Analysis of Learning Management System Governance Capability Levels Using the COBIT 2019 Framework in Higher Education Institutions

Robet Hotma Silaban, Muhammad Syahputra Novelan, Eko Hariyanto

Abstract

The governance of Learning Management Systems (LMS) plays a crucial role in ensuring the effectiveness, reliability, and sustainability of digital learning services in higher education institutions. However, the increasing complexity of LMS implementation requires systematic governance evaluation to ensure alignment between information technology management and institutional objectives. This study aims to analyze LMS governance capability levels using the COBIT 2019 framework and identify potential areas for governance improvement. The research employs a descriptive qualitative approach involving data collection through interviews, questionnaires, direct observations, and institutional documentation. The evaluation process includes identifying relevant governance and management objectives, mapping LMS operational practices to COBIT 2019, examining assessment indicators, evaluating supporting evidence, and conducting capability level and gap analyses. Fifteen candidate COBIT 2019 objectives are considered to represent essential governance dimensions, including strategic direction, IT resource management, risk management, information security, data governance, service availability, incident management, operational continuity, and performance monitoring. The assessment emphasizes evidence-based evaluation to ensure that capability measurements accurately reflect actual institutional governance practices. The proposed analytical structure organizes the evaluation into four components: governance objective mapping, assessment indicators and supporting evidence, capability level assessment, and gap analysis with improvement recommendations. The study is expected to provide a systematic basis for identifying governance strengths, operational weaknesses, and priority areas requiring institutional improvement. Since verified assessment data are not yet available, numerical capability levels and empirical gap measurements are not reported. The resulting evaluation framework is intended to support informed decision-making, strengthen institutional IT governance, and promote effective, secure, and sustainable LMS management in higher education institutions through continuous improvement initiatives.

Keywords: COBIT 2019; Learning Management System; IT Governance; Capability Level; Higher Education.

[1]Robet Hotma Silaban
[1]Magister Teknologi Informasi, Universitas Pembangunan Panca Budi, Indonesia
e-mail: robertsilaban96@gmail.com [1]

[2]Muhammad Syahputra Novelan, [3]Eko Hariyanto
[2,3]Magister Teknologi Informasi, Universitas Pembangunan Panca Budi, Indonesia
e-mail: putranovelan@dosen.pancabudi.ac.id [2], eko.hariyanto@dosen.pancabudi.ac.id [3]
2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era
https://proceeding.pancabudi.ac.id/index.php/ICIE/index

Introduction

The development of information and communication technology has significantly transformed the implementation of higher education, particularly in the delivery of teaching and learning activities. Digital transformation in higher education institutions encourages the adoption of technology-based learning systems to improve the effectiveness, flexibility, and accessibility of educational services. One of the technologies widely implemented is the Learning Management System (LMS), which provides an integrated platform for managing learning materials, distributing assignments, conducting online assessments, monitoring student participation, and facilitating interactions between lecturers and students. The implementation of LMS has become an important component in supporting modern academic activities because it enables learning processes to be conducted more efficiently, systematically, and independently of geographical and temporal limitations[1] [2] [3].

Despite its benefits, LMS implementation requires effective information technology governance to ensure that the system operates optimally and aligns with institutional objectives. Higher education institutions face various challenges in managing LMS, including system availability, information security, data management, service quality, infrastructure reliability, and user satisfaction. Inadequate governance may lead to ineffective system utilization, operational disruptions, data security risks, and inconsistencies between technology investments and institutional needs. Therefore, evaluating LMS governance capabilities is essential to determine whether the implemented technology has achieved the expected level of performance and whether its management processes support sustainable digital learning services [4][5][6].

Information technology governance provides a structured approach to ensuring that technology resources are managed responsibly, risks are controlled, and organizational objectives are achieved. One framework that can be used to evaluate IT governance is Control Objectives for Information and Related Technologies (COBIT) 2019, developed by ISACA. COBIT 2019 provides a comprehensive governance and management framework consisting of principles, governance components, and management objectives that help organizations assess and improve their IT governance capabilities. The framework enables higher education institutions to identify governance priorities, evaluate existing processes, measure capability levels, and formulate improvement strategies based on organizational requirements. Its flexible and systematic approach makes COBIT 2019 relevant for assessing the governance of digital learning platforms, including LMS [7] [8][9].

This study focuses on analyzing the capability level of Learning Management System governance in higher education institutions using the COBIT 2019 framework. The evaluation is conducted by identifying relevant governance and management objectives that correspond to LMS operational requirements, particularly in areas related to IT service management, system performance, information security, risk management, and service monitoring. The assessment process involves collecting organizational data, identifying existing governance practices, evaluating process implementation, and measuring capability levels against the established COBIT 2019 criteria. Furthermore, a gap analysis is performed to identify differences between the current capability level and the expected capability level. The results are expected to provide an objective overview of the effectiveness of LMS governance and reveal areas that require improvement [10], [11].

The contribution of this study is to provide an evidence-based evaluation model for assessing LMS governance capabilities in higher education institutions through the application of COBIT 2019. The findings are expected to support institutional decision-making in establishing governance improvement priorities, strengthening IT management practices, and improving the quality and reliability of digital learning services. In addition, the study provides practical recommendations for aligning LMS governance with institutional strategic objectives,

ensuring sustainable technology utilization, and supporting the development of a more effective digital learning environment. Thus, the implementation of COBIT 2019 is expected to serve as a reference for higher education institutions in improving IT governance maturity and strengthening the role of digital technology in educational service delivery [12].

Literature Review

Learning Management System (LMS) is an information technology platform designed to support the management, delivery, and evaluation of digital learning activities in educational institutions. LMS provides various functionalities, including learning material distribution, assignment management, online assessments, academic communication, and student learning progress monitoring. In higher education institutions, LMS plays an important role in supporting the digital transformation of academic services by providing flexible and integrated learning environments. However, the successful implementation of LMS is not solely determined by technological availability but also depends on effective system management, information security, service reliability, and the ability to align technology utilization with institutional objectives. Therefore, appropriate IT governance is required to ensure that LMS implementation delivers sustainable benefits and supports institutional performance [13], [14].

Information technology governance refers to the structures, processes, and organizational mechanisms used to ensure that IT resources support business objectives, optimize technology investments, and manage information technology-related risks. One of the established frameworks for implementing IT governance is COBIT 2019, developed by the Information Systems Audit and Control Association (ISACA). COBIT 2019 provides a comprehensive framework for evaluating and improving IT governance through governance and management objectives, design factors, performance management, and capability assessment. The framework consists of five domains: Evaluate, Direct and Monitor (EDM), Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), and Monitor, Evaluate and Assess (MEA). These domains provide a systematic foundation for assessing organizational IT governance practices, including the management, operation, security, and monitoring of LMS in higher education institutions [15].

Capability level assessment in COBIT 2019 is used to determine the extent to which governance and management processes have been implemented effectively and consistently. The assessment adopts a structured measurement approach to identify existing capabilities, evaluate process performance, and determine areas requiring improvement. Capability levels range from Level 0 (Incomplete) to Level 5 (Optimizing), representing progressive stages of process implementation and improvement. In the context of LMS governance, capability assessment can help higher education institutions identify weaknesses in IT service management, information security, risk control, system performance, and service monitoring. Furthermore, the results can be used to conduct gap analysis between current and expected capability levels, providing a basis for developing targeted improvement recommendations. Thus, COBIT 2019 serves as a methodological foundation for evaluating LMS governance capabilities and supporting continuous improvement in digital learning services [15] [16].

Research Methodology

This study employs a descriptive qualitative research approach to evaluate the governance capability of Learning Management Systems (LMS) in higher education institutions using the COBIT 2019 framework. The research aims to assess the current capability level of LMS governance, identify gaps between existing practices and expected capability levels, and formulate recommendations for improving IT governance. Data are collected through interviews with IT personnel and relevant stakeholders, questionnaires, direct observations of LMS operational activities, and analysis of institutional documents related to IT policies, procedures, system management, and digital learning services.

The evaluation process is conducted systematically by aligning the collected data with the governance and management objectives defined in the COBIT 2019 framework. The methodology emphasizes identifying relevant governance objectives, examining existing LMS management practices, assessing process capability levels, analyzing gaps, and formulating improvement recommendations. The assessment is designed to provide an objective overview of LMS governance implementation and establish improvement priorities that support effective IT management and sustainable digital learning services in higher education institutions.



Figure 1. Research Methodology

1. Research Planning and Scope Definition
   The first stage involves defining the research objectives, determining the scope of LMS governance evaluation, and identifying stakeholders involved in LMS management and utilization. The institutional IT environment, organizational structure, LMS infrastructure, and existing academic digital services are examined to establish the research boundaries. Furthermore, relevant governance and management objectives are selected based on the COBIT 2019 design factors and the characteristics of LMS implementation in higher education institutions.
2. Data Collection
   Data collection is conducted using multiple techniques to obtain comprehensive information regarding LMS governance practices. Primary data are obtained through interviews with IT managers, system administrators, LMS operators, lecturers, and other relevant stakeholders. Questionnaires are distributed to assess the implementation of governance and management activities based on selected COBIT 2019 objectives. Direct observations are also conducted to examine actual LMS operational activities. Secondary data consist of institutional IT policies, standard operating procedures, system documentation, infrastructure records, and other relevant institutional documents. All assessment results are based on actual research evidence.
3. Mapping LMS Governance Practices to COBIT 2019
   The collected information is analyzed by mapping existing LMS governance and management practices to relevant COBIT 2019 governance and management objectives. The mapping process considers the five COBIT 2019 domains: Evaluate, Direct and Monitor (EDM), Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), and Monitor, Evaluate and Assess (MEA). Relevant objectives are selected according to the research scope and organizational requirements. This stage provides a structured understanding of how existing LMS governance practices correspond to the COBIT 2019 framework.

4. Capability Level Assessment and Gap Analysis
   After the mapping process, the selected governance and management objectives are assessed to determine their implementation capability levels. The assessment is conducted by examining actual evidence obtained from interviews, questionnaires, observations, and institutional documentation. The results are evaluated using the COBIT 2019 Performance Management approach to determine the extent to which the assessed processes meet the established capability criteria. Subsequently, gap analysis is performed by comparing the current capability levels with the expected capability levels. This process identifies governance weaknesses, implementation deficiencies, and areas requiring improvement.
5. Formulation of Improvement Recommendations
   Based on the capability assessment and gap analysis results, improvement recommendations are formulated to strengthen LMS governance in higher education institutions. The recommendations focus on improving IT governance policies, optimizing LMS operational procedures, strengthening information security, enhancing risk management, improving service quality, and establishing systematic performance monitoring. Improvement priorities are determined based on the identified capability gaps and institutional requirements. The proposed recommendations are expected to provide practical guidance for achieving more effective, measurable, and sustainable LMS governance.
6. Conclusion and Validation
   The final stage summarizes the research findings, including the identified capability levels, governance gaps, and proposed improvement recommendations. Validation is conducted through discussions with relevant stakeholders to examine the feasibility, relevance, and applicability of the proposed recommendations. Feedback from the validation process is used to refine the improvement priorities. The final results are expected to provide a structured reference for strengthening LMS governance capabilities and supporting continuous improvement in digital learning services within higher education institutions.

Results

This section presents the results of the Learning Management System (LMS) governance evaluation using the COBIT 2019 framework in higher education institutions. The evaluation focuses on identifying relevant governance and management objectives, examining assessment indicators, evaluating supporting evidence, determining capability levels, and analyzing gaps between current and expected governance conditions. The analysis is structured into four tables covering objective mapping, assessment indicators and supporting evidence, capability-level assessment, and improvement recommendations. A total of 15 candidate COBIT 2019 objectives are included to represent essential aspects of LMS governance, including governance direction, IT management, human resource management, risk management, information security, data governance, service availability, operational management, incident handling, service continuity, and performance monitoring. Each objective is examined based on its relevance to LMS operations and institutional requirements. The assessment process emphasizes the use of actual research evidence obtained through interviews, questionnaires, observations, and institutional documentation. Furthermore, the evaluation is intended to identify governance strengths, implementation weaknesses, and improvement priorities. The final capability levels, target values, and gap measurements must be established through validated assessment results rather than assumptions, ensuring that the research findings provide an objective and reliable representation of LMS governance implementation.

Table 1. Mapping of Selected COBIT 2019 Objectives for LMS Governance

No.	Objective Code	COBIT 2019 Objective	Relevance to LMS Governance	Selection Status
1	EDM01	Ensured Governance Framework Setting and Maintenance	Governance structure, decision rights, accountability, and policies for LMS	Candidate; confirm through design-factor assessment
2	EDM02	Ensured Benefits Delivery	Expected academic and institutional benefits generated through LMS	Candidate; confirm through design-factor assessment
3	EDM03	Ensured Risk Optimization	Governance oversight of LMS-related security, availability, privacy, and continuity risks	Candidate; confirm through design-factor assessment
4	APO01	Managed I&T Management Framework	IT governance framework, process ownership, policies, and responsibilities	Candidate; confirm through design-factor assessment
5	APO07	Managed Human Resources	Competencies, staffing, training, and role readiness of LMS personnel	Candidate; confirm through design-factor assessment
6	APO09	Managed Service Agreements	Service catalogue, service expectations, and measurable LMS service commitments	Candidate; confirm through design-factor assessment
7	APO12	Managed Risk	Identification, assessment, treatment, and monitoring of LMS-related risks	Candidate; confirm through design-factor assessment
8	APO13	Managed Security	Information security management policies and arrangements for LMS	Candidate; confirm through design-factor assessment
9	APO14	Managed Data	Data ownership, quality, access, retention, and protection of LMS information	Candidate; confirm through design-factor assessment
10	BAI04	Managed Availability and Capacity	Availability, performance, capacity, and scalability of LMS services	Candidate; confirm through design-factor assessment
11	BAI06	Managed IT Changes	Assessment, approval, testing, implementation, and recording of LMS changes	Candidate; confirm through design-factor assessment
12	DSS01	Managed Operations	Daily LMS operation, operational procedures, and infrastructure monitoring	Candidate; confirm through design-factor assessment
13	DSS02	Managed Service Requests and Incidents	Handling of LMS user requests, access problems, and service incidents	Candidate; confirm through design-factor assessment
14	DSS04	Managed Continuity	Backup, recovery, and continuity arrangements for LMS services	Candidate; confirm through design-factor assessment
15	MEA01	Managed Performance and Conformance Monitoring	Monitoring of LMS service performance and conformance with defined targets	Candidate; confirm through design-factor assessment

Table 1 presents 15 candidate COBIT 2019 governance and management objectives that can be considered in evaluating LMS governance. The selection is organized to represent several important dimensions of LMS management. The EDM objectives address governance direction, expected benefits, and risk oversight. The APO objectives relate to the institutional IT management framework, human resources, service agreements, risk management, information security, and data governance. The BAI objective concerns availability and capacity as well as the control of system changes, while the DSS objectives focus on daily operations, service requests, incidents, and continuity. MEA01 provides a basis for monitoring performance and conformance. This mapping is intended to ensure that the evaluation considers

both management and operational aspects of the LMS rather than focusing only on technical functionality. Nevertheless, the 15 objectives remain a proposed assessment scope and should not be interpreted as a confirmed institutional selection. Their relevance must be verified through COBIT 2019 design factors, institutional priorities, the LMS operating environment, and the availability of valid assessment evidence. Objectives that are not relevant to the actual research context should be excluded or replaced with a justified alternative before the assessment is conducted.

Table 2. Assessment Indicators and Supporting Evidence for Selected Objectives

No.	Code	Objective	Indicators and Evidence to be Examined	Potential Evidence Source
1	EDM01	Ensured Governance Framework Setting and Maintenance	Approved governance structure; documented decision rights; LMS policies; defined accountability; periodic governance review records	Interview, observation, questionnaire, or institutional document
2	EDM02	Ensured Benefits Delivery	Defined expected benefits; benefit indicators; monitoring reports; evidence of review against academic and institutional objectives	Interview, observation, questionnaire, or institutional document
3	EDM03	Ensured Risk Optimization	Risk oversight responsibilities; risk tolerance; escalation arrangements; risk reports; periodic governance review	Interview, observation, questionnaire, or institutional document
4	APO01	Managed I&T Management Framework	IT management framework; process ownership; approved policies; documented roles and responsibilities; process review records	Interview, observation, questionnaire, or institutional document
5	APO07	Managed Human Resources	Staff competency profiles; LMS administrator duties; training plans; training attendance; competency evaluation	Interview, observation, questionnaire, or institutional document
6	APO09	Managed Service Agreements	LMS service catalogue; service-level targets; service agreements; service review reports; service issue records	Interview, observation, questionnaire, or institutional document
7	APO12	Managed Risk	LMS risk register; risk assessment; risk owners; mitigation plans; monitoring and review schedule	Interview, observation, questionnaire, or institutional document
8	APO13	Managed Security	Information security policies; access-control rules; security responsibilities; security assessment; corrective actions	Interview, observation, questionnaire, or institutional document
9	APO14	Managed Data	Data ownership; data classification; data quality checks; access rules; data retention and disposal procedures	Interview, observation, questionnaire, or institutional document
10	BAI04	Managed Availability and Capacity	Availability targets; capacity plans; performance monitoring; infrastructure utilization; service availability records	Interview, observation, questionnaire, or institutional document
11	BAI06	Managed IT Changes	Change requests; impact assessment; authorization records; test results; implementation records; rollback procedures	Interview, observation, questionnaire, or institutional document
12	DSS01	Managed Operations	Operational schedules; standard operating procedures; system logs; routine monitoring; operational issue records	Interview, observation, questionnaire, or institutional document

Table 2 describes the assessment indicators and supporting evidence required to examine the implementation of each selected objective. The indicators are intended to guide the collection and verification of evidence rather than serve as predetermined findings. For example, governance-related objectives require evidence such as approved policies, defined responsibilities, decision-making records, and governance reviews. Objectives associated with risk, security, and data management require risk registers, access-control documentation, data-management procedures, and records of security reviews. Operational objectives require evidence from system logs, service request records, incident tickets, backup schedules, recovery tests, and performance monitoring reports. The evidence-source column indicates the types of research materials that may be used to substantiate each assessment, including interviews, observations, questionnaires, and institutional documents. During the actual research, this column should be made more specific by recording the document title, interviewee role, observation date, questionnaire item, or system record used. Triangulation among different evidence sources is important to reduce reliance on individual perceptions and to strengthen the validity of the assessment. An indicator should only be considered fulfilled when the available evidence demonstrates that the relevant activity has been performed and can be verified.

Table 3. Capability Level Assessment of Selected COBIT 2019 Objectives

No.	Objective Code	Governance/Management Objective	Current Capability Level	Evidence Reference	Assessment Status
1	EDM01	Ensured Governance Framework Setting and Maintenance	To be assessed	Insert verified evidence reference	Pending assessment
2	EDM02	Ensured Benefits Delivery	To be assessed	Insert verified evidence reference	Pending assessment
3	EDM03	Ensured Risk Optimization	To be assessed	Insert verified evidence reference	Pending assessment
4	APO01	Managed I&T Management Framework	To be assessed	Insert verified evidence reference	Pending assessment
5	APO07	Managed Human Resources	To be assessed	Insert verified evidence reference	Pending assessment
6	APO09	Managed Service Agreements	To be assessed	Insert verified evidence reference	Pending assessment
7	APO12	Managed Risk	To be assessed	Insert verified evidence reference	Pending assessment
8	APO13	Managed Security	To be assessed	Insert verified evidence reference	Pending assessment
9	APO14	Managed Data	To be assessed	Insert verified evidence reference	Pending assessment
10	BAI04	Managed Availability and Capacity	To be assessed	Insert verified evidence reference	Pending assessment
11	BAI06	Managed IT Changes	To be assessed	Insert verified evidence reference	Pending assessment
12	DSS01	Managed Operations	To be assessed	Insert verified evidence reference	Pending assessment
13	DSS02	Managed Service Requests and Incidents	To be assessed	Insert verified evidence reference	Pending assessment
14	DSS04	Managed Continuity	To be assessed	Insert verified evidence reference	Pending assessment
15	MEA01	Managed Performance and Conformance Monitoring	To be assessed	Insert verified evidence reference	Pending assessment

Table 3 provides the format for presenting the capability assessment results for the 15 selected COBIT 2019 objectives. The current capability level must be established through a structured examination of the relevant activities and their supporting evidence, using the COBIT 2019 Performance Management approach. The assessment should determine the extent

to which the required practices are implemented and achieved, rather than simply converting questionnaire averages into capability levels. Evidence may include approved procedures, documented responsibilities, transaction records, operational logs, monitoring reports, and interview confirmations that can be cross-checked against institutional documents. The evidence-reference column should identify the source used to support the assessment decision so that the result can be traced and reviewed. The current capability level and assessment status are deliberately marked as pending because the actual assessment data have not yet been supplied. Once the assessment is completed, each objective should be assigned a capability result only where the required evidence supports that conclusion. If the evidence is insufficient, the limitation should be recorded instead of assigning an assumed score. This approach ensures that the capability profile reflects the actual governance condition of the LMS and remains methodologically defensible.

Table 4. Gap Analysis and Improvement Recommendations for LMS Governance

No.	Code	Current Level	Target Level	Gap	Priority	Improvement Recommendation
1	EDM01	To be measured	To be justified	To be calculated	To be prioritized	If governance roles or policies are not sufficiently defined, formalize the LMS governance structure, decision rights, accountability, and policy review schedule.
2	EDM02	To be measured	To be justified	To be calculated	To be prioritized	If benefits are not systematically evaluated, define measurable LMS benefit indicators and periodically review their contribution to academic objectives.
3	EDM03	To be measured	To be justified	To be calculated	To be prioritized	If risk oversight is incomplete, strengthen risk reporting, escalation, treatment monitoring, and periodic governance review for LMS-related risks.
4	APO01	To be measured	To be justified	To be calculated	To be prioritized	If the IT management framework is unclear, document process ownership, responsibilities, governance policies, and review procedures.
5	APO07	To be measured	To be justified	To be calculated	To be prioritized	If competency gaps are identified, develop role-based training and competency improvement plans for LMS administrators and support personnel.
6	APO09	To be measured	To be justified	To be calculated	To be prioritized	If service expectations are not measurable, establish an LMS service catalogue, service-level targets, responsibilities, and periodic service reviews.
7	APO12	To be measured	To be justified	To be calculated	To be prioritized	If risk management is not documented consistently, maintain an LMS risk register with risk owners, mitigation actions, and scheduled reviews.
8	APO13	To be measured	To be justified	To be calculated	To be prioritized	If information security controls are inadequate, strengthen security policies, access governance, security assessments, and corrective-action monitoring.
9	APO14	To be measured	To be justified	To be calculated	To be prioritized	If data governance is incomplete, define data ownership, classification, quality controls, access rules, retention, and disposal procedures.
10	BAI04	To be measured	To be justified	To be calculated	To be prioritized	If service availability or capacity is insufficient, implement capacity planning, performance thresholds, availability monitoring, and periodic review.
11	BAI06	To be measured	To be justified	To be calculated	To be prioritized	If system changes are not controlled, formalize change requests, impact assessments, authorization, testing, implementation, and post-change review.
12	DSS01	To be measured	To be justified	To be calculated	To be prioritized	If operational practices vary, standardize LMS operating procedures, operational schedules, log reviews, and routine monitoring responsibilities.

Table 4 is intended to connect the capability assessment with a structured improvement plan for LMS governance. The gap is determined by comparing the current capability level with the target capability level established for each objective. Both values must be based on a documented assessment and a clear institutional rationale; the target should not automatically be set at the highest capability level without considering organizational needs, risk exposure, available resources, and strategic priorities. The recommendations in the table are conditional examples and should only be retained when the corresponding weakness is confirmed by actual research evidence. For instance, recommendations concerning governance structure, security, data management, service agreements, incident handling, and continuity should be adapted to the specific gaps identified in the institution. The priority column should be determined by considering the magnitude of the capability gap together with the potential impact on learning activities, the likelihood and consequences of operational risks, stakeholder requirements, and the feasibility of implementing corrective actions. In this way, the gap analysis does not merely describe differences between current and expected conditions but also provides a reasoned basis for selecting improvement actions. The final improvement plan can be used by institutional decision-makers to determine which governance areas require immediate attention and which can be addressed through medium- or long-term initiatives.

Conclusion

This study presents a framework for evaluating Learning Management System (LMS) governance in higher education institutions using COBIT 2019. The evaluation is structured to identify relevant governance and management objectives, examine their implementation through assessment indicators and supporting evidence, determine capability levels, and analyze gaps between existing practices and institutional expectations. The proposed assessment structure covers key aspects of LMS governance, including strategic direction, IT management, risk management, information security, data governance, service availability, operational management, and performance monitoring.

The use of COBIT 2019 provides a systematic basis for assessing LMS governance practices and identifying areas that require improvement. However, the final capability levels and governance gaps can only be established after collecting and validating actual institutional data. Therefore, this study does not present numerical capability scores or empirical conclusions that have not been supported by research evidence. The findings are expected to provide a basis for developing prioritized improvement recommendations aligned with institutional needs, thereby supporting more effective, secure, reliable, and sustainable LMS governance in higher education institutions..

References

[1] E. Syahputra, M. Iqbal, R. Farta Wijaya, and D. Nasution, “EVALUATION OF INFORMATION TECHNOLOGY GOVERNANCE E-KINERJA SYSTEMS IN ASSESSING EMPLOYEE PERFORMANCE USING THE MODEL COBIT 2019 AT THE DISTRICT COMMINFO OFFICE WAS REALLY FUN,” *Bulletin of Engineering Science, Technology and Industry*, 2024, [Online]. Available: https://bestijournal.org

[2] M. S. Novelan, S. Efendi, P. Sihombing, and H. Mawengkang, “VEHICLE ROUTING PROBLEM OPTIMIZATION WITH MACHINE LEARNING IN IMBALANCED CLASSIFICATION VEHICLE ROUTE DATA,” *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 3(125), pp. 49–56, 2023, doi: 10.15587/1729-4061.2023.288280.

[3] B. Susanto and L. Hakim, "Customizing IT Governance in Healthcare Organizations Using COBIT 2019 Design Factors," in Proc. 8th International Conference on Information Technology and Healthcare (ICITH), IEEE, 2022, pp. 134-139.

[4] H. Akbar and R. Saputra, "Evaluasi Kinerja Tata Kelola Teknologi Informasi terhadap Tools Internal Framework Cobit," *Sebatik*, vol. 27, no. 2, p. 27, 2023, doi: 10.46984/sebatik.v26i2.2336.

[5] K. Y. Lee and T. H. Chen, "Evaluating the Efficacy of IT Governance Frameworks in Modern Hospital Management," IEEE Transactions on Engineering Management, vol. 71, no. 2, pp. 1102-1115, Feb. 2024.

[6] J. Martinez, E. Silva, and R. Gomez, "The Role of Organizational Culture and Human Capital in Information Technology Governance," IEEE IT Professional, vol. 27, no. 1, pp. 45-51, Jan.-Feb. 2025.

[7] M. T. Anwar and N. Zahra, "Applying COBIT 2019 Design Factors for Mapping IT Governance Maturity in Healthcare Institutions," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 54, no. 3, pp. 1560-1572, 2024

[8] Z. Sitorus, D. Prayogi, M. A. Rizko, A. G. Suteja, and M. R. Harahap, "Implementation of the Insertion Sort Algorithm to Sort Positive Integers in Ascending Order Using Flowgorithm," *Journal of Information Technology, computer science and Electrical Engineering (JITCSE)*, vol. 1, no. 3, pp. 323–328, 2024, doi: 10.30596/jitcse.

[9] J. Kim and H. Park, "The Impact of IT Governance on Digital Literacy and Employee Performance in Smart Hospitals," IEEE Access, vol. 13, pp. 33201-33215, 2025.

[10] G. S. Mahendra and I. K. Sari, "Measurement of IT Governance Capability Level using COBIT 2019: A Case Study on Hospital Information Systems," Journal of Electrical Engineering and Computer Sciences (JEECS), vol. 8, no. 2, pp. 45-53, Dec. 2023.

[11] Sitorus, Z., Syahputra, H., & Sugito, B. (2024). Predicting The Effectiveness of Online Exam Platforms With LMS to Improve Online Learning Using The Cobit 5 Method. *Journal of Information Technology, Computer Science and Electrical Engineering (JITCSE)*, *1*(2), 1–09. https://doi.org/10.61306/jitcse

[12] Z. Sitorus, H. Syahputra, and B. Sugito, "Predicting The Effectiveness of Online Exam Platforms With LMS to Improve Online Learning Using The Cobit 5 Method," *Journal of Information Technology, computer science and Electrical Engineering (JITCSE)*, vol. 1, no. 2, pp. 1–09, 2024, doi: 10.61306/jitcse.

[13] R. Rezki, R. Farta Wijaya, and M. S. Novelan, "UKInstitute Evaluation of Information Technology Governance Related to Digital Transformation on The Alignment of Company Business Strategy Using Cobit 2019 And Fuzzy C-Means (Case Study: Perumda Tirtanadi, North Sumatra Province)," *Journal of Research in Social Science and Humanities*, vol. 5, no. 4, 2025, doi: 10.47679/jrssh.v5i4.

[14] R. Farta Wijaya, F. Kurniawan, R. R. Putrai, A. Alvin, F. Sains, and D. Teknologi, "OPTIMIZING THE MANAGEMENT OF VILLAGE ACTIVITIES THROUGH INFORMATION SYSTEMS FOR TRANSPARENCY AND ACCOUNTABILITY IN PERTUMBUKAN VILLAGE, WAMPU DISTRICT," 2024.

[15] T. A. Karo Karo and A. Faza, "Evaluation of Integration and Human Resources in Information Technology Governance using COBIT 2019: PT. Pelabuhan Indonesia Tanjung Priok Branch," *Journal of Information Systems and Informatics*, vol. 5, no. 3, pp. 902–914, Aug. 2023, doi: 10.51519/journalisi.v5i3.538.