Sebatik Vol. 30 No. 1 June 2026
ISSN: 1410-3737(p) 2621-069X(e)

DOI:10.46984/sebatik.v 2 9i1. 2753

Optimizing IT Service Performance Through COBIT 2019-Based Governance Design at Keling Kumang Institute of Technology

Angela. AL [1)], Alva Hendi Muhammadi [2)]

[1, 2]Magister Informatika, Universitas Amikom
[1,2] Jl. Ring Road Utara, Condong Catur, Sleman, Yogyakarta
E-mail: angela.al@students.amikom.ac.id[1)], alva@amikom.ac.id[2)]

ABSTRACT

The Keling Kumang Institute of Technology (ITKK) is a new university in Sekadau Regency, West Kalimantan, which faces challenges in IT management to support academic and managerial operations, including delays in IS and IT infrastructure maintenance, power and internet disruptions, a lack of competent IT human resources , and limited budget and network infrastructure. The complexity of IT services such as SIAKAD, Server and Network Systems, and OJS, requires the implementation of structured IT governance so that IT services run optimally and in line with the institution's vision and mission . This study aims to find weaknesses in IT governance through an analysis of current IT capabilities (as-is) and expected conditions (to-be), as well as to develop recommendations to achieve good governance levels. This study was conducted using the COBIT 2019 framework with 4 process objective domains that have been identified through consultation with ITKK stakeholders and stakeholders, namely APO04, APO07, DSS05, and BAI06. Based on the gap analysis, APO04 has evidence work of product at the Largely Achieved level (50-84%), APO07 has significant challenges in IT HR management with a Not Achieved value (0-49%) at Level 1, DSS05 shows weaknesses in network and endpoint security aspects with a Partially Achieved value (15-49%) at Level 2, and BAI06 requires substantial improvements in IT change management with a Partially Achieved value (15-49%) at all levels. The recommendations provided include the preparation of IT governance policies that are integrated with the ITKK Strategic Plan and VMTS, improving IT HR competency through training and certification, strengthening network security infrastructure, and implementing documented IT change management procedures.

Keywords: COBIT 2019, IT Governance, IT Infrastructure, Capability Level, Gap Analysis

1. INTRODUCTION

In the rapidly developing digital era, the role of information technology (IT) in higher education institutions has become a strategic element that determines operational success and the achievement of academic goals (Ramadhany, et al., 2025; Astika et al., 2025) . Digital transformation in the education sector not only includes the adoption of new technologies, but also requires structured IT governance to ensure that technology investments can provide optimal value for institutions (Ramadhany et al., 2025). The Keling Kumang Institute of Technology (ITKK) as a new higher education institution in Sekadau Regency, West Kalimantan, faces unique challenges in IT management due to its geographical position directly bordering Malaysia and the limitations of existing infrastructure.

ITKK currently operates various complex information systems, including the Academic Information System (SIAKAD), server and network systems, and the Open Journal System (OJS) to support research activities and scientific publications (Jannah et al., 2025). However, the implementation of these systems faces significant operational constraints. Delays in the maintenance of information systems and IT infrastructure, continuous power and internet outages, and a lack of competent human resources (HR) in the IT field are the main problems (Purwani et al., 2025) that hinder the optimization of IT services at ITKK. This condition is exacerbated by budget limitations and inadequate computer network infrastructure to optimally support academic and managerial operations.

IT governance issues in higher education institutions are not only limited to technical aspects, but also include interrelated strategic, tactical, and operational aspects (Wandita NP, 2014). Without a structured IT governance framework, organizations will face high risks of service sustainability, suboptimal information security, and misalignment between business objectives and technology implementation (Kusbandono et al., 2019; Cahyono & Widianti, 2025). Therefore, a systematic approach is needed in designing and implementing IT governance that can accommodate the specific needs of the institution while still referring to standards and best practices that have been proven effective (Zein & Septiani, 2024; Dawis et al., 2025) .

In the context of IT management in higher education institutions, the COBIT (Control Objectives for Information and Related Technologies) framework has been widely recognized as a comprehensive and effective framework (Tafdhilla et al., 2023; Rosyadi, 2024). COBIT

2019, as the latest version of this framework, offers a more flexible and contextual approach than previous versions, taking into account various design factors that allow organizations to customize IT governance according to their unique characteristics (Muksin, 2025; Kusbandono et al., 2019). This framework includes 40 domains divided into five main areas: Evaluate, Direct, Monitor (EDM); Align, Plan, Organize (APO); Build, Acquire, Implement (BAI); Deliver, Service, Support (DSS); and Monitor, Evaluate, Assess (MEA) (Septiawan & Hendrik, nd) .

Several previous studies have demonstrated the effectiveness of implementing COBIT 2019 in the context of higher education institutions. conducted a systematic literature review which showed that the DSS05 domain (Managing Security Services) was the main focus in the implementation of COBIT 2019 in various universities, with varying levels of capability between institutions. In addition, research on IT governance at XY University focused on domains APO04 (Managing Innovation), APO03 (Managing Enterprise Architecture), APO07 (Managing Human Resources), and BAI07 (Managing IT Change Acceptance and Transition), which resulted in specific action recommendations to improve IT governance capabilities (Hendayun, 2017) . In addition, evidence that the implementation of COBIT 2019 in an educational foundation was at the capability level 2, with a focus on domains BAI04, BAI05, and BAI11 can be implemented (Junaidy, 2023) .

However, these studies are limited in their depth of analysis of the specific conditions of newly established higher education institutions facing infrastructure limitations such as ITKK. A subsequent study evaluating the IT governance maturity level at a small higher education institution found that the maturity level was at level 0 (incomplete) with a target of level 2. However, the study did not provide comprehensive guidance for gradually increasing capabilities from a very low initial level (Purwanto & Dirgahayu, 2017) . Furthermore, a 2024 study focused on the APO12 (Managing Risk) domain at the Faculty of Industrial Engineering, XYZ University, demonstrated the importance of mapping accreditation standards with the COBIT 2019 framework, but was limited to a single domain (Prasetya et al., 2021)

This study fills the existing literature gap by designing a comprehensive IT governance at ITKK using the COBIT 2019 framework, focusing on four objective domains that have been identified through an in-depth evaluation process of 40 COBIT 2019 domains and consultation with ITKK stakeholders. The selected domains are APO04 (Managed Innovation) to manage IT innovation to align with institutional strategy, APO07 (Managed Human Resources) to address the challenges of managing competent IT HR, DSS05 (Managed Security Services) to maintain the security of student, staff, and lecturer data, and BAI06 (Managed IT Changes) to manage IT changes systematically without disrupting academic services (Doharma et al., 2021).

The selection of these four domains is based on the results of a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis (Utsalina & Primandari, 2020); Strategis, 2021) conducted to understand the internal and external conditions of ITKK, as well as in-depth discussions with key stakeholders including the ITKK Rector, Vice Rectors I, II, III, and IV, as well as the Head of the IT Subdivision and Information Systems Staff. The SWOT analysis identified that ITKK's strengths lie in management's commitment to improving IT services and the availability of several basic infrastructures, while the main weaknesses include limited competent IT human resources, suboptimal network infrastructure, and poorly documented IT governance procedures. Opportunities that can be exploited include local government support for the development of higher education institutions in border areas and potential collaboration with institutions in Malaysia, while the main threats are competition with other more established higher education institutions and limited operational budgets (Wahidah et al., 2022).

2. SCOPE AND LIMITATION

This research focuses on the design and evaluation of Information Technology (IT) governance at the Keling Kumang Institute of Technology (ITKK) using the COBIT 2019 framework. The main focus of the research is to assess the level of IT governance process capability and design structured recommendations to improve the quality of IT services to align with the institution's strategy and needs.

The scope of this research is limited to the four COBIT 19 domains as follows:

1. APO04 - *Managed Innovation*
2. APO07 - *Managed Human Resources*
3. DSS05 - *Managed Security Services*
4. BAI06 - *Managed IT Changes*

The study evaluated the current (as-is) and expected (to-be) levels of IT process capabilities in the four domains using Capability Maturity COBIT 2019.

This research is expected to provide practical contributions to ITKK in improving the quality of IT services and supporting the achievement of academic goals and institutional management.

3. MATERIAL AND METHOD

This section explains the design and research procedures used to assess and design IT governance at ITKK using the COBIT 2019 framework. The explanation includes the research design, research stages, data collection techniques, and analysis methods applied to evaluate IT process capabilities, identify gaps, and develop recommendations for improving IT governance.

3.1 Research Design

This study uses a descriptive research design with a mixed-methods approach that integrates qualitative and quantitative methods. This approach was chosen to provide a comprehensive analysis of IT governance

conditions at the Keling Kumang Institute of Technology (ITKK). Qualitative methods were used to explore organizational conditions, governance practices, and stakeholder perspectives, while quantitative methods were applied to support the assessment and prioritization of governance objectives. The combination of both methods enables a more complete understanding of the existing IT governance environment.

The study was conducted in 2025 through several stages, including data collection, analysis, evaluation, and recommendation development. This research adopts the COBIT 2019 framework as the primary reference for evaluating and designing IT governance. The framework provides 40 governance and management objectives that can be tailored to organizational needs through the design factors mechanism (ISACA, 2019). In addition, COBIT 2019 offers a structured and flexible approach for aligning IT governance with organizational goals, identifying priority domains, and supporting continuous improvement in governance practices. As a result, the framework serves as an effective tool for assessing current governance conditions and formulating strategic recommendations for ITKK.

3.2 Research Stages

The research was conducted at the Keling Kumang Institute of Technology (ITKK), located in Sekadau Regency, West Kalimantan. The research location was selected based on several strategic considerations:

1. ITKK is a new higher education institution that is developing IT governance,
2. ITKK's geographical position bordering Malaysia provides a unique context for IT management.
3. The limitations of IT infrastructure and human resources at ITKK reflect the challenges faced by many new higher education institutions in Indonesia, particularly in border areas.

This phase aims to understand the initial state of IT governance at ITKK and identify gaps between existing practices and best practices. Observations were made on:

1. IT infrastructure including server rooms, network devices, and physical security systems
2. The information systems in operation include SIAKAD, academic portals, and other supporting systems.
3. IT operational processes include maintenance procedures, change management, and incident handling.
4. Available IT governance documentation such as policies, SOPs, and user guides.

Stakeholders and other relevant users were systematically identified and subsequently mapped based on their respective levels of interest and degree of influence (power) in relation to the implementation and effectiveness of IT governance at ITKK. This mapping process was carried out to ensure a structured and comprehensive understanding of each stakeholder's role, level of involvement, expectations, and potential impact on decision-making processes within IT governance. In addition, the analysis helps in prioritizing stakeholder engagement strategies, enabling the organization to manage relationships more effectively and align IT governance initiatives with stakeholder needs and organizational objectives (Ageng et al, 2025). The results of this identification and mapping are comprehensively illustrated through a stakeholder matrix, which categorizes stakeholders according to their interest influence dynamics, as presented in Table 1 and Table 2.

Table 1. Distribution of Research Subjects

No	Respondent Category	Amount	Percent	Role in Research
1	Rector ITKK	1	3.33%	Strategic validation and domain approval
2	Vice Rector I (Academic)	1	3.33%	Evaluation of academic needs
3	Vice Rector II (Administration)	1	3.33%	Evaluation of administrative needs
4	Vice Rector III (Student Affairs)	1	3.33%	Evaluation of student needs
5	Vice Rector IV (Cooperation)	1	3.33%	Evaluation of cooperation needs
6	Head of Study Program	3	10.00%	Input study program requirements
7	Head of IT Subdivision	1	3.33%	IT operational key informants
8	Information Systems Staff	2	6.67%	SI technical implementer
9	Computer Network Staff	2	6.67%	Technical implementer of infrastructure
10	Lecturer	8	26.67%	Academic system users
11	Educational Personnel	5	16.67%	Administration system users
12	Student	4	13.33%	End users of IT services

Table 1 presents the distribution of research subjects based on respondent categories, proportions, and their roles in the study. The respondents represent multiple organizational levels within ITKK, including strategic, managerial, technical, and end-user perspectives. At the strategic level, the Rector and Vice Rectors (each 3.33%) contribute to validation and evaluation processes. At the managerial level, the Head of Study Program (10.00%) and Head of IT Subdivision (3.33%) provide input on academic and IT operational needs. Technical roles are

represented by Information Systems Staff and Computer Network Staff (each 6.67%) as system implementers. At the user level, Lecturers dominate the sample (26.67%) as primary users of academic systems, followed by Educational Personnel (16.67%) and Students (13.33%) as administrative users and end users of IT services. Overall, the respondent distribution ensures a comprehensive and representative perspective in the research.

Table 2. Stakeholder Interest Matrix

Stakeholder	Level of Importance	Level of Influence	Category	Engagement Strategy
Rector of ITKK	Tall	Tall	Key Player	Intensive consultation and decision validation
Vice Chancellors I-IV	Tall	Tall	Key Player	Regular discussions and decision making
Head of IT Subdivision	Tall	Currently	Keep Informed	Technical coordination and implementation
IT Staff	Tall	Low	Keep Informed	Operational input and feedback
Lecturer	Currently	Low	Monitor	Survey and sampling
Student	Currently	Low	Monitor	Limited survey

Table 2 presents a Stakeholder Interest Matrix designed to guide engagement strategies by assessing the relative importance and influence of various project stakeholders at ITKK. The matrix classifies stakeholders into three primary categories Key Players, those to be kept informed, and those to be monitored allowing project managers to tailor their communication efforts effectively. Key players, such as the Rector of ITKK and the Vice Chancellors, are identified as having high importance and high influence, necessitating intensive consultation and formal decision-making involvement. Conversely, stakeholders with lower influence, such as lecturers and students, are assigned to the monitor category, where engagement is appropriately managed through broader, less resource-intensive methods like surveys and sampling. By aligning communication tactics with these specific stakeholder profiles, the framework ensures that project efforts are prioritized according to the individuals most critical to the project's success (Driya et al., 2021).

Preparation of Research Instruments The research instruments developed consist of:

1. Structured Interview Guidelines Interview guidelines were developed for each stakeholder category with a focus on:
   a. Perceptions of the current state of IT governance
   b. Challenges faced in IT management
   c. Expectations for IT governance development
   d. Priority of necessary repairs .
2. COBIT 2019 40 Domain Evaluation Questionnaire This questionnaire is used to evaluate the suitability of each COBIT 2019 domain to the ITKK needs. The questionnaire structure includes five questions for each domain:
   a. How is this domain applied in ITKK policies and strategies?
   b. Are there any control mechanisms to ensure this domain is running optimally?
   c. How does the organization measure the effectiveness of implementing this domain?
   d. Are there any major challenges in implementing this domain in the ITKK environment?
   e. What is the level of ITKK's compliance with this domain standard?
3. Each question has three assessment components: Availability of evidence of implementation (Yes/No/Not Yet)
   a. Suitability score (1-5)
   b. Level of importance (Low/Medium/High)
4. Capability Level Assessment Questionnaire This questionnaire is based on the Process Capability Model in COBIT 2019 to measure the capability level of each selected domain. The questionnaire structure follows the capability level hierarchy:
   a. Level 0: Incomplete Process
   b. Level 1: Performed Process
   c. Level 2: Managed Process
   d. Level 3: Established Process
   e. Level 4: Predictable Process
   f. Level 5: Optimizing Process

   For each activity in the domain, respondents were asked to rate it on a binary scale:
   a. Yes (1): Activities carried out and done documentation
   b. No (0) : Activities not carried out or not -documented.

3.3 Evaluation of 40 COBIT 2019 Domains

This stage is crucial in determining the domains that will be the focus of IT governance design at ITKK. The evaluation was conducted collaboratively, involving key stakeholders in a series of Focus Group Discussions (FGDs). The FGDs were held in three sessions with different participants and agendas:

1. FGD Session 1: Evaluation of EDM and APO Domains
   Participants: Chancellor, Vice Chancellors I-IV, Head of IT Subdivision Output: Scores and priorities for 18 domains (5 EDM+13 APO).
2. FGD Session 2: Evaluation of BAI and DSS Domains
   Participants: Chancellor, Vice Chancellors I-IV, Head of IT Subdivision, IT Staff
   Output: Scores and priorities for 16 domains (10 BAI + 6 DSS).

3. FGD Session 3: Evaluation of AEC Domains and Priority Setting
   Participants: Chancellor, Vice Chancellors I-IV, Head of IT Subdivision
   Output: Scores for the 6 MEA domains and priority domain determination

Domain Assessment Method Each domain is evaluated using *a scoring system* that considers three dimensions:

1. Suitability Score (SK): Average score of 5 domain evaluation questions (scale 1-5).
2. Importance Level (ISC): Aggregation of importance ratings (Low=1, Medium=2, High=3)
3. Availability of Evidence (AA): Percentage of questions with available evidence.

3.4 SWOT Analysis

Following a quantitative evaluation of 40 domains, a SWOT analysis was conducted to strengthen the selection of priority domains, considering ITKK's internal and external factors. Data for the SWOT analysis was collected through:

1. In-depth interviews with 8 key informants (Chancellor, Vice Chancellors I-IV, Head of IT Subdivision, 2 senior IT staff).
2. Review of ITKK strategic documents (Renstra, Annual Report, Self-Evaluation).
3. Direct observation of IT facilities and operations.

3.5 Questionnaire

The capability level assessment questionnaire was distributed to a targeted group of 30 respondents, all of whom were selected based on their deep technical expertise and comprehensive operational understanding of IT management processes within the ITKK environment. By ensuring that these participants possessed significant institutional knowledge, the data collected from the survey provides a robust and reliable foundation for evaluating the maturity of internal IT practices. Furthermore, the capability level assessment questionnaire for each specific domain was meticulously structured in strict alignment with the Process Capability Model defined by COBIT 2019, which ensures that the benchmarking process adheres to internationally recognized standards for IT governance and management. This rigorous methodological structure is outlined in the following sections, detailing how each domain was systematically analyzed to produce actionable insights regarding the current organizational capability level.

Table 3. Capability Level Assessment Structure

Domain	Level 1	Level 2	Level 3	Level 4	Total Item
APO04	4 item	9 item	15 item	4 item	32 item
APO07	1 item	21 item	13 item	5 item	40 item
DSS05	3 item	30 item	22 item	5 item	60 item
BAI06	3 item	8 item	5 item	5 item	21 item

The table 3 presents the distribution of assessment items across different capability levels for each domain evaluated using the COBIT framework. Each domain, namely APO04, APO07, DSS05, and BAI06, represents a specific IT governance process area being assessed. The capability levels range from Level 1 (Performed), indicating that processes are implemented, to Level 4 (Predictable), where processes are measured and consistently controlled. The number of items in each level reflects the indicators or criteria used to evaluate the maturity of the processes within that domain. For example, the DSS05 domain has the highest number of assessment items, totaling 60, indicating a more detailed evaluation compared to other domains, while BAI06 has the lowest with 21 items. Overall, this table illustrates the composition of assessment indicators used to measure the capability level of each domain, which serves as the basis for determining the overall maturity of IT governance in the study.

Each questionnaire item represents a specific activity in the practice domain that is assessed on a binary scale:

a. Yes (1): Activities are carried out and documented with verifiable evidence.
b. No (0): Activity not implemented, not documented, or no evidence of implementation.

3.6 Capability Level

The capability level calculation follows the Process Assessment Model (PAM) in COBIT 2019 with the following provisions:

1. Achievement Rating for Each Level For each capability level, the percentage of achievement is calculated using the formula:
   Achievement Rating (AR) = (Σ Yes) / (Σ Total Items) × 100%.
2. Classification of Achievement Rating Achievement Rating is categorized into:
   a. N (Not Achieved): 0% - 14% achievement
   b. P (Partially Achieved): 15% - 49% achievement
   c. L (Largely) Achieved): 50% - 84% achievement
   d. F (Fully Achieved): 85% - 100% achievement
3. Determination of Capability Level Domain reaches a capability level if:
   a. The level reaches a minimum rating of L (Largely Achieved)

b. All levels below have reached an F (Fully) rating. Achieved)

3.7 Gap Analysis

This stage aims to identify the gap between the current condition (as-is) and the expected condition (to-be), and determine the priority of necessary improvements.

3.8 Preparation of Recommendations

The recommendations are compiled following the COBIT 2019 framework which includes the enabler dimensions:

1. Processes: Procedures and activities that must be carried out.
2. Organizational Structures: Organizational structure and required roles.
3. Culture, Ethics and Behavior: Work culture and ethics that need to be developed**.**
4. Information: Documentation and knowledge management.
5. Services, Infrastructure and Applications: Supporting infrastructure and applications.
6. People, Skills and Competencies: IT Human Resource Development.

4. DISCUSSION

Furthermore, the selection of these domains reflects the organization's focus on improving several important aspects of IT governance, including strategic planning, human resource management, system security, and implementation processes. These domains were selected because they are closely related to the effectiveness, efficiency, and reliability of IT services within the organization. Effective governance in these areas can support better decision-making, improve operational performance, reduce potential risks, and ensure that IT services align with organizational objectives and user expectations. In addition, these domains also contribute to maintaining service quality and supporting sustainable organizational development in the digital era.

Moreover, the involvement of stakeholders in the domain selection process strengthens the validity and relevance of the research results. By considering input from management, staff, and related users, the selected domains are more representative of actual organizational conditions and challenges faced in daily operations. This collaborative approach helps ensure that the evaluation process is not only theoretically appropriate but also practically applicable to the organization's needs. Therefore, the selected domains provide a strong and reliable foundation for conducting further analysis, identifying existing gaps, and formulating recommendations for continuous improvement in the following sections.

4.1 COBIT Domains

The results of the evaluation of 40 COBIT domains indicate that the selected priority domains are APO04, APO07, DSS05, and BAI06. These domains were determined based on both quantitative and qualitative considerations. Quantitatively, the selection process considered the Total Score of Domain (TSD) obtained from the assessment results. Qualitatively, the selection was strengthened through stakeholder input, organizational priorities, and recommendations from related parties. As a result, several domains categorized as High priority were still selected even though their TSD values did not exceed 3.5, because they were considered important for supporting organizational performance and improving IT governance practices.

In addition, a similar evaluation process was conducted across all 40 COBIT 2019 domains to ensure consistency and comprehensiveness in the assessment. The results of this process produced a complete evaluation matrix, which became the basis for identifying and determining the four priority domains. These selected domains represent important areas from the APO, DSS, and BAI categories that require further analysis and improvement. Therefore, the evaluation results provide a clearer understanding of the organization's current IT governance conditions and support the formulation of appropriate improvement recommendations. The results for the APO domain are presented in Table 4 below.

Table 4 . APO Domain Determination

Domain Code	Name Domain	SK (1-5)	(1-3)	KB (%)	TSD	Priority
APO01	Managing IT Governance Framework	3.2	2.8	60	2.52	Currently
APO02	Managing Strategy	2.8	2.4	40	2.16	Low
APO03	Managing Enterprise Architecture	3.0	2.2	40	2.16	Low
APO04	Managing Innovation	3.6	2.8	60	3.00	Tall
APO05	Managing Portfolio	2.6	2.0	60	1.96	Low
APO06	Managing Budget	2.8	2.4	40	2.16	Currently
APO07	Manage HR	2.8	2.8	40	2.32	Tall *
APO08	Managing Relationships	3.4	2.6	80	2.56	Currently
APO09	Managing Service Agreements	3.2	2.8	60	2.52	Currently
APO10	Managing External Providers	2.6	2.4	60	2.12	Low

APO11	Managing Quality	3.2	2.6	40	2.40	Currently
APO12	Managing Risk	2.0	2.8	40	2.00	Tall*
APO13	Managing Security	3.0	2.8	60	2.56	Currently

Table 4 presents the evaluation results of domains within the COBIT framework, specifically in the APO domain. Each domain is assessed based on the Importance Scale (SK), current condition, and Business Needs (KB), which are combined to produce the Total Score of Domain (TSD). The TSD value is used to determine the priority level of each domain for IT governance improvement.

The results show that APO04 (Managing Innovation) has the highest TSD and is classified as high priority. Other domains, such as APO07 and APO12, are also categorized as high priority based on stakeholder considerations and organizational needs. Meanwhile, domains with lower TSD values are classified as low priority, while moderate scores fall into the current category. Overall, the table shows how domain priorities are determined to support effective IT governance improvement.

4.2 SWOT Analysis

Factor identification can be seen in table 5.

Table 5. SWOT Matrix on IT Governance ITKK

STRENGTHS	WEAKNESSES
S1. Top management commitment to IT development	W1. Limited competent IT human resources (only 3 technical staff)
S2. Availability of basic infrastructure (400 Mbps bandwidth)	W2. Network infrastructure is not optimal (WiFi coverage 60%)
S3. The academic information system is already operational	W3. IT governance procedures are not documented
S4. IT budget is available although limited	W4. There is no dedicated unit for information security.
S5. Strategic location close to Malaysia	W5. IS maintenance is often late (average 3 days)
S6. Local government support for campus development	W6. There is no disaster recovery plan yet
	W7. System documentation is incomplete
	W8. There is no formal change management mechanism.
OPPORTUNITIES	THREATS
O1. Government program for the development of border campuses	T1. Competition with established universities
O2. Potential collaboration with institutions in Malaysia	T2. Annual operational budget limitations
O3. The need for quality human resources in border areas	T3. Frequent power and internet outages
O4. Rapid development of digital technology	T4. Difficulty recruiting qualified IT HR
O5. Digital transformation policy in higher education	T5. High user expectations of IT services
O6. Availability of online training and IT certification	T6. High IT staff turnover
	T7. Increasing cybersecurity threats

Table 5 presents a SWOT analysis based on the COBIT framework to evaluate the current condition of IT governance within the organization. The analysis identifies several strengths, such as management support and the availability of existing IT infrastructure, which support organizational operations and IT service implementation. However, weaknesses were also identified, including limited IT staff, inadequate documentation, and the lack of security planning.

In addition, opportunities arise from government support and the ongoing development of digital transformation initiatives. On the other hand, the organization also faces threats such as increasing competition, budget limitations, and cybersecurity risks that may affect the effectiveness of IT governance implementation.

Table 6. ITKK SWOT Strategy Matrix

Quadrant	Strategy	Related COBIT 2019 Domains
SO (Strengths-Opportunities)		
SO1	Leveraging management commitment and government support to develop IT innovations that support competitive advantage.	APO04 (Managed Innovation)
SO2	Leveraging the availability of online training to improve the competency of existing IT HR	APO07 (Managed Human Resources)
SO3	Developing a robust information security system to support international cooperation	DSS05 (Managed Security Services)
ST (Strengths-Threats)		
ST1	Optimizing IT budget use to build systems that are resilient to infrastructure disruptions	APO06, DSS04
ST2	Leveraging existing information systems to increase efficiency and reduce reliance on IT resources	BAI04, DSS01
ST3	Develop change management procedures to securely manage IT changes.	BAI06 (Managed IT Changes)
WO (Weaknesses-Opportunities)		
WO1	Take advantage of government programs to get IT HR development assistance	APO07 (Managed Human Resources)

WO2	Leveraging cloud technology and managed services to overcome infrastructure limitations	BAI02, DSS01
WO3	Develop IT governance policies and procedures that comply with national standards.	APO01, APO13
	WT (Weaknesses-Threats)	
WT1	Prioritize documentation and process standardization to reduce the risk of HR turnover.	BAI06 (Managed IT Changes)
WT2	Develop a comprehensive IT risk management strategy	APO12 (Managed Risk)
WT3	Building a multi-layered security system to protect against cyber threats	DSS05 (Managed Security Services)

The table 6 presents strategic actions from the SWOT analysis mapped to the COBIT. The SO strategies focus on using strengths to seize opportunities, ST on using strengths to reduce threats, WO on overcoming weaknesses through opportunities, and WT on minimizing weaknesses and avoiding threats. Overall, it shows how each strategy aligns with relevant COBIT domains to improve IT governance.

Table 7. Priority Domain Selection Criteria

No	Criteria	Weight	Description
1	Urgency	30%	How urgently this domain should be implemented
2	Impact	25%	How big is the impact of domain implementation on ITKK operations?
3	Eligibility	20%	How feasible is the implementation of the domain with existing resources?
4	Relatedness	15%	How strong is the domain's relationship to the main problem?
5	Alignment	10%	How aligned is the domain with ITKK strategy?

The table 7 presents weighted criteria used to prioritize domains in the COBIT. Urgency (30%) and Impact (25%) are the main factors, followed by Feasibility (20%), Relatedness (15%), and Alignment (10%). These criteria help determine which domains should be prioritized for implementation.

Table 8. MCDA Results for Domain Selection

Domain	30%	25%	20%	15%	10 %	Total Score	Rank
APO04	8.2	8.5	7.0	8.0	9.0	8.09	2
APO07	9.0	8.0	6.5	9.0	8.5	8.13	1
APO12	7.5	7.0	6.0	7.5	8.0	7.05	6
DSS05	8.5	9.0	7.5	8.5	8.0	8.38	3
BAI06	8.0	8.5	7.0	8.0	7.5	7.95	4
DSS01	7.0	7.5	8.0	7.0	7.0	7.28	5
BAI04	6.5	7.0	6.5	6.5	7.5	6.73	7

The table 8 based on the results of MCDA and discussions with *stakeholders*, four priority domains were determined which will be the focus of IT governance design at ITKK:

1. APO07 - *Managed Human Resources* (Ranking 1).
2. APO04 - *Managed Innovation* (Ranking 2).
3. DSS05 - *Managed Security Services* (Ranking 3).
4. BAI06 - *Managed IT Changes* (Ranking 4).

Although APO12 (*Managed Risk*) scored quite high in the initial evaluation, but this domain was not selected due to resource constraints for simultaneous implementation with the other four domains. Domain APO12 will be a priority in the next implementation phase, but not in this study.

4.3 Capability Level

The Capability Level table can be seen in tables 9, 10, 11 and 12.

Table 9 . APO04 Capability Assessment Results

Capability Level	Number of Items	Yes	No	Rating (%)	Rating Category	Note
Level 0	-	-	-	-	-	The process is not implemented or fails to achieve the goal
Level 1: Performed	4	102	18	85.00%	F	Process implemented and achieved goals
Level 2: Managed	9	159	111	58.89%	L	Process is managed with planning and monitoring
Level 3: Established	15	267	183	59.33%	L	Process defined and documented
Level 4: Predictable	4	56	64	46.67%	P	Process is measured and controlled
Level 5: Optimizing	-	-	-	-	-	Not yet rated

Based on Table 9, the capability assessment of the APO04 domain in the COBIT shows that the process has reached Capability Level 2 (Managed). This conclusion is drawn from the evaluation of each criterion, where Level 1 (Performed) is categorized as Fully Achieved with a score of 85%, indicating that the process has been successfully implemented. Meanwhile, Level 2 (Managed) is categorized as Largely Achieved with a score of 58.89%, showing that the process has been

planned, monitored, and controlled, although not yet fully consistent.

These results indicate that the APO04 processes have been implemented and managed in a structured manner within the organization. Activities such as planning, monitoring, evaluation, and basic control have begun to be carried out systematically to support organizational objectives and improve IT governance effectiveness. This shows that the organization has made efforts to ensure the processes are performed consistently and support operational activities effectively.

However, the processes have not yet reached a fully standardized and optimized stage. Some practices may still be inconsistent, rely on individual implementation, or lack formal documentation and integration between processes. Therefore, APO04 is classified at Capability Level 2, meaning the processes are managed and repeatable but still require improvement in standardization, documentation, and integration to achieve higher capability levels.

Table 10 . APO07 Capability Assessment Results

Capability Level	Items	Yes	No	Rating (%)	Rating Category	Information
Level 0	-	-	-	-	-	Process not executed
Level 1: Performed	1	8	22	26.67%	P	Process partially implemented
Level 2: Managed	21	389	115	77.18%	L	Process managed with planning
Level 3: Established	13	249	71	77.81%	L	Process defined
Level 4: Predictable	5	93	67	58.13%	L	The process is predictable
Level 5: Optimizing	-	-	-	-	-	Not yet rated

Based on the rationale presented in Table 10, the capability assessment of the APO07 domain remains at Capability Level 1 (Performed). The achievement is categorized as Partially Achieved with a score of 26.67%, which is still below the minimum threshold of Largely Achieved (50%) required to progress to the next level. This indicates that the APO07 processes have not yet been implemented consistently and systematically.

The low score shows that several activities related to IT human resource management, such as competency development, training, performance evaluation, and role management, are still not carried out optimally. In addition, documentation, standard procedures, and monitoring mechanisms are still limited, causing process implementation to rely heavily on individual efforts. Therefore, APO07 has not met the requirements to achieve Capability Level 2 and still requires significant improvements to create more structured and controlled processes.

Table 11 . DSS05 Capability Assessment Results

Capability Level	Items	Yes	No	Rating (%)	Rating Category	Information
Level 0	-	-	-	-	-	Process not executed
Level 1: Performed	3	50	40	55.56%	L	Process implemented
Level 2: Managed	30	403	497	44.78%	P	Process not fully managed
Level 3: Established	22	357	303	54.09%	L	Process defined
Level 4: Predictable	5	85	75	53.13%	L	Process can be measured
Level 5: Optimizing	-	-	-	-	-	Not yet rated

Based on the rationalization presented in Table 11, the capability assessment of the DSS05 domain in the COBIT indicates that it is still positioned at Capability Level 1 (Performed). At this level, the achievement for Level 1 has reached the Largely Achieved category with a score of 55.56%, which shows that the basic processes related to security services have been implemented to a certain extent. This means that essential activities, such as basic security controls and operational practices, are already in place and functioning, although their implementation may not yet be fully consistent across all areas.

However, when evaluated at Level 2 (Managed), the achievement is still categorized as Partially Achieved with a score of 44.78%, which is below the minimum threshold required to meet the Largely Achieved or Fully Achieved criteria. This indicates that the processes have not yet been properly managed, monitored, or controlled in a structured and systematic way. Key elements such as formal documentation, standardized procedures, regular evaluation, and performance measurement are still limited or not consistently applied within the organization.

Furthermore, this condition suggests that while security-related activities are already being carried out, they tend to be reactive rather than proactive, and may depend on individual initiatives rather than established organizational standards. The absence of strong governance mechanisms also implies that there is still a risk of inconsistency in implementation, which can affect the overall effectiveness of IT security management.

Therefore, based on these findings, the DSS05 domain remains at Capability Level 1. To progress to Capability Level 2 (Managed), the organization needs to strengthen process management by establishing clear procedures, improving documentation, implementing consistent monitoring and control mechanisms, and ensuring that security practices are applied uniformly. These improvements are essential to achieve more structured, repeatable, and reliable security processes within the organization.

Table 12 . BAI06 Capability Assessment Results

Capability Level	Items	Yes	No	Rating (%)	Rating Category	Information
Level 0	-	-	-	-	-	Process not executed
Level 1: Performed	3	44	46	48.89%	P	Process partially implemented
Level 2: Managed	8	80	160	33.33%	P	The process has not been managed systematically
Level 3: Established	5	46	104	30.67%	P	Process not yet documented
Level 4: Predictable	5	58	92	38.67%	P	The process is not yet measurable
Level 5: Optimizing	-	-	-	-	-	Not yet rated

The table 12 presents results of the capability level assessment based on the COBIT, showing how well processes are implemented and managed across Levels 0 to 5. The evaluation includes several indicators such as the number of assessment items, the number of "Yes" and "No" responses, the percentage score, the rating category, and descriptive information explaining the condition at each level.

At Level 1 (Performed), the process achieves a score of 48.89% and is categorized as Partially Achieved (P), indicating that the process has been implemented but not consistently or completely. Moving to Level 2 (Managed), the score drops to 33.33%, which suggests that the process has not yet been properly planned, monitored, or controlled in a systematic manner. At Level 3 (Established), the score is 30.67%, showing that standardization and formal documentation of processes are still lacking. Similarly, Level 4 (Predictable) has a score of 38.67%, indicating that the process has not yet reached a stage where it can be measured and controlled effectively using defined metrics. Level 0 reflects that processes are not executed, while Level 5 (Optimizing) has not yet been evaluated.

Overall, all assessed levels fall within the Partially Achieved category, highlighting that the organization's processes are still at an early stage of maturity. Although some activities are already being carried out, they are not yet consistent, standardized, or well-managed. This indicates a need for significant improvements, particularly in process management, documentation, monitoring, and performance measurement, in order to achieve higher capability levels and more effective IT governance.

4.4 Capability Level AS-IS

The results on Capability Level as- is can be seen in table 13 as follows:

Table 13. As- Is Capability Level Results (Current)

Domain	Code	Current	Achieve	Level 1 Status	Key Findings
Managed Innovation	APO04	Level 2	85.00%	Fully Achieved	The basic innovation process has been running, but is not yet fully established.
Managed Human Resources	APO07	Level 1	26.67%	Partially Achieved	The IT HR system is not well structured
Managed Security Services	DSS05	Level 1	55.56%	Largely Achieved	Security awareness exists, control implementation is not optimal
Managed T Changes	BAI06	Level 1	48.89%	Partially Achieved	Change management is not documented and consistent

Table 13 presents the capability level assessment of BAI06 in the COBIT. At Level 1 (Performed), the achievement is Partially Achieved with a score of 48.89%, which is below the minimum threshold of Largely Achieved (50%). This indicates that IT change management processes are not yet fully implemented or consistent.

Although some activities already exist, they are still informal and lack standard procedures, documentation, and proper control. Therefore, BAI06 remains at Capability Level 1 and requires improvement to reach a higher level.

4.5 Capability Level To-Be

Based on discussions with stakeholders and by referring to best practices for developing higher education institutions, realistic target capability levels (to-be) are established to be achieved within a three-year period using the COBIT. The target setting process considers several key factors, including the availability of resources such as human resources and technology, the complexity of implementing each domain, and the urgency of improvements based on risk analysis. In addition, alignment with the ITKK development roadmap is also taken into account to ensure that the targets support the institution's long-term strategic direction. Through these considerations, the defined targets are expected to be both achievable and effective in improving overall IT governance. Target setting takes into account:

1. Availability of resources (human resources, technology)
2. Complexity of implementation of each domain
3. Urgency of repair based on risk analysis
4. ITKK development roadmap

Table 14 . Target Capability Level (to-be) and Gap Analysis

Domain	Code	As-Is	To-Be (Year 3)	Gap	Priorities	Effort Estimation
Managed Innovation	APO04	Level 2	Level 4	2 levels	Tall	Currently
Managed Human Resources	APO07	Level 1	Level 4	3 levels	Very high	Tall
Managed Security Services	DSS05	Level 1	Level 4	3 levels	Very high	Tall
Managed IT Changes	BAI06	Level 1	Level 4	3 levels	Very high	Currently

Table 14 presents Level 4 Target Setting (*Predictable) Process*) for all domains is based on:

1. Level 4 is the minimum level for higher education institutions that wish to achieve *good standards. governance* .
2. Level 4 ensures that the process can be measured and controlled quantitatively.
3. Level 4 provides *predictability* in IT services that are critical to academic operations.
4. Achieving Level 4 is in line with the accreditation targets of institutions and study programs.

4.6 GaP Analysis

The GAP analysis in this section aims to identify the differences between the current condition (as-is) and the expected condition (to-be) related to the organization's IT governance performance. This analysis is important for evaluating how well the existing processes and practices align with organizational objectives, operational needs, and established standards such as COBIT. By identifying these gaps, the organization can better understand which processes have not yet achieved the expected capability levels and determine the factors causing the gaps, including limitations in resources, procedures, and process implementation.

In addition, the GAP analysis serves as a basis for determining improvement priorities and developing strategic recommendations to enhance IT governance performance more effectively and systematically. The analysis also supports decision-makers in focusing improvement efforts on the most critical areas that require immediate attention. The results of the analysis for each domain are presented in Tables 15, 16, 17, and 18, which provide comparisons between current achievements and targeted conditions, along with the identified gaps and their implications for each domain.

Table 15. Gap Analysis APO04

Practice	Level	As-Is Achieve	To-Be Target	Gap	Priority	Evidence Gap
APO04.01: Create an environment or innovation	2	62.50%	100%	37.50 %	Tall	Innovation plans are not yet formal, collaboration infrastructure is limited
APO04.02: Maintain enterprise environment	2	76.70%	100%	23.30 %	Currently	Good understanding of business drivers
APO04.03: Monitor technology environment	2	50.00%	100%	50.00 %	Tall	The technology scanning process is not systematic
APO04.04: Assess potential technologies	2-3	56.70%	100%	43.30 %	Tall	Ad-hoc evaluation of new technologies
APO04.05: Recommend initiatives	3	50.00%	100%	50.00 %	Very high	Undocumented proof-of-concept
APO04.06: Monitor innovation implementation	3-4	59.30%	100%	40.70 %	Tall	There is no mechanism for tracking innovation ROI.

The table 15 presents a gap analysis of practices within the APO04 domain in the COBIT, comparing the current condition (as-is) with the expected target (to-be) and identifying the gaps that need to be addressed. Each practice is evaluated based on its current achievement level, the desired target (100%), the resulting gap, priority level, and supporting evidence of the gap.

Overall, the results show that all practices in APO04 still have significant gaps, ranging from 23.30% to 50.00%, indicating that improvements are required to reach the expected capability level. High and very high priorities are mainly found in practices such as monitoring the technology environment (APO04.03), recommending innovation initiatives (APO04.05), and assessing potential technologies (APO04.04), which reflect weaknesses in systematic processes, documentation, and evaluation mechanisms. Meanwhile, APO04.02 has the smallest gap, showing that the organization already has a relatively good understanding of business needs, although further improvement is still necessary.

Table 16. GAP Analysis APO07

Practice	Level	As-Is Achiev	To-Be Target	Gap	Priority	Evidence Gap
APO07.01: Acquire and maintain staff	1-2	72.4%	100%	27.6 %	Tall	The recruitment process is not systematic
APO07.02: Identify key IT personnel	2	68.3%	100%	31.7 %	Tall	There is no succession plan
APO07.03: Maintain skills and competencies	2-3	69.2%	100%	30.8 %	Very high	Unstructured training program
APO07.04: Evaluate employee performance	2-3	90.0%	100%	10.0 %	Currently	The evaluation system is quite good
APO07.05: Plan HR usage	2-3	50.0%	100%	50.0 %	Very high	There is no workforce planning
APO07.06: Manage contract staff	2-3	81.7%	100%	18.3 %	Currently	Contract management is quite good

Table 16 shows that all APO07 practices in the COBIT domain still have gaps between the current condition and the expected targets. The largest gaps are found in APO07.02 and APO07.03, which are related to IT staff identification and competency management. This indicates that the organization still faces challenges in determining appropriate IT personnel requirements, managing competencies, and ensuring that employees possess the necessary skills and knowledge to effectively support organizational objectives and IT-related activities.

Meanwhile, APO07.04 and APO07.06 show relatively smaller gaps compared to other practices, suggesting that several activities related to staff development, training, and performance management have been implemented more effectively. Nevertheless, these practices have not yet reached the expected capability level and still require continuous improvement. Overall, the findings indicate that the organization needs to strengthen IT human resource planning, competency development initiatives, training programs, and performance evaluation processes. Enhancing these areas is essential to improve workforce capabilities, support organizational performance, and ensure more effective and sustainable IT governance implementation.

Table 17. GAP Analysis DSS05

Practice	Level	As-Is Achieve	To-Be Target	Gap	Priority	Evidence Gap
DSS05.01: Protect against malware	2-3	50.0%	100 %	50.0%	Very high	Antivirus does not update automatically on all devices
DSS05.02: Network security management	2-3	23.3 %	100 %	76.7%	Very high	Firewall and IDS are not optimal, many ports are open
DSS05.03: Endpoint security management	2-3	30.0 %	100 %	70.0%	Very high	Endpoint configuration is not secure, no encryption
DSS05.04: Identity and access management	2-3	47.5 %	100 %	52.5%	Very high	Uncontrolled access rights management
DSS05.05: Physical access management	2-3	45.8 %	100 %	54.2%	Tall	Physical access to the server room is not strictly controlled.
DSS05.06: Sensitive documents management	2-3	83.3 %	100 %	16.7%	Currently	Sensitive document management procedures are in place
DSS05.07: Vulnerability and monitoring	2-3	48.8 %	100 %	51.2%	Very high	No routine vulnerability scanning

Table 17 shows that the DSS05 domain still has significant gaps across most practices, with several areas categorized as having high to very high priority levels for improvement. The largest gap is identified in DSS05.02, which relates to network security management. This indicates that the organization's network security controls, monitoring activities, and protection mechanisms are still not implemented optimally. As a result, the organization may face higher risks of unauthorized access, cyberattacks, data breaches, and disruptions to information systems that could affect operational continuity and service reliability.

Other practices, such as malware protection and endpoint security, also show considerable gaps, reflecting weaknesses in system protection, security awareness, and the implementation of security measures within the organization. These conditions suggest that existing security practices are still limited and may not yet fully support the protection of organizational information assets and critical systems. In addition, the lack of comprehensive monitoring and regular security evaluations may reduce the organization's ability to detect and respond to security threats effectively.

Overall, the DSS05 domain highlights that information security remains a critical area requiring immediate

attention and continuous improvement. The organization needs to strengthen security controls, improve monitoring and incident response mechanisms, enhance user awareness regarding cybersecurity, and implement more structured risk mitigation strategies to support effective and sustainable cybersecurity management.

Table 18. GAP Analysis BAI06

Practice	Level	As-Is Achieve	To-Be Target	Gap	Priority	Evidence Gap
BAI06.01 : Evaluate and authorize changes	2-3	30.0%	100%	70.0%	Very high	There is no Change Advisory Board (CAB)
BAI06.02 : Manage emergency changes	2-3	43.3%	100%	56.7%	Very high	Emergency changes are not well documented
BAI06.03 : Track and report change status	4	30.0%	100%	70.0%	Very high	There is no change tracking system
BAI06.04 : Close and document changes	2-3	30.0%	100%	70.0%	Very high	Incomplete change documented

Table 18 shows the results of the GAP analysis in the BAI06 domain show that all practices have significant gaps, with very high priority levels. The largest gaps, reaching 70%, are found in practices related to evaluating and authorizing changes, tracking change status, and documenting changes. These findings indicate that change management processes are still not well established and lack standardization within the organization.

In addition, BAI06.02 (Manage emergency changes) shows a gap of 56.7%, highlighting that emergency changes are not properly documented or controlled. The evidence further reveals several key issues, such as the absence of a Change Advisory Board (CAB), the lack of a formal change tracking system, and incomplete change documentation. These conditions suggest that changes are not managed in a structured and controlled manner, which may increase the risk of system errors or disruptions.

Overall, the BAI06 domain requires significant improvement, particularly in establishing formal change management procedures, improving documentation practices, and implementing proper monitoring and control mechanisms to ensure that all changes are managed effectively and consistently.

4.7 Recommendation

Based on the gap analysis results, the prioritization of improvement needs is carried out using the Risk Impact Assessment Matrix, as presented in Table 19. This matrix is used to identify the priority level of each issue based on its potential impact and risks on organizational performance and IT governance effectiveness. Through this approach, the organization can determine which areas require immediate improvement and allocate resources more effectively.

The assessment uses a scale from 1 to 5, where 1 = Very Low, 2 = Low, 3 = Medium, 4 = High, and 5 = Very High. Higher scores indicate greater risks and higher urgency for improvement. The assessment results provide a basis for determining improvement priorities and formulating recommendations that are aligned with organizational needs and objectives.

Table 19. Risk Impact Assessment Matrix for Prioritization

Gap Area	Likelihood of Risk (1-5)	Impact if Not Addressed (1-5)	Risk Score (L×I)	Priority
DSS05: Network security vulnerability	5	5	25	Critical
DSS05: Endpoint security weaknesses	5	5	25	Critical
BAI06: Uncontrolled IT changes	4	5	20	Critical
APO07: Lack of skilled IT staff	5	4	20	Critical
DSS05: Inadequate access control	4	5	20	Critical
APO07: No succession planning	4	4	16	High
APO04: Unsystematic innovation process	3	4	12	High
BAI06: Poor change documentation	4	3	12	High
DSS05: Limited security awareness	4	3	12	High
APO04: No innovation tracking mechanism	3	3	9	Medium

Table 19 shows based on the results of the gap analysis and prioritization of improvement needs, comprehensive recommendations are prepared to increase the capability level of each domain towards the Level 4 target. The

recommendations are prepared following the COBIT 2019 framework which includes the enabler dimensions:

1. Processes: Procedures and activities that must be carried out
2. Organizational Structures: Organizational structure and required roles
3. Culture, Ethics and Behavior: Work culture and ethics that need to be developed
4. Information: Documentation and knowledge management
5. Services, Infrastructure and Applications: Infrastructure and supporting applications
6. People, Skills and Competencies: IT HR Development

The implementation of the recommendations is designed in a 3-year roadmap with the following phase divisions:

Table 20. ITKK IT Governance Implementation Plan for 3 Years

Phase	Period	Main Focus	Priority Domain	Target Capability Level
Phase 1: Foundation	Year 1 (2025-2026)	Building the foundation of IT governance	APO07, DSS05, BAI06	Level 2
Phase 2: Strengthening	Year 2 (2026-2027)	Strengthening processes and controls	All domains	Level 3
Phase 3: Optimization	Year 3 (2027-2028)	Optimization and continuous improvement	All domains	Level 4

Table 20 shows outlines a three-year roadmap for improving IT governance at ITKK. In Phase 1 (2025–2026), the focus is on building the foundation by prioritizing APO07, DSS05, and BAI06, with a target of Capability Level 2.

In Phase 2 (2026–2027), the organization aims to strengthen processes across all domains and reach Level 3. Finally, Phase 3 (2027–2028) focuses on optimization and continuous improvement, targeting Capability Level 4. This phased plan ensures gradual and structured improvement in IT governance maturity.

5. CONCLUSION

This study shows that the COBIT 2019 framework can be used effectively as a framework for assessing and designing improvements to information technology governance at the Keling Kumang Institute of Technology (ITKK). Measurement results in the APO04, APO07, DSS05, and BAI06 domains show that the current capability level is still at an early to intermediate level, so there is still a significant gap from the expected maturity level.

Key weaknesses were identified in IT human resource management, service security, and change management, potentially hampering the stability and quality of institutional services if not addressed systematically. Through gap analysis and the development of a development roadmap, this study provides a realistic and structured direction for ITKK improvement and can serve as a reference for other universities with similar resource constraints in their efforts to strengthen IT governance sustainably.

6. SUGGESTIONS

ITKK can implement the COBIT 2019-based IT governance development roadmap in stages, with a focus on improving IT human resource competency, strengthening service security, and structured IT change management. Future research can expand the evaluation to other COBIT domains or examine the impact of roadmap implementation on IT service performance.

7. REFERENCES

Ageng, R., Susandy, S., Paramitha, P., Ignatia, S., & Puspita, E. (2025). *Optimalisasi Tata Kelola Sistem Informasi BLUD melalui Evaluasi Tingkat Kematangan Layanan TI*. *4*(01), 50–59. https://doi.org/10.58812/smb.v4i01

Cahyono, Y. D., & Widianti, L. W. (2025). *IMPLEMENTASI TATA KELOLA DAN MANAJEMEN RISIKO TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 2019 (STUDI KASUS : POLITEKNIK ANGKATAN DARAT)*. *9*(1), 250–256.

Dawis, A. M., Rahmayanti, D., Rachman, T., Impron, A., Pius, Y., & Kelen, K. (2025). *PENDEKATAN MODERN DALAM ANALISIS DAN DESAIN TEKNOLOGI INFORMASI*.

Daya, M., Sekolah, S., Kompetensi, D. A. N., Astika, I. K. C., Arthasusila, I. N. A., Ananta, I. G. P., Agus, I. M., Gunawan, O., & Indrawan, G. (2025). *INSERT: Information System and Emerging Technology Journal . Vol. 6, No. 2, Desember 2025 243*. *6*(2), 243–253.

Doharma, R., Prawoto, A. A., & Andry, J. F. (2021). *AUDIT SISTEM INFORMASI MENGGUNAKAN FRAMEWORK COBIT 5 (STUDI KASUS : PT MEDIA CETAK) AUDIT OF INFORMATION SYSTEM USING FRAMEWORK COBIT 5 (CASE STUDY : PT MEDIA CETAK) Perusahaan Media merupakan*. *4*(1), 22–28.

Driya, P. D., Lanang, I. G., Raditra, A., & Ardwi, I. M. (2021). *TEKNIK PENGUMPULAN DATA PADA AUDIT SISTEM INFORMASI DENGAN FRAMEWORK COBIT*. *2*(2), 70–83.

Hendayun, M. (2017). *Tata Kelola Teknologi Informasi pada Perguruan Tinggi Menggunakan Control Objective for Information & Related Technology (COBIT) 5*. *3*(April), 206–216.

Jannah, M., Hidayat, M. F., Almadira, A., Ramadhan, M. R., & Purwani, F. (2025). *Optimalisasi Infrastruktur Teknologi Informasi Dalam Mendukung Layanan Pelanggan Pada Kopi Dari Hati*. *4*(2), 325–333.

Junaidy, M. F. F. (2023). *Audit teknologi informasi dengan menggunakan framework cobit 2019 pada dinas Komunikasi dan Informatika (DISKOMINFO) Kota Malang*. Universitas Islam Negeri Maulana Malik Ibrahim.

Kusbandono, H., Ariyadi, D., & Lestariningsih, T. (2019). *Tata Kelola Teknologi Informasi* (1st ed.). CV. Nata Karya.

Prasetya, R., Muhammad, A. H., & Nasiri, A. (2021). *PERANCANGAN MODEL MANAJEMEN (TATA KELOLA) DATA MENGGUNAKAN DOMAIN APO14 COBIT 2019 STUDI KASUS : FAKULTAS SYARIAH IAIN PONOROGO*. 389–396.

Purwani, F., Febriyana, R., Febyanti, D., Tanjung, I., Raden, U., Palembang, F., Raden, U., Palembang, F., Selatan, S., Raden, U., Palembang, F., Selatan, S., Raden, U., Palembang, F., Selatan, S., Raden, U., Palembang, F., & Selatan, S. (2025). *Halaman Jurnal : https://journal.smartpublisher.id/index.php/jissi OBSERVASI DAN ANALISIS INFRASTRUKTUR TEKNOLOGI INFORMASI (ITI)*. *2*(2), 18–22.

Purwanto, L. A., & Dirgahayu, R. T. (2017). *Pengukuran Tingkat Kematangan Tata Kelola Pengelolaan Permasalahan Sistem Informasi Akademik Menggunakan Framework (Maturity Level Measurement of Governance of Academic Information System Problems Management Using COBIT 4 . 1 Framework)*. *V*(November), 103–113.

Rosyadi, D. B. A. (2024). *EVALUASI KEMATANGAN TEKNOLOGI INFORMASI PELAYANAN AKADEMIK PERGURUAN TINGGI MENGGUNAKAN FRAMEWORK CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT) 2019*. Universitas Islam Negeri Maulana Malik Ibrahim.

Septiawan, E., & Hendrik, B. (n.d.). *Evaluasi Tata Kelola E-Government di Dukcapil Menggunakan Framework COBIT 5 : Analisis Kapabilitas dan Rekomendasi*. *0738*(1), 70–78.

Strategis, P. (2021). *TIPE D DI PROVINSI DKI JAKARTA Erma Handayani dan Adang Bachtiar Universitas Indonesia Diterima : Abstrak Direvisi : Disetujui : Analisa Swot Rsud Sawah Besar Sebagai Rumah Sakit Tipe D Di Provinsi DKI Jakarta Pendahuluan*. *1*(September).

Tafdhilla, A., Iftinan, J. H., Rahmadani, A., & Wulansari, A. (2023). *BULLETIN OF COMPUTER SCIENCE RESEARCH Penilaian Penggunaan Framework COBIT 2019 dalam Pengelolaan Teknologi Informasi Pada Institusi Perguruan Tinggi*. *4*(1), 91–100. https://doi.org/10.47065/bulletincsr.v4i1.314

Utsalina, D. S., & Primandari, L. A. (2020). *Analisis swot dalam penentuan bobot kriteria pada pemilihan strategi pemasaran menggunakan analytic network process*. *14*(1), 51–60.

Wahidah, R. N., Lutfiyana, N., Ramadanti, V. F., Septiyo, P., & Drefiyanto, R. (2022). *AUDIT SISTEM INFORMASI ABSENSI MESIN FINGERPRINT PADA PT . METAL CASTINDO INDUSTRITAMA DENGAN MENGGUNAKAN FRAMEWORK COBIT 5*. *XI*(02), 51–57.

Zein, M. H. M., & Septiani, S. (2024). *DIGITALISASI PEMERINTAHAN DAERAH : Katalis Untuk Integrasi dan Optimasi Good Governance*.