CoreID JOURNAL

Vol. 4 No. 1, March 2026 (32-37)
ISSN: 2987-6990
DOI: https://doi.org/10.60005/coreid.v4i1.159

Information System Audit of Learning Management System Using COBIT 5 Army Staff and Command School

Erfin Erfiana[1], Erwin Teguh Arujisaputra[2], Purwadi[3]
[1,2,3]Faculty of Computer Science Universitas Kebangsaan Republik Indonesia Bandung, Indonesia

Article Info

Article history:

Received March 27, 2026
Revised April 22, 2026
Accepted May 13, 2026

Keywords:

COBIT 5
Information System Audit
Maturity Level
Learning Management System
Risk Management

ABSTRACT

In the digital era, information technology has become a core component of the education system, with the Learning Management System (LMS) as the primary platform for online learning. The Army Staff and Command College (SESKOAD) have implemented an LMS to support educational effectiveness and efficiency, but has not yet undergone a formal audit, thus risking regulatory non-compliance and security weaknesses. This study aims to measure the maturity level of IT governance and LMS management using the COBIT 5 framework through a descriptive quantitative approach. Data were collected through observation, structured interviews, and a Likert-scale questionnaire (0–5) distributed to selected respondents using purposive sampling, covering the roles of IT administrators, operational users, and management. The research instruments were derived from practices and process activities in the domains APO9, DSS01, DSS04, DSS05, DSS06, MEA01, and MEA02. The assessment was conducted using the COBIT 5 Process Capability Model by measuring the achievement of process attributes (PA1.1 to PA5.2) which were converted into numerical scores, then the average value per process was calculated and aggregated to determine the capability level (Level 0–5) based on the ISO/IEC 15504 standard threshold. The results showed that the LMS was at Level 2 (Managed Process) with gaps in formal documentation, risk control, and security control. Recommendations focused on standardizing SOPs, increasing user awareness and competence, and implementing continuous security audits to gradually reach Level 4 within five years.

Corresponding Author:

Erfin Erfiana
Faculty of Computer Science Universitas Kebangsaan Republik Indonesia Bandung, West Java, Indonesia
Email: erfin.erfiana@student.ukri.ac.id

1. INTRODUCTION

In the era of digital transformation, the integration of information technology in education has evolved from a mere tool to a key enabler in creating adaptive, efficient, and data-driven learning systems. A Learning Management System (LMS) is a key infrastructure that supports online learning, content management, and integrated learning analytics. The use of an LMS has been proven to improve the quality of learning and the flexibility of educational access, especially after the COVID-19 pandemic [1][2]. However, increasing reliance on LMS is also accompanied by various risks, including information security, data privacy, and compliance with good information technology governance [3],[4]. Therefore, a systematic information system audit is needed to ensure that the LMS implementation is not only operationally effective, but also meets the principles of governance, risk, and compliance (GRC).

In the context of military education, the urgency of IT governance becomes even more critical due to the environment's demanding high levels of security, confidentiality, and compliance. The Army Staff and

Command College (Seskoad), as a strategic educational institution within the Indonesian Army (TNI AD), has adopted an LMS to support its officer training process. However, to date, there has been no formal audit of the LMS system in use. This lack of auditing has the potential to create a gap between system implementation and IT governance standards, which could lead to increased security risks, regulatory inconsistencies, and low information reliability [5]. Studies show that organizations with low levels of IT governance maturity tend to have a higher vulnerability to system disruptions and security incidents [6],[7].

Several previous studies have examined information systems audits using the COBIT 5 framework in the education sector. For example, evaluations of e-learning systems and academic systems show varying levels of capability, generally ranging from level 1 to level 3, with major weaknesses in documentation and process control [8], [9]. Other studies have shown that although some domains have reached higher levels of maturity, evaluations are often limited to specific domains and do not include comprehensive gap analysis [10]. Furthermore, most research still focuses on civilian educational institutions, while studies in the context of military education, which has more complex security and control needs, are still very limited [11], [12]. This indicates a research gap in the development of a comprehensive and contextual COBIT 5-based LMS audit model [13], [14].

Based on this gap, this study aims to conduct an audit of the LMS information system at SESKOAD using the COBIT 5 framework with a focus on measuring capability levels and analyzing gaps between existing conditions and expected targets [15] [16]. The contributions of this study include the application of COBIT 5 in the context of military education, the development of a process attributes-based evaluation instrument to increase measurement objectivity, and the preparation of a structured roadmap for improving IT governance. Thus, this study is expected to provide theoretical contributions to the development of IT governance as well as practical implications in improving the effectiveness, efficiency, and security of LMS.

2. METHOD

This research uses the COBIT 5 framework as its methodology because it offers a comprehensive and structured approach to assessing IT governance and information system capabilities [17]. The research focuses on three main domains relevant to an operational LMS (as opposed to development or strategic-level domains): **(1) Align, Plan and Organize (APO)**: Sub-domain APO9 (**Manage Service Agreements**) assesses the extent to which service agreements between LMS providers and users are designed and implemented in accordance with the operational needs of military education. (2) **Deliver, Service and Support (DSS)**: Sub-domains DSS01 (**Manage Operations**), DSS04 (**Manage Continuity**), DSS05 (**Manage Security Services**), and DSS06 (**Manage Business Process Controls**) cover service delivery, disaster recovery, data and system security, and business process control. (3) **Monitor, Evaluate and Assess (MEA)**: Sub-domains MEA01 (**Monitor Performance and Conformance**) and MEA02 (**Monitor Compliance**) manage performance monitoring and formal compliance evaluation [18].

The average score for each domain is calculated as:

$$\text{Average Score} = \frac{\sum PA}{n}$$

Table 1. Capability Level Mapping

Score Range	Capability Level
0 – <1	Level 0 (Incomplete)
1 – <2	Level 1 (Performed)
2 – <3	Level 2 (Managed)
3	Level 3 (Established)

The domains EDM (Evaluate, Direct and Monitor) and BAI (Build, Acquire and Implement) were excluded because they focus on strategic governance at top-management level and new system construction, respectively, which are outside the scope of auditing an already-operational LMS system [19].

2.1. Data Collection

Data was collected through four approaches : (1) **Observation** – direct observation of LMS usage at Seskoad including workflow, features, and constraints; (2) **Interviews** – semi-structured interviews with IT staff, instructors, and system administrators (7 respondents) based on COBIT 5 process criteria [19]; (3) **Questionnaire** – Likert-scale (1–5) questionnaire with 23 items administered to 162 respondents (student officers, instructors, and staff); and (4) **Literature Review** – review of peer-reviewed journals and books related to IT governance, COBIT 5, and LMS auditing.

2.2. Capability Assessment

Data was analyzed using the COBIT 5 Process Assessment Model (PAM) to determine the capability level of each sub-domain. The assessment evaluates process goal achievement, documentation availability, procedure implementation, risk management readiness, disaster recovery, security governance, and performance monitoring [10]. Maturity levels were determined by comparing actual conditions against COBIT 5 standards, then validated through triangulation of the three data sources (observation, interview, questionnaire) [20].

3. RESULTS AND DISCUSSION

3.1. Triangulation Results and Maturity Level

Triangulation of the three data collection methods yielded consistent results across all seven evaluated sub-domains. Table 2 presents a summary of findings.

Table 2. Triangulation Results by Sub-domain

Aspect	Observation & Interview Result	Sub-domain	Maturity Level
Risk Management	Risk management is still weak, with minimal documentation, no formal risk identification, no mitigation plans, and no system security audits. Privacy policy compliance is not enforced.	APO9 - Manage Risk	Level 2 (Managed)
Operations Management	Technical documentation and SOPs are inadequate; operations frequently experience technical constraints; data backup is available but not optimal.	DSS01 - Manage Operations	Level 2 (Managed)
Service Continuity	Disaster recovery plan is not documented or consistently tested. Routine backup exists but service recovery readiness needs strengthening.	DSS04 - Manage Continuity	Level 2 (Managed)
Security Services	Security governance is weak; no security audit has been conducted; no clear responsible person; physical security is suboptimal.	DSS05 - Manage Security Services	Level 2 (Managed)
Business Process Controls	Manual guide documentation exists, but business process controls lack adequate monitoring and audit. Security responsibilities are unclear.	DSS06 – Manage Business Process Controls	Level 2 (Managed)
Performance Monitoring	LMS performance is measured through user surveys and academic data, but measurement is unstructured and not supported by adequate audit and control.	MEA01 – Monitor, Evaluate and Assess Performance	Level 2 (Managed)
Compliance Monitoring	Compliance with policies is not well-documented; no formal compliance audit has been conducted; regular checks are urgently needed.	MEA02 – Monitor, Evaluate and Assess Compliance	Level 2 (Managed)

Table 2 shows that all seven sub-domains are at Maturity Level 2 (Managed). This indicates systemic governance issues rather than isolated problems. Level 2 means processes have been performed and planned, but they are not consistently documented, monitored, or formally controlled. The LMS is operational but relies on informal and unintegrated processes.

This finding is consistent with similar studies. Krisyawan et al. [5] found an academic IS at capability level 1 in a university setting. Pratiwi et al. [4] found a library IS at capability level 2. The military context of Seskoad introduces additional governance complexity, as information security and operational continuity are mission-critical concerns that demand higher accountability and documentation standards than civilian institutions.

3.2. GAP Analysis

Based on the COBIT 5 maturity model [7], a GAP analysis was conducted comparing the current state (Level 2) against the target state (Level 4 – Quantitatively Managed). The target was set at Level 4 because Seskoad, as a military educational institution, requires high reliability, security, and quantitatively measurable governance for its information systems. The GAP spans two levels across all seven sub-domains, indicating that significant and structured improvement efforts are required.

At Level 4 (target), the LMS would exhibit: (1) fully integrated documentation and SOPs; (2) proactive real-time operational monitoring; (3) a robust, tested, and automated disaster recovery plan; (4) comprehensive security governance with regular audits; (5) integrated business process controls with quantitative measurement; and (6) a structured, data-driven performance and compliance monitoring system.

Table 3. Rating Scale

Score	Category	Description
0	Not Achieved	No evidence of implementation
1	Partially Achieved	Minor implementation exists
2	Largely Achieved	Most requirements are fulfilled
3	Fully Achieved	Fully implemented and documented

3.3. Improvement Recommendations

Based on the triangulation results and GAP analysis, seven improvement recommendations were formulated, as shown in Table 4.

Table 4. LMS System Improvement Recommendations

No.	Aspect	Improvement Recommendation	Benefit
1	Documentation & SOP	Develop and update technical documentation and SOPs for each sub-domain; ensure all processes are clearly documented and easily accessible.	Improve user understanding and reduce operational errors.
2	User Training	Conduct regular training for instructors, student officers, and administrative staff on LMS usage and new features.	Improve overall user proficiency and experience.
3	Risk Management	Formally identify risks and develop clear mitigation plans; conduct system security audits regularly.	Reduce harmful incidents such as data loss or security breaches.
4	Security Audit	Conduct routine security audits to verify controls are functioning properly and in line with established policies.	Identify security gaps and ensure user data protection.
5	Business Process Control	Implement stricter controls for LMS-related business processes, including data management and user activity monitoring.	Improve operational efficiency and reduce data management errors.
6	Performance Evaluation	Implement a structured performance evaluation system with periodic user satisfaction surveys and academic result analysis.	Identify areas needing improvement; ensure LMS meets user needs.
7	Compliance Policy	Develop and implement clear compliance policies for LMS usage, including data privacy policies and academic procedures.	Ensure all users comply with established standards; reduce violation risks.

The recommendations in Table 5 are prioritized in order of urgency: documentation and SOP development must come first (Year 1) as it underpins all subsequent improvements. User training follows to ensure adoption. Risk management and security audits address the most critical operational vulnerabilities, while business process controls, performance evaluation, and compliance policy represent higher-maturity governance capabilities to be built incrementally.

Table 5. Scores per Sub-Domain

Domain	PA1.1	PA2.1	PA2.2	Average Score	Level
APO9	3	2	2	2.33	2
DSS01	3	2	2	2.33	2
DSS04	2	2	1	1.67	2
DSS05	3	2	1	2.00	2
DSS06	2	2	2	2.00	2
MEA01	3	2	2	2.33	2
MEA02	2	2	2	2.00	2

3.4. System Blueprint and Five-Year Roadmap

Based on the capability assessment results and the identified two-level GAP, a transformation blueprint and strategic roadmap were developed following the principles of Ahlaro et al. [12]. The blueprint describes the transition from the current state (Level 2) to the target state (Level 4) through five implementation phases:

Year 1 - Foundation: Draft and finalize documentation and SOPs; conduct user training (two batches); perform initial risk identification, mitigation, and security audit; conduct annual review. Year 2 – Development: Design and implement business process controls; set up performance monitoring tools; develop and simulate a disaster recovery plan; conduct initial compliance assessment and integrate compliance with monitoring. Year 3 - Implementation: Pilot implementation on a limited area; phased rollout; full deployment; system stabilization; audit and documentation of implementation results. Year 4 – Optimization: Performance analysis; advanced feature development; external system integration; innovation prototyping lab. Year 5 – Evolution: Multi-region system adaptation; AI-based feature integration; system showcase; final documentation as

organizational legacy.

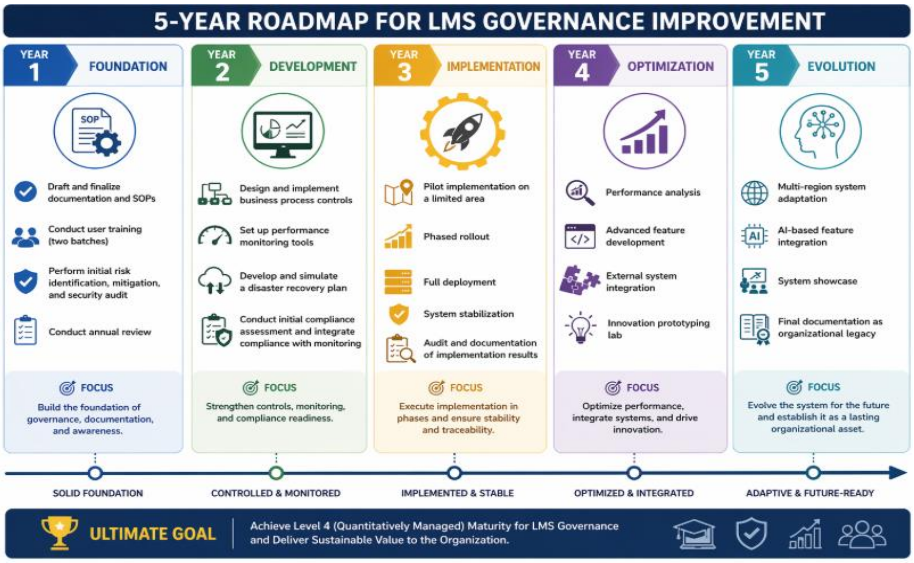

Figure 1. Roadmap E-Learning SESKOAD

This phased approach ensures sustainable progress, with each year building on the governance foundations established in the preceding year. The five-year roadmap is expected to elevate all seven sub-domains from Level 2 to Level 4, making the LMS governance structure quantitatively measurable and aligned with Seskoad's educational mission.

4. CONCLUSION

This study conducted an audit of the LMS information system at Seskoad using the COBIT 5 framework in seven sub-domains (APO9, DSS01, DSS04, DSS05, DSS06, MEA01, and MEA02), with the results showing the capability level at Level 2 (Managed Process). This condition indicates that the process has been running but is still partial, not standardized, and not supported by adequate documentation and performance measurement. Key findings include weaknesses in technical documentation and SOPs, unstructured risk management, the absence of a documented disaster recovery plan, weak security governance without regular audits, and the absence of an integrated performance monitoring and evaluation system. Based on a gap analysis of the COBIT 5 capability model, a target for upgrading to Level 4 (Quantitatively Managed) is set with the prerequisite of having measurable performance indicators (KPIs), data-based control, and comprehensive process integration. The proposed five-year roadmap is structured in stages, taking into account inter-process dependencies, organizational readiness, and resource requirements. Its implementation still requires further validation through feasibility testing and performance measurement based on baselines and quantitative targets. Conceptually, COBIT 5 provides a systematic evaluation framework, but its implementation effectiveness is highly dependent on consistency of implementation, managerial support, and organizational readiness. Therefore, further research is recommended to expand the audit scope to other systems, conduct comparative studies across military educational institutions, integrate other frameworks such as ITIL and ISO 27001, and evaluate implementation achievements longitudinally based on performance indicators at each stage of the roadmap.

ACKNOWLEDGEMENTS

The author would like to express his deepest gratitude to all parties who have provided support in the implementation of this research, especially to the leaders and ranks within the Army Staff and Command School (Seskoad) for permission, data access, and support during the research process, as well as to the information technology management team, LMS system users, and all respondents who have actively participated in data collection through questionnaires and interviews; appreciation is also expressed to fellow academics and colleagues for the constructive input provided, as well as to the author's home institution which has supported this research morally and academically, and to all other parties who cannot be mentioned one by one for their contributions, with the hope that the results of this research can provide benefits for the development of information technology governance, especially in improving the quality of LMS-based learning systems in the military education environment.

REFERENCES

[1] M. A. Almaiah, A. Al-Khasawneh, and A. Althunibat, "Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemicc," *Educ. Inf. Technol. (Dordr).*, vol. 25, no. 6, pp. 5261–5280, Nov. 2020, doi: 10.1007/s10639-020-10219-y.

[2] S. Dhawan, "Online Learning: A Panacea in the Time of COVID-19 Crisis," *Journal of Educational Technology Systems*, vol. 49, no. 1, pp. 5–22, Sep. 2020, doi: 10.1177/0047239520934018.

[3] C. Zhang, D. Jia, L. Wang, W. Wang, F. Liu, and A. Yang, "Comparative research on network intrusion detection methods based on machine learning," *Comput. Secur.*, vol. 121, p. 102861, Oct. 2022, doi: 10.1016/J.COSE.2022.102861.

[4] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/J.COSE.2013.04.004.

[5] Mikko T. Siponen, "A conceptual foundation for organizational information security awareness," 2021.

[6] E. Etzold, E. Liebscher, L.-M. Müller, L. Hennersdorf, and G. Weber, "LMS Check: Tailored Checklists for Creating Course-Specific Accessibility Statements for Learning Management Systems," *Procedia Comput. Sci.*, vol. 278, pp. 1210–1217, Jan. 2026, doi: 10.1016/J.PROCS.2026.03.102.

[7] L. Lai, Y. Dong, A. Wang, and D. M. Frangopol, "AI-assisted bridge management system using deep reinforcement learning with expert demonstrations," *Autom. Constr.*, vol. 187, p. 106934, Jul. 2026, doi: 10.1016/J.AUTCON.2026.106934.

[8] Z. P. Mkra, "Student feedback as an institutional analytic lens: Learning support and retention in an open distance e-learning university," *Social Sciences & Humanities Open*, vol. 13, p. 102610, Jun. 2026, doi: 10.1016/J.SSAHO.2026.102610.

[9] R. P. Alvarez, I. Jivet, M. Perez-Sanagustin, M. Scheffel, and K. Verbert, "Tools Designed to Support Self-Regulated Learning in Online Learning Environments: A Systematic Review," *IEEE Transactions on Learning Technologies*, vol. 15, no. 4, pp. 508–522, Aug. 2022, doi: 10.1109/TLT.2022.3193271.

[10] A. Anderson, D. Huttenlocher, J. Kleinberg, and J. Leskovec, "Engaging with massive online courses," *WWW 2014 - Proceedings of the 23rd International Conference on World Wide Web*, pp. 687–697, Apr. 2014, doi: 10.1145/2566486.2568042.

[11] R. Azevedo and J. G. Cromley, "Does training on self-regulated learning facilitate students' learning with hypermedia?," *J. Educ. Psychol.*, vol. 96, no. 3, pp. 523–535, Sep. 2004, doi: 10.1037/0022-0663.96.3.523.

[12] C. N. Alam and I. Firdaus, "Implementation of Finite State Automata on e-Knows Telegram Chatbot," *CoreID Journal*, vol. 1, no. 1, pp. 33–41, Mar. 2023, doi: 10.60005/coreid.v1i1.3.

[13] Z. Hao, J. Jiang, J. Yu, Z. Liu, and Y. Zhang, "Student-AI Interaction in an LLM-Empowered Learning Environment: A Cluster Analysis of Engagement Profiles," Oct. 2025, Accessed: Apr. 22, 2026. [Online]. Available: http://arxiv.org/abs/2503.01694

[14] W. Ge *et al.*, "SRLAgent: Enhancing Self-Regulated Learning Skills through Gamification and LLM Assistance," Jun. 2025, Accessed: Apr. 22, 2026. [Online]. Available: http://arxiv.org/abs/2506.09968

[15] S. Steinert, K. E. Avila, S. Ruzika, J. Kuhn, and S. Küchemann, "Harnessing Large Language Models to Enhance Self-Regulated Learning via Formative Feedback," *arXiv:2311.13984*, pp. 1–9, 2023, Accessed: Apr. 22, 2026. [Online]. Available: http://arxiv.org/abs/2311.13984

[16] S. Wang *et al.*, "Large Language Models for Education: A Survey and Outlook," Apr. 2024, Accessed: Apr. 22, 2026. [Online]. Available: http://arxiv.org/abs/2403.18105

[17] Z. Sakyoud, A. Aaroud, and K. Akodadi, "Optimization of purchasing business process in Moroccan public universities based on COBIT and artificial intelligence techniques," *Kybernetes*, vol. 53, no. 5, pp. 1607–1635, Feb. 2023, doi: 10.1108/K-02-2022-0167.

[18] T. R. McIntosh *et al.*, "From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models," *Comput. Secur.*, vol. 144, p. 103964, Sep. 2024, doi: 10.1016/J.COSE.2024.103964.

[19] J. van Wyk and R. Rudman, "COBIT 5 compliance: best practices cognitive computing risk assessment and control checklist," *Meditari Accountancy Research*, vol. 27, no. 5, pp. 761–788, Jun. 2019, doi: 10.1108/MEDAR-04-2018-0325.

[20] I. Kirpitsas and T. Pachidis, "KIBO, a new hybrid software development method with enhanced information systems auditing capability," *Inf. Softw. Technol.*, vol. 190, p. 107958, Feb. 2026, doi: 10.1016/J.INFSOF.2025.107958.