at 3.21. This indicates gaps in proactive security monitoring and evaluation, underscoring the need for advanced security tools and regular staff training [16].

3.5. Design of Governance Framework

The design of the governance framework at PUSTIK STMIK Lombok focuses on addressing identified gaps in ICT management and aligning the institution's processes with COBIT 2019 standards. This framework is built on three interconnected components: policies, standards, and procedures, which collectively provide a structured approach to ICT governance and operational improvement.

Policies are the cornerstone of the governance framework, offering high-level principles and guidelines that shape decision-making processes and align operational practices with organizational objectives. The Information Security Policy, for instance, establishes comprehensive guidelines for data protection, access control, and incident response mechanisms. This policy ensures that sensitive information is safeguarded against unauthorized access while fostering a culture of accountability and compliance. Similarly, the Operational Change Policy outlines the procedures for managing changes within the ICT infrastructure, minimizing disruptions, and maintaining service continuity. The Vendor Management Policy complements these efforts by defining the roles and responsibilities of external vendors, setting performance expectations, and ensuring accountability in service delivery.

Standards within the governance framework serve as benchmarks for ensuring consistency and compliance across all ICT processes. Service Level Standards are

established to define measurable metrics for evaluating the quality and efficiency of ICT operations. These standards ensure that service delivery aligns with user expectations and institutional goals. Incident Management Standards provide a structured approach to handling and escalating service issues, thereby reducing resolution times and enhancing user satisfaction. Infrastructure Security Standards, on the other hand, outline minimum security requirements for ICT assets, ensuring that the institution's technological infrastructure is resilient against emerging threats.

Procedures operationalize the policies and standards, providing detailed, step-by-step instructions for implementation. The Change Management Procedure, for example, describes the processes for submitting, reviewing, and approving changes to ICT systems. This procedure ensures that all changes are thoroughly evaluated for their potential impact before implementation. The Incident Reporting and Resolution Procedure establishes a clear workflow for identifying, reporting, and resolving ICT issues, enhancing the institution's responsiveness to operational challenges. Furthermore, the Security Audit Procedure provides a systematic approach to evaluating system vulnerabilities and ensuring compliance with security policies. These procedures are designed to facilitate seamless coordination among stakeholders while fostering a proactive approach to ICT governance.

The integration of these components within the governance framework ensures that ICT processes are not only standardized but also adaptable to the dynamic needs of the institution. By formalizing policies, setting clear standards, and detailing actionable procedures, the framework provides a robust foundation for enhancing service delivery, improving operational efficiency, and mitigating risks. This structured approach aligns with the best practices outlined in the COBIT 2019 framework, reinforcing the institution's commitment to achieving higher levels of capability and maturity in ICT governance. Future evaluations will focus on assessing the implementation effectiveness of these components and identifying opportunities for continuous improvement.

Table 2. Governance Framework

Domain	Maturity Level	Governance Design Elements	Gap	Focus Area for Improvement	Objective
APO04	Level 3 (Established)	Innovation policy, standardized documentation	1.13	Formalization and regular evaluation of innovation processes	Strengthen innovation alignment with institutional objectives
APO10	Level 3 (Established)	Vendor management policy	1.02	Performance assessment	Ensure accountability and

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Domain	Maturity Level	Governance Design Elements	Gap	Focus Area for Improvement	Objective
				and SLA enforcement	enhance vendor service quality
BAI02	Level 3 (Established)	Needs analysis standards	1.18	Broaden stakeholder involvement	Improve accuracy and comprehensiveness of system requirements
DSS01	Level 3 (Established)	Service standards, help desk procedures	1.15	Structured escalation and prioritization processes	Enhance service reliability and responsiveness
DSS05	Level 3 (Established)	Information security policy, audit procedures	1.16	Advanced security tools and staff training	Strengthen resilience against cybersecurity threats
EDM01	Level 3 (Established)	Governance policy	1.07	Periodic policy reviews	Maintain compliance with evolving regulatory standards

3.6. SWOT Analysis of ICT Governance

The SWOT analysis of ICT governance at PUSTIK STMIK Lombok provides a structured understanding of the institution's internal strengths and weaknesses, as well as external opportunities and threats. The findings are summarized in the following matrix, which forms the basis for targeted recommendations to enhance governance capabilities.

Table 3. SWOT Matrix

Strengths (S)	Weaknesses (W)
Standardized ICT processes across key domains	Limited proactive security measures
Dedicated ICT team with institutional support	Operational changes lack structured communication
Established service desk operations	Limited engagement with stakeholders for validation
Alignment with COBIT 2019 best practices	Insufficient training for ICT staff on new tools
Opportunities (O)	**Threats (T)**
Government funding for ICT infrastructure upgrades	Increasing cybersecurity risks
Emerging technologies to improve efficiency	Budgetary constraints for advanced tools

Collaborative opportunities with external vendors	Rapid changes in regulatory requirements
Support for digital transformation in education	High dependency on a single internet provider

Based on Table 3 can be explained as follow.

1. Strengths PUSTIK STMIK Lombok benefits from having standardized ICT processes in place, aligned with COBIT 2019 best practices. This provides a solid foundation for further improvement. Additionally, the institution's dedicated ICT team and robust service desk operations ensure reliable support for end users. The alignment with best practices facilitates the implementation of structured governance improvements.
2. Weaknesses Despite the strengths, the institution faces challenges such as limited proactive security measures and insufficient stakeholder engagement during system requirement validations. Communication regarding operational changes is also lacking, leading to potential disruptions. The lack of structured training programs for ICT staff further limits their ability to adopt and leverage new tools effectively.
3. Opportunities External opportunities include access to government funding for ICT upgrades and the availability of emerging technologies that can enhance operational efficiency. Collaborative opportunities with vendors also present avenues for innovation and cost-sharing in infrastructure development. Additionally, the emphasis on digital transformation in education provides a supportive environment for advancing ICT governance.
4. Threats The primary threats include escalating cybersecurity risks, which require robust defenses and constant monitoring. Budgetary constraints pose challenges for acquiring advanced tools and maintaining existing systems. Furthermore, rapid regulatory changes demand agility in governance processes, while high dependency on a single internet provider risks service interruptions.

3.7. Comparison with Previous Studies

To contextualize these findings, this study compared the results with previous research on ICT governance maturity in higher education institutions. Research by Wulandari et al. (2023), on a regional telecommunications company found that most domains were at Level 2 (Managed) [23], demonstrating a less structured governance framework. Similarly, Mambu et al. (2022), in their study on a private university, reported that key domains such as APO04 (Managed Innovation) and APO10 (Managed Vendor Relationships) were below Level 3 [24], indicating gaps in strategic alignment and vendor management. In contrast, a study by Sipayung & Yunis (2022) at a research institution found that governance domains related to risk management and security (APO12 and APO13) remained at Level 2 [25], underscoring persistent challenges in cybersecurity governance. The results from PUSTIK STMIK Lombok suggest that despite limited resources, structured

processes have been implemented more effectively compared to some other institutions, highlighting the relevance of COBIT 2019 as a governance model in educational settings with constrained budgets.

3.8. Effectiveness and Contextual Relevance of the Proposed Framework

The findings indicate that adapting COBIT 2019 in an institution with limited ICT resources can still yield substantial governance improvements. By reaching Level 3, PUSTIK STMIK Lombok has demonstrated that standardized and repeatable ICT processes can be achieved even in resource-constrained environments. This aligns with previous findings by [24], who emphasized the importance of structured governance approaches in enhancing ICT service efficiency.

3.9. Recommendations for ICT Governance Improvement

The table below summarizes targeted recommendations for improving ICT governance at PUSTIK STMIK Lombok, structured by COBIT 2019 domains. These recommendations are based on capability maturity levels, SWOT analysis, and governance design considerations.

Table 4. Recommendations

Domain	Focus Area for Improvement	Recommendation	Expected Outcome
APO04	Formalization and evaluation of innovation processes	Develop a standardized innovation framework with periodic monitoring and assessment	Improved alignment of innovation with strategic goals and better adaptability
APO10	Vendor assessment and SLA management	Establish a structured vendor performance review system tied to SLA compliance	Enhanced vendor accountability and consistent service quality
BAI02	Broaden stakeholder involvement	Conduct inclusive workshops with key stakeholders for requirement analysis	Increased accuracy and relevance of system requirements
DSS01	Structured escalation and prioritization	Implement a clear escalation mechanism for help desk issues with defined priority levels	Faster issue resolution and enhanced user satisfaction
DSS05	Security tools and staff training	Invest in advanced security tools and provide regular cybersecurity training for ICT staff	Improved cybersecurity resilience and proactive threat mitigation

Domain	Focus Area for Improvement	Recommendation	Expected Outcome
EDM01	Policy review and regulatory alignment	Schedule periodic reviews of governance policies to ensure compliance with evolving regulations	Sustained regulatory compliance and readiness for policy changes

Explanation of Recommendations :

1. Innovation Management (APO04), Introducing a formal framework ensures that innovation efforts are consistently aligned with institutional goals. Monitoring and evaluation activities enable adaptability to emerging opportunities.
2. Vendor Performance (APO10), A structured review system allows the institution to identify underperforming vendors and ensure service levels are maintained, addressing risks associated with vendor dependency.
3. Requirements Analysis (BAI02), Involving stakeholders in workshops ensures that all perspectives are considered, leading to more comprehensive and actionable system requirements.
4. Help Desk Optimization (DSS01), Escalation mechanisms improve responsiveness by addressing high-priority issues promptly, leveraging established help desk operations.
5. Cybersecurity Enhancement (DSS05), Advanced tools and training create a proactive security environment capable of mitigating increasing cyber risks.
6. Policy Adaptability (EDM01), Regular policy reviews keep the institution agile in the face of regulatory changes, ensuring governance practices remain effective and compliant.

3.10. Discussion

The findings of this study highlight the current state of ICT governance at PUSTIK STMIK Lombok, revealing both strengths and areas for improvement. The institution has achieved a standardized and repeatable process maturity level (Level 3 – Established) across all six COBIT 2019 domains, indicating that governance structures are in place and consistently followed. However, the results also suggest that moving to a higher maturity level will require strategic interventions in key areas such as security management, operational governance, and stakeholder engagement.

One of the key takeaways from the study is the strong performance in innovation management and vendor relationships. The institution has demonstrated a structured approach to fostering innovation and maintaining vendor partnerships, which aligns with best practices in ICT governance. However, the governance framework still lacks formal mechanisms for evaluating and refining innovation processes. Without structured monitoring, the institution risks inefficiencies in

leveraging technological advancements for long-term growth. Similarly, vendor management practices, while relatively strong, require a more systematic performance assessment process to ensure service quality and compliance with contractual agreements.

A notable challenge identified in the study is the limited capability in security governance. While security processes are standardized, they are not yet predictive or optimized, leaving room for potential vulnerabilities. The absence of proactive monitoring mechanisms and structured cybersecurity training for ICT staff poses a risk to the institution's ability to defend against evolving threats. To address this, a more comprehensive security strategy, including real-time monitoring, threat intelligence, and periodic security audits, should be implemented. Furthermore, integrating advanced security tools and enhancing incident response protocols can significantly improve the institution's resilience against cyber threats.

Operational governance also presents challenges, particularly in change management and incident resolution. Although the service desk functions effectively, the institution lacks a well-structured escalation mechanism for operational changes. This gap can lead to delays in issue resolution and miscommunication among stakeholders. Implementing a more structured operational change framework with clear communication channels will enhance efficiency and minimize service disruptions. Additionally, training programs focusing on operational best practices can equip ICT staff with the necessary skills to handle complex system changes effectively.

The governance framework proposed in this study serves as a strategic roadmap for addressing these gaps. By formalizing policies, setting clear standards, and developing detailed procedures, the institution can enhance its governance structure. The introduction of a structured vendor management policy, operational change policy, and security policy is crucial in aligning ICT governance with institutional objectives. Moreover, defining measurable service level standards and implementing an incident management framework will improve responsiveness and user satisfaction. These improvements will not only strengthen governance but also ensure that ICT services remain adaptable to the institution's evolving needs.

A SWOT analysis further contextualizes these findings, emphasizing that while the institution benefits from structured governance practices, weaknesses such as insufficient stakeholder engagement and a lack of structured cybersecurity measures must be addressed. The availability of government funding and emerging technologies presents opportunities for strengthening governance. However, increasing cybersecurity threats and budgetary constraints pose risks that require

proactive mitigation strategies. Aligning ICT governance improvements with these external factors will be essential for long-term sustainability.

When compared with previous studies, this research underscores that despite resource limitations, structured governance models like COBIT 2019 can drive meaningful improvements in higher education institutions. While many institutions struggle to reach Level 3 maturity, PUSTIK STMIK Lombok has demonstrated that a commitment to governance best practices can lead to a more stable and efficient ICT management system. However, achieving higher maturity levels will require continued investment in process automation, strategic decision-making, and performance monitoring.

Based on these findings, several targeted recommendations are proposed. Strengthening innovation management through structured evaluation, improving vendor accountability with formal performance assessments, and enhancing cybersecurity resilience through advanced monitoring and staff training are key priorities. Additionally, broadening stakeholder engagement and refining operational governance through structured escalation processes will further optimize ICT service delivery. Regular policy reviews will also ensure that governance frameworks remain aligned with evolving regulatory standards.

In conclusion, while PUSTIK STMIK Lombok has successfully implemented structured ICT governance practices, there is still significant potential for enhancement. Moving towards a more predictive and optimized governance model will require a combination of strategic policy implementation, continuous training, and investment in advanced security and operational tools. Future studies should focus on longitudinal assessments to measure the effectiveness of these improvements over time, ensuring that governance remains agile and responsive to institutional needs.

4. CONCLUSION

This study evaluated the ICT governance framework at PUSTIK STMIK Lombok using the COBIT 2019 methodology, focusing on six key domains: APO04 (Managed Innovation), APO10 (Managed Vendor Relationships), BAI02 (Managed Requirements Definition), DSS01 (Managed Operations), DSS05 (Managed Security Services), and EDM01 (Ensured Governance Framework Setting and Maintenance). The findings revealed that all domains achieved a maturity level of Level 3 (Established), indicating that standardized processes are in place but require further development to reach higher levels of maturity. The gap analysis identified security resilience, vendor management, and operational change management as key areas requiring improvement. The SWOT analysis further highlighted weaknesses such as limited stakeholder engagement,

insufficient training for ICT staff, and reliance on a single internet provider, while opportunities such as government funding and emerging technologies provide potential avenues for enhancement. Based on these findings, a governance framework was proposed, integrating policies, standards, and procedures to address identified gaps and optimize ICT governance practices. This study contributes to the growing body of knowledge on ICT governance by demonstrating the applicability of COBIT 2019 in a resource-constrained educational institution. The research provides practical recommendations for bridging governance capability gaps, emphasizing the importance of structured governance frameworks in improving ICT service reliability and security. For future research, it is recommended to assess the long-term impact of implementing the proposed framework and explore its scalability in similar institutions. Additionally, further studies could adopt longitudinal approaches or comparative analyses across multiple institutions to evaluate the effectiveness of different governance strategies. Expanding research to include other ICT governance models alongside COBIT 2019 may also offer valuable insights into optimizing governance frameworks for higher education institutions. The findings of this study underscore the necessity for continuous improvement and adaptive governance to align ICT processes with strategic objectives. By leveraging the structured approach of COBIT 2019, educational institutions can enhance their efficiency, security, and overall ICT governance maturity.

REFERENCES

[1] E. B. Naibaho and A. D. Cahyono, "Information technology governance analysis using COBIT 2019 framework in Salatiga City Community and Civil Services," *J. Inf. Syst. Inform.*, vol. 6, no. 2, pp. 865–881, Jun. 2024, doi: 10.51519/journalisi.v6i2.734.

[2] A. Yusuf, W. A. Saputra, and J. Jamilah, "Capability gap analysis in IT governance for a logistics company using COBIT 2019," *J. Inf. Syst. Inform.*, vol. 6, no. 3, pp. 1804–1821, Sep. 2024, doi: 10.51519/journalisi.v6i3.832.

[3] K. Kevin and J. Setiawan, "IT proficiency in a media and publishing company using the COBIT 2019 framework," *J. Inf. Syst. Inform.*, vol. 6, no. 3, pp. 1435–1449, Sep. 2024, doi: 10.51519/journalisi.v6i3.794.

[4] K. Leonardo and R. Latuperissa, "Information technology governance design in trading companies using the COBIT 2019 framework," *J. Inf. Syst. Inform.*, vol. 6, no. 3, pp. 1466–1483, Sep. 2024, doi: 10.51519/journalisi.v6i3.798.

[5] M. W. Loppies and C. Fibriani, "Designing information technology governance in trading companies using COBIT 2019 framework," *J. Inf. Syst. Inform.*, vol. 5, no. 4, pp. 1581–1594, Dec. 2023, doi: 10.51519/journalisi.v5i4.602.

[6] M. I. Fianty and M. Brian, "Leveraging COBIT 2019 framework to implement IT governance in business process outsourcing company," *J. Inf. Syst. Inform.*, vol. 5, no. 2, pp. 568–579, May 2023, doi: 10.51519/journalisi.v5i2.492.

[7] G. M. W. Tangka and E. Lompoliu, "Information technology governance using the COBIT 2019 framework in Manado Post Companies," *J. Inf. Teknol.*, pp. 53–62, 2024.

[8] I. F. Wulandari et al., "The performance analysis of SIKITO LLDIKTI Region II system using COBIT 2019 framework: A case study," *Int. J. Artif. Intell. Res.*, vol. 7, no. 2, pp. 111–121, 2024.

[9] J. Y. Mambu, T. Wulyatiningsih, and S. Adam, "Applying COBIT 2019 to design a tailored IT governance system for PT. Telekomunikasi Seluler Manado Branch," *J. Inf. Teknol.*, pp. 229–237, 2024.

[10] A. Rusman, R. Nadlifatin, and A. P. Subriadi, "Information system audit using COBIT and ITIL framework: literature review," *Sinkron J. Penelit. Tek. Inform.*, vol. 6, no. 3, pp. 799–810, 2022.

[11] A. B. Sipayung and R. Yunis, "Evaluation of information technology governance at Mikroskil University using COBIT 2019 framework with BAI11 domain," *Int. J. Res. Appl. Technol. (INJURATECH)*, vol. 2, no. 2, pp. 128–143, 2022.

[12] E. M. Lompoliu et al., "Information technology governance analysis using the COBIT 2019 framework at XYZ institution," *Cogito Smart J.*, vol. 8, no. 2, pp. 346–358, 2022.

[13] A. R. Sengik et al., "Using design science research to propose an IT governance model for higher education institutions," *Educ. Inf. Technol.*, vol. 27, no. 8, pp. 11285–11305, 2022.

[14] A. Nugroho and H. Ginardi, "Information technology governance analysis to reduce information security risks using COBIT 2019: A case study of manufacturing companies," *J. Indones. Sos. Teknol.*, vol. 5, no. 8, pp. 3721–3733, 2024.

[15] F. Ajismanto and S. Surahmat, "Information technology governance analysis of STMIK Palcomtech in the new normal era using COBIT 2019 method," *J. Comput. Netw. Archit. High Perform. Comput.*, vol. 3, no. 2, pp. 263–272, 2021.

[16] K. Imtihan, "The impact of visual quality and user interface responsiveness on student satisfaction in academic information systems (AIS)," *Pak. J. Life Soc. Sci. (PJLSS)*, vol. 22, no. 2, 2024, doi: 10.57239/PJLSS-2024-22.2.001455.

[17] E. Amore et al., "Leverage the COBIT 2019 design toolkit in an SME context: A multiple case study," *KnE Soc. Sci.*, pp. 73–101, 2023.

[18] D. Ferdiansyah, S. A. Majapahit, and M. F. Muttaqin, "Assessment of village readiness for electronic citizen complaint services (e-AduMas) using COBIT 4.1," *J. Inf. Syst. Inform.*, vol. 5, no. 4, Dec. 2023, doi: 10.51519/journalisi.v5i4.578.

[19] V. P. Pradana et al., "Evaluating IT performance management in the Faculty of Industrial Engineering at Telkom University through COBIT 2019 domain MEA01 in alignment with LAM-INFOKOM standards," *Electron. Integr. Comput. Algorithm J.*, vol. 1, no. 2, pp. 41–49, 2024.

[20] A. Lelengboto, G. Mandoya, and J. Y. Mambu, "Tailoring governance system design through capability level identification using COBIT 2019 at a paper and mills company," *JURIKOM J. Ris. Komput.*, vol. 9, no. 6, pp. 1865–1873, 2022.

[21] G. Bagus et al., "Information technology governance audit using the COBIT 2019 framework at XYZ institution," *Cogito Smart J.*, vol. 8, no. 2, 2022.

[22] A. Lelengboto, G. Mandoya, and J. Y. Mambu, "Tailoring governance system design through capability level identification using COBIT 2019 at a paper and mills company," *JURIKOM J. Ris. Komput.*, vol. 9, no. 6, pp. 1865–1873, 2022.

[23] I. F. Wulandari, M. I. Herdiansyah, Y. N. Kunang, W. Cholil, M. Ariandi, and U. Ependi, "The performance analysis of SIKITO LLDIKTI Region II system using COBIT 2019 framework: A case study," *Int. J. Artif. Intell. Res.*, vol. 7, no. 2, pp. 111–121, 2024.

[24] G. Bagus, R. Francolla, G. R. Mandoya, M. D. Walangitan, E. Lompoliu, and J. Y. Mambu, "Information technology governance audit using the COBIT 2019 framework at XYZ institution," *Cogito Smart J.*, vol. 8, no. 2, 2022.

[25] A. B. Sipayung and R. Yunis, "Evaluation of information technology governance at Mikroskil University using COBIT 2019 framework with BAI11 domain," *Int. J. Res. Appl. Technol. (INJURATECH)*, vol. 2, no. 2, pp. 128–143, 2022.