

From Assessment to Improvement: IT Governance Lessons from Indonesian Higher Education Using COBIT 2019

Poppy Buana Mega Putri^{1*}, Muhammad Rifki Shihab², Imairi Eitiveni³

Abstract—This study's objective is to identify capability gaps and provide standardized improvement recommendations to support Indonesian higher education institutions' digital transformation roadmap. It was achieved by measuring the information technology (IT) governance capability levels across all 11 processes within the Build, Acquire, and Implement (BAI) domain of the COBIT 2019 framework in one Indonesian higher education institution. Utilizing a qualitative case study design, data collection involved semi-structured interviews with five purposively sampled key IT stakeholders and a comprehensive review of internal operational documents. Data analysis followed a five-stage protocol, converting qualitative compliance findings into quantitative maturity metrics based on COBIT 2019 scoring criteria. The findings reveal an asymmetric capability landscape in which five processes focusing on requirements, solution building, organizational change, knowledge, and project management achieved the target capability level 3 (Defined). On the other hand, six operational processes failed to meet the benchmark, with four processes stalling at level 2 (Managed) and two at level 1 (Initial) due to a lack of formal standard operating procedures, missing configuration baselines, and severe personnel constraints. These results imply that imposing rigid governance frameworks amid critical resource shortages can induce administrative compliance traps that degrade operational agility. Consequently, the study recommends that resource-constrained public institutions prioritize lightweight, scalable documentation aligned with actual staffing capacity. Lagging process maturity possibly indicates a rational, survival-driven prioritization of immediate operational demands over formal administrative workflows.

Index Terms—IT governance, COBIT 2019, BAI domain, capability level, digital transformation.

I. INTRODUCTION

The role of Information Technology (IT) in higher education institutions has transformed from an operational support function into a critical strategic asset that determines organizational sustainability [1]. This transformation aligns with the Indonesian government's national strategy, which prioritizes digitally based higher education governance, thereby making the performance measurement of IT governance a crucial element [2]. As a higher education institution, EFG University (EFGU) has established efficient, transparent, and principled Good Governance as the university's Key Performance Indicators (KPIs) through its Information Technology Department (which will be called ITD), as formally outlined in the university's strategic IT Master Plan for 2025–2029. The ITD Director has mandated the Control Objectives for Information and Related Technology (COBIT 2019) Level 3 (Defined) as the minimum target for all organizational processes, consistent with broader institutional targets [3], [4].

A historical review of an external audit conducted in 2021 revealed that the overall IT governance performance of ITD remained within the capability range of 0–1, indicating a significant capability gap. This gap directly impacts on IT service delivery within EFGU, which currently faces various operational constraints. These include deploying new applications without business unit authorization, heavy reliance on specific individuals without backup personnel, manual service recovery

Received: 27 April 2026; Revised: 1 June 2026; Accepted: 17 July 2026.

*Corresponding author

¹Poppy Buana Mega Putri, Faculty of Computer Science, University of Indonesia (email: poppy.buana41@ui.ac.id).

²Muhammad Rifki Shihab, Faculty of Computer Science, University of Indonesia (email: shihab@cs.ui.ac.id).

³Imairi Eitiveni, Faculty of Computer Science, University of Indonesia (email: imairi@cs.ui.ac.id).

processes, and inconsistent implementation of Standard Operating Procedures (SOPs).

While the adoption of COBIT 2019 in the education sector is widespread, existing studies predominantly utilize goal cascade, design factor, or focus area approaches. These methodologies shape the evaluation to focus only on a few selected processes within a domain, based on localized problem prioritization. For instance, the goal-cascade study by [5] evaluated only five selected processes within the APO and DSS domains, whereas [6] evaluated nine processes scattered across the EDM, APO, and BAI domains. Similarly, [7] applied design factors, and [8] utilized focus areas to evaluate specific processes across the APO, EDM, BAI, and DSS domains. Taking a different approach, Prabowo et al. [9] conducted a comprehensive domain evaluation of the BAI domain; however, their study was limited to a senior high school context and utilized the older COBIT 5 framework.

Given these precedents and the ITD Director's mandate, there is a lack of research that provides a comprehensive evaluation of a single specific domain using COBIT 2019 in a higher education context. The operational constraints in IT service delivery at ITD map directly to the Build, Acquire, and Implement (BAI) domain of the COBIT 2019 framework. Therefore, this study aims to measure the IT governance capability levels across all processes within the BAI domain using the COBIT 2019 framework. This evaluation aims to provide a holistic overview of the current capability status and improvement recommendations. The outcomes of this evaluation are expected to serve as a strategic foundation for ITD management to mitigate operational risks in IT service delivery, achieve the mandated Level 3 capability target, and fulfill EFGU's organizational KPIs for the 2025–2029 period while simultaneously closing the identified literature gap.

II. RELATED WORK

A. IT Governance Framework

An IT governance framework establishes a systematic approach integrating organizational elements to ensure effective IT utilization aligned

with corporate objectives [10]. Structurally, defining clear roles and responsibilities creates accountability through formal governance bodies, such as steering committees, to oversee strategic alignment. Operationally, structured processes link IT investments directly to business value, utilizing specific metrics for performance assessment and risk mitigation. Furthermore, institutionalized communication systems bridge the IT department and business units, fostering collaborative stakeholder engagement to achieve unified governance [11].

To implement these governance components during digital transformation, organizations frequently adopt international standards, primarily ISO/IEC 38500, ITIL, or COBIT 2019 [12]. However, ensuring service excellence within EFGU's higher education context requires a critical evaluation of each framework's structural relevance and limitations. For instance, while ISO/IEC 38500 effectively guides high-level strategic governance [13], it lacks granular operational capability metrics, fails to support digital transformation, and is insufficiently adaptive to modern technologies such as cloud computing and DevOps [12]. Conversely, ITIL provides actionable, process-level best practices to optimize tactical and operational IT service delivery, such as help desk efficiency and service availability [14]. However, it lacks an overarching governance layer to map investments to strategic goals, fails to capture cloud-native and DevOps environments, and remains too procedural to support digital agility [12].

Addressing these strategic-operational mismatches, COBIT 2019 offers a comprehensive Enterprise Governance of IT (EGIT) framework by clearly mapping out governance from management [10]. Its CMMI-based performance management system quantitatively scores process capabilities from level 0 to 5, serving as a robust diagnostic tool. Although COBIT 2019 faces criticism for lacking contextual adaptability, which requires downstream integration with execution-focused frameworks such as ITIL or PMBOK, its structural relevance to this study remains critical [12]. It provides the rigorous methodology needed to identify capability gaps,

enabling EFGU to transition from a localized 'Managed' state to an institutionalized 'Defined' state, thereby securing its 2025–2029 digital transformation targets.

B. COBIT 2019

The COBIT 2019 framework provides organizations with guidance for overseeing and controlling their information and technology operations. ISACA created this framework as the next step after COBIT 5, introducing seven fundamental elements that organizations need to develop and maintain their governance frameworks. The governance responsibilities of COBIT 2019 need to remain separate from the duties that managers must perform. The board of directors oversees the governance function within the EDM domain. At the same time, organizational leadership and staff members handle management functions across four domains: APO, BAI, DSS, and MEA (Monitor, Evaluate, and Assess) [10].

The current version of the framework provides users with greater flexibility, enabling organizations to adopt it in line with present-day governance requirements and international compliance standards [10]. The COBIT 2019 framework includes a performance management system that follows the Capability Maturity Model Integration (CMMI) framework. The framework establishes specific

instructions through its capability and maturity levels, which range from level 0 to 5, to ensure that IT processes maintain organized, quantifiable characteristics that are subject to ongoing assessment. COBIT 2019 serves as an important guide for implementing governance principles, helping organizations achieve their business objectives while using their resources as efficiently as possible [10].

C. BAI Domain

The BAI domain is a core management area within the COBIT 2019 framework that governs the lifecycle of IT solutions and their integration into business processes. This domain is responsible for transforming strategic requirements defined in the APO domain into operational services and for managing program delivery, solution identification, and organizational transitions [10].

The BAI domain of the COBIT 2019 framework comprises eleven separate processes, which extend the ten processes established in COBIT 5, as summarized in Table 1 [16]. The execution process in this field is particularly important to an agent who brings about transformation. Low capability levels in BAI processes increase the risk that IT projects will fail to meet both user expectations and the university's 2025–2029 strategic targets.

Table 1.
BAI Process Objectives

Process	Objectives	Total Activities
BAI01 – Managed Program	Realize desired business value and reduce the risk of unexpected delays, costs, and value erosion.	28
BAI02 – Managed Requirements Definition	Create optimal solutions that meet enterprise needs while minimizing risk.	15
BAI03 – Managed Solutions Identification and Build	Ensures the agile and scalable delivery of digital products by establishing timely and cost-effective solutions, including technology, business processes, and workflows, that align with the enterprise's strategic and operational objectives.	57
BAI04 – Managed Availability and Capacity	Maintain service availability, manage resources efficiently, and optimize system performance by predicting future performance and capacity requirements.	9
BAI05 – Managed Organizational Change	Prepare and commit stakeholders to business change and reduce the risk of failure.	23
BAI06 – Managed IT Changes	Enable the fast, reliable delivery of change to the business while mitigating the risk of adversely affecting the environment's stability or integrity.	13
BAI07 – Managed IT Change Acceptance and Transitioning	Implement solutions safely and in accordance with agreed expectations and outcomes.	47

Process	Objectives	Total Activities
BAI08 – Managed Knowledge	Provide the knowledge and information required to support staff in the governance and management of enterprise I&T and to enable informed decision-making.	11
BAI09 – Managed Assets	Account for all I&T assets and optimize the value derived from their use.	23
BAI10 – Managed Configuration	Provides sufficient information about service assets to enable effective management, assess the impact of changes, and address service incidents.	11
BAI11 – Managed Projects	Realizes defined project outcomes and maximizes their contribution to the investment portfolio by ensuring the quality of deliverables, improving user involvement to reduce delays and costs, and providing sufficient information about service assets to support effective management and change impact assessment.	46

Table 2.
Previous Research

Author	Organizational Context	COBIT Domain Assessed	Methods	Capability Level Results	Gaps
Febriyani et al. [5]	Higher Education (Indonesia)	- APO02, APO12, APO13 - DSS01, DSS03	Interview	Two processes (APO12, DSS03) are at level 1, while the others are at level 0.	No BAI domain processes are included.
Ishlahuddin et al. [6]	Small-sized Higher Education Institute (XYZ-edu)	- EDM01, EDM02, EDM04 - APO01, APO02, APO04, APO07 - BAI01, BAI02	Interview, questionnaire, and document study	One process (EDM04) is at level 1; the rest are at level 0.	The BAI domain is not the primary focus of the evaluation.
Nugraha & Syaidah [7]	XYZ Polytechnic (a state university)	- EDM02, EDM04 - APO08, APO11, APO13 - BAI01-BAI08, BAI10, BAI11 - DSS03, DSS06	Interview, observation, and questionnaire	Only the DSS domain provides capability-level results; the others are not listed.	Capability assessment results for the BAI domain are unavailable.
Siboro et al. [8]	Educational Institutions	- EDM03 - APO12, APO13 - BAI06 - DSS05	Descriptive qualitative study	None of the processes achieved the target capability level of 4.	The BAI domain is not the primary focus of the evaluation.
Prabowo et al. [9]	Senior High School	- BAI01-BAI10)	Qualitative (interview and literature study) & quantitative (questionnaire)	The BAI domain reaches level 3.93.	No detailed evaluation was performed for the activities in the BAI domain.
Pratama & Umaroh [17]	Higher Education (Bandung)	BAI09	Interview, questionnaire, and observation	The capability level is 2.46 against a target of 3.	The evaluation is restricted to a single BAI domain.
Afiani et al. [18]	Higher Education (XYZ University)	BAI09	Interview & observation	3 activities within the BAI09 process have reached the target, while the remaining 2 have not.	The evaluation is restricted to a single BAI domain.
Fauzi et al. [19]	Higher Education (XYZ University)	APO07	Interview	One activity failed to achieve the target capability level of 2.	No BAI domain processes are included.

D. Capability Level

The capability level assessment in this study follows the COBIT Performance Management (CPM) model, which is based on the CMMI concept. This model provides a structured framework for measuring how well a process operates and achieves its objectives. The assessment uses a scale from level 0 to 5, where each level represents an increasing degree of process refinement and sophistication. The

criteria for each capability level are defined in Table 3 [10]. In the COBIT 2019 assessment framework, a process capability level is determined by the fulfillment of specific attributes and indicators. To reach a certain level, all attributes at that level and lower levels must generally achieve the category of Fully Achieved or Largely Achieved. This structured measurement enables gap analysis, which compares the current state of IT capability with the target level defined by the organization's strategic vision.

Table 3.
COBIT 2019 Process Capability Levels

Level	Name	Description
0	Incomplete	The process is not implemented or fails to achieve its basic purpose, characterized by a lack of understanding of basic practices.
1	Initial	The process achieves its objectives through a limited set of actions that are preliminary or intuitive rather than structured.
2	Managed	The process achieves its objectives by executing a complete set of basic tasks that are documented and tracked as completed.
3	Defined	The process is performed in a more structured manner, using organizational assets, and is generally well-defined.
4	Quantitative	The process for achieving objectives is clearly defined, and its performance is quantitatively measured and controlled.
5	Optimizing	The process is fully defined, and its performance is systematically evaluated to support continuous improvement.

E. Previous Research

Prior studies have utilized COBIT to evaluate IT governance across various educational institutions. As summarized in Table 2, prior work frequently overlooks or limits evaluation of the BAI domain. Several researchers excluded BAI from their scope [5], [19], while others focused strictly on isolated processes such as BAI09 [17], [18], or omitted granular, activity-level data [7], [9]. Furthermore, even when evaluated, BAI processes failed to meet target capability levels [8]. This persistent gap leaves a vulnerability in educational IT governance research. By providing a direct capability measurement across the BAI domain within the ITD EFGU context, this research successfully bridges the empirical gaps identified in the literature and establishes a new contribution.

III. RESEARCH METHOD

A. Data Sources

This study draws on both primary and secondary data sources. Primary data were gathered through semi-structured, in-depth interviews conducted with five key respondents from ITD EFGU. Participants were selected via purposive sampling for their capacity to provide richly textured information relevant to the phenomenon under investigation [20]. This deliberate approach ensures that each

participant possesses the necessary authority, technical competence, and direct accountability to assess the BAI domain [21] meaningfully. Each respondent serves as either a process owner or a subject-matter expert with hands-on responsibility for managing IT program lifecycles, asset procurement, and system transitions within the university. These individuals are the most knowledgeable and capable of representing ITD EFGU [22]. By bringing together senior decision-makers and specialized IT professionals, the study achieves data triangulation, capturing both the strategic and operational dimensions of IT governance. The profiles of these stakeholders, along with their respective interview topics, are presented in Table 4.

Table 4.
List of Research Respondents

No	Position	Interview Topic
1	Director of ITD	Identification of research problems.
2	Head of IT Planning and Policy	Identification of research problems and activities related to IT governance in the BAI domain.
3	Head of IT Infrastructure	Activities related to IT Infrastructure in the BAI domain.
4	Application Development & Integration Specialist	Activities related to the system development process within the BAI domain.
5	IT Governance & Security Specialist	Activities related to IT Governance in the BAI domain.

Secondary data were collected through internal document reviews and a comprehensive literature study. Internal operational documentation from ITD EFGU served as empirical evidence to verify whether actual field practices align with the COBIT 2019 framework. This was supplemented by a literature review consisting of academic journals, textbooks, and scientific publications on IT governance evaluation to reinforce the theoretical foundation of the assessment.

B. Data Analysis and Capability Assessment Procedure

The qualitative data obtained from the semi-structured interviews and internal document reviews were analyzed using a systematic, five-stage sequential protocol designed to convert empirical

field findings into measurable capability assessment matrices. The process began with interview transcript coding, in which verbal recordings were transcribed verbatim and manually coded to map key stakeholder insights directly to the corresponding process activity indicators within the COBIT 2019 framework. An activity fulfillment mapping stage followed this to evaluate the implementation of the core governance items. To convert these qualitative mappings into quantitative metrics, a percentage calculation was executed based on the completeness of objective documentary evidence. The resulting metrics informed the level-assignment stage, in which capability achievements were verified against established category thresholds. Finally, the procedure concluded with a gap-determination analysis to identify operational deficiencies and formulate strategic governance recommendations.

When conducting activity fulfillment mapping, the researchers evaluated the explicit execution of 283 total activities distributed across the 11 processes of the BAI domain [16]. The structural distribution of these operational assessment items across each core process is detailed in Table 1.

To transition from qualitative observations to a structured quantitative assessment, the percentage calculation phase utilized the formal rating methods established by the COBIT 2019 guidance. Each mapped activity was assigned a specific percentage score determined entirely by the availability and maturity of supporting documentary evidence. The structural hierarchy of the BAI domain dictates that each process contains multiple sub-processes, each sub-process is mapped to a distinct capability level, and each capability level comprises a specific set of operational activities. The quantitative rating calculation sequence begins by determining and assigning a subjective value to each activity, guided by the baseline criteria established in Table 5. Following this step, the activity value for each specific level is obtained by calculating the arithmetic meaning of the Activity Subjective Values within that same target level and sub-process. If a process contains more than one sub-process, this calculation is executed independently for each sub-process.

Table 5.
Scoring Scale and Criteria

Category	Percentage Score	Objective Evidence and Compliance Criteria
Not achieved (N)	10%	The activity has not been performed or initiated by the organization.
Partially achieved (P)	25%	The activity is performed verbally or informally but lacks supporting operational documentation.
Largely achieved (L)	75%	The activity is executed systematically but is supported by incomplete or draft-state documentation.
Fully achieved (F)	100%	The activity is executed thoroughly and is backed by finalized, authorized documentary evidence.

To calculate the overall capability, score for an entire process, the sub-processes are first grouped according to their respective capability levels. Once properly grouped, the previously calculated level-specific values for each sub-process are input into the dataset. The final capability value for that targeted level is then determined by averaging the scores of all sub-processes operating at that level. If the final assessment score at a specific level satisfies the thresholds for either the largely achieved (L) or fully achieved (F) categories, that capability level is formally designated as successfully achieved. Meeting this threshold is a strict procedural prerequisite, allowing the evaluation sequence to advance to the next, higher level of capability [6].

The assessment concluded with the gap determination phase, which compared the verified current capability levels against the ITD EFGU management team's level 3 target capability benchmark. Fulfilling level 3 indicates that the organization successfully operates its IT governance and management processes through institutionalized, structured, and completely documented standard operating procedures. The identified variances between the verified current state and the target state provided the empirical foundation for generating evidence-based recommendations tailored to support ITD EFGU's digital transformation roadmap for the 2025–2029 strategic period.

C. Data Validity

To ensure the objectivity, reliability, and validity of the qualitative capability assessment, this study employed a dual-layer validation strategy comprising method/source triangulation and respondent member checking. The credibility of the

primary data was reinforced by cross-checking interviewees' verbal assertions against empirical evidence from ITD EFGU's internal operational documents, including standard operating procedures (SOPs), terms of reference (TOR/KAK), user acceptance test (UAT) logs, and periodic project performance updates. For instance, the fulfillment of staff training activities in BAI05.04 was validated through official internal memoranda requesting approval of training budgets from the Directorate of Human Resources and Talent Development. Physical asset distribution within BAI07.06 was verified through signed Handover Certificates (*Berita Acara Serah Terima*, or BAST), and project execution tracking within BAI11.02 was checked against authenticated Weekly Reports that documented iterative progress percentages.

To minimize subjective bias and resolve information discrepancies or differences of opinion among stakeholders, the evaluation strictly adhered to the highest level of documentary compliance. If a respondent verbally claimed an activity was functional. However, if no consistent operational documentation could be retrieved to support the claim, the activity score was capped at 25% to reflect the organization's documented state rather than subjective verbal impressions.

Once the preliminary evaluation draft was complete, a formal member-checking process was conducted. The initial capability assessment findings were presented back to the ITD EFGU team during a collaborative validation forum. This feedback loop allowed respondents to review the evaluation instruments, submit formal counterarguments, and provide new documentary evidence that may have been previously overlooked. Any adjustments to the final capability scores were made based on this consensus, ensuring an accurate, objective, and institutionally verified outcome.

IV. RESULT AND DISCUSSION

A. Capability Level Result

The researchers measured all process capabilities using the COBIT 2019 framework after selecting the prioritized processes requiring improvement. The

framework evaluates fulfillment percentages by assessing designated activities required at each capability level. For the BAI01 process, the framework establishes the assessment starting points at level 2 because it lacks defined activities between levels 0 and 1. The assessment results showed that the process achieved a 55% fulfillment score at level 2, indicating it was largely achieved, and a 39% fulfillment score at level 3, indicating it was partially achieved. The researchers determined that the BAI01 process achieved level 2 (managed) because its level 2 fulfillment met the minimum requirements for a largely achieved rating. In contrast, its level 3 fulfillment did not meet the same standards. The results indicate that the process has not yet met the organization's level 3 (defined) target, as it can only deliver basic, non-standardized outcomes.

The overall results of the capability-level evaluation of the prioritized BAI domain processes at the ITD are summarized in Table 6. The assessment shows that the organization needs to improve its IT governance capability because six evaluated processes failed to meet their target capability requirements of level 3. The 11 processes were assessed, 2 processes (BAI04, BAI10) achieved level 1 while 4 processes (BAI01, BAI06, BAI07, BAI09) reached level 2 and 5 processes (BAI02, BAI03, BAI05, BAI08, BAI11) attained level 3.

The absence of formal documentation and SOP restricts ITD to Level 1 for BAI04 and BAI10. BAI04 (managed availability and capacity) remained at level 1, with fulfillment scores of 25% (Partially Achieved) at level 2 and 50% (Partially Achieved) at level 3, as capacity evaluations rely solely on informal discussions. The head of IT Infrastructure noted, "*The lack of strict enforcement of incident management SOPs and absence of formal capacity planning documents make service mitigation efforts sporadic and poorly documented.*" Similarly, BAI10 (Managed Configuration) was constrained to level 1, scoring only 12% (not achieved) at level 2 and 30% (partially achieved) at level 3. Configuration activities lack formal documentation and verification against approved requests. Regarding this, the Head of IT Infrastructure stated, "*The absence of formal*

documentation for configuration baselines and lack of a change verification mechanism indicate that our configuration asset management is not yet properly standardized."

Low strategic integration and poor standardization in initiative and change management stagnated BAI01 and BAI06 at capability level 2. While BAI01 achieved 55% (largely achieved) at level 2, its progress stalled at level 3 with a 39% (partially achieved) score because IT initiative management operated strictly at the project level, lacking program-level resources and coordinated budgeting. The Head of IT Planning & Policy confirmed, *"The lack of a standardized approach in program management means that cross-project coordination and the measurement of business value from our digital transformation outcomes cannot yet be formally documented or monitored."* Similarly, BAI06 (Managed IT Changes) reached 70% (largely achieved) at level 2 but dropped to 37% (partially achieved) at level 3, plagued by a lack of CMDB configuration mapping and missing external SLAs. The Head of IT Infrastructure noted that emergency access rights are rarely reviewed after use. At the same time, an IT Specialist added that the absence of CMDB mapping severely hinders accurate asset impact analysis.

Incomplete formal documentation and a lack of lifecycle oversight stagnated BAI07 and BAI09 at capability level 2. BAI07 (Managed IT Change Acceptance and Transitioning) reached 81% (largely achieved) at level 2 but dropped to 47% (partially achieved) at level 3 due to transition phases lacking rollback plans and post-implementation review (PIR) reports. The IT Governance & Security Specialist highlighted that *"The absence of an audit trail of test results and the failure to update contingency documents makes it difficult to track accountability for changes."* At the same time, the Application Development & Integration Specialist noted, *"A deficiency in handover standardization is revealed when automated distribution is missing and business owners do not formally authorize UAT results."* Similarly, BAI09 (Managed Assets) achieved 75% (largely achieved) at level 2 but scored only 38% (partially achieved) at level 3 due to weak licensing controls and inventory gaps. The Head of IT Infrastructure explained that *"Asset traceability is compromised by the absence of archived*

procurement records and formal remote access approvals," and the Head of IT Planning & Policy emphasized, *"The lack of a comprehensive asset review process hinders our ability to ensure asset alignment with business needs and cost optimization opportunities."*

Conversely, ITD's system development lifecycle and project management processes achieved standardized level 3 capability across BAI02, BAI03, and BAI11. Specifically, BAI02 (Managed Requirements Definition) secured 71% at level 2 and 75% at level 3; BAI03 (Managed Solutions Identification and Build) reached 64% at Level 2 and 51% at level 3; and BAI11 (Managed Projects) scored 82% at level 2 and 65% at level 3. ITD relies on formal terms of reference (TORs) to establish requirements, which are validated during user acceptance testing (UAT). The Head of IT Planning & Policy stated, *"Feature implementation and system configurations now reflect responses to identified risks. These are executed strictly within the agreed contract scope to guarantee the integrity of the developed solutions."* Solution selection and procurement occur within separate staging environments, validating the organization's commitment to standardized methods. The Head of IT Infrastructure noted, *"The selection of development methodologies and the availability of the service catalog have been formally established to support the organization's strategic goals."* Continual control of all activities is based on the TOR as a baseline, as the IT Governance & Security Specialist stated, *"The consistent application of Change and Risk Management SOPs ensures that every deviation is appropriately documented and mitigated."* The Application Development & Integration Specialist added, *"The handover process through the Minutes of Transfer and Acceptance documents, which involves independent user verification, ensures that project outcomes meet quality standards and business requirements."*

Achieving level 3 in processes BAI05 (Managed Organizational Change) and BAI08 (Managed Knowledge) further demonstrates ITD's maturity in managing human factors and information assets. Process BAI05 scored 68% at level 2 and 61% at level 3 (both largely achieved), while BAI08 performed strongly with 82% at level 2 (largely achieved) and 90% at level 3 (fully achieved). This

organizational transformation was sustained by leadership commitment through quick-win strategies and KPI alignment. The Head of IT Planning & Policy remarked, *"The achievement of the change vision is now secured through organizational KPI alignment and comprehensive operational planning. This ensures the sustainable adoption of a digital culture."* This maturity was further supported by systematic knowledge management through technical documentation and knowledge repository SOPs governing information classification and access control. The Head of IT Planning & Policy added, *"Knowledge user identification is now formally conducted to reduce dependency on specific individuals. This ensures that both public and internal information can be securely distributed through the organization's designated platforms."* By reaching level 3 across these five processes, ITD now has well-defined, standardized procedures documented throughout the organization, successfully ensuring long-term operational consistency.

B. Gap Analysis

The IT Governance program aims to increase IT capability and strengthen controls to levels appropriate for each business unit, prioritized [10]. To support this improvement, a gap analysis is conducted to determine how current capabilities align with the desired objectives. The target capability level is determined by examining the organization's strategic plan, internal environmental observations at ITD, and stakeholder expectations regarding the implementation of COBIT 2019 processes.

Based on interviews with ITD leadership, the target capability level has been set at level 3 for all measured processes. The visualization in Figure 1 shows that multiple processes need improvement to

meet the established benchmark. Table 6 shows that five processes reached level 3 (defined), but there exists a significant gap for all other processes. BAI04 and BAI10 maintain their status at level 1 (Initial), and BAI01, BAI06, BAI07, and BAI09 remain at level 2 (Managed). The gap analysis shows that organizations require additional standardization and formalization processes to achieve their goal of bringing all high-priority processes to the Defined State.

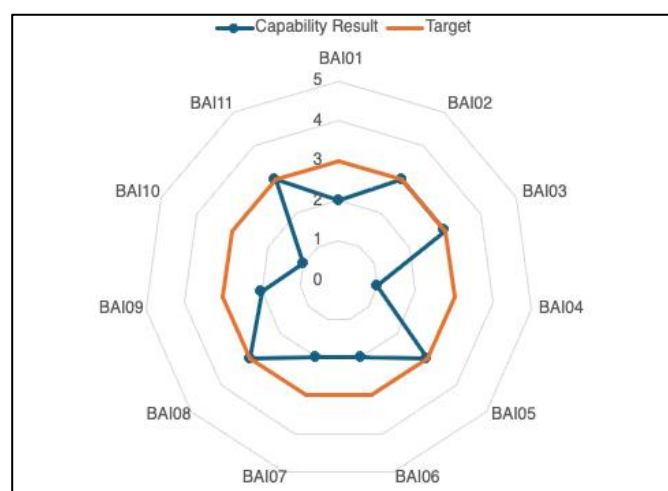


Fig. 1. Gap analysis.

C. Recommendation for Improvement

Process improvement recommendations are developed based on the activities defined by COBIT 2019 to address capability targets that have not yet been achieved. Based on the capability level calculations, six COBIT 2019 processes within the BAI domain at ITD have not yet met the established Level 3 target. These processes include BAI01, BAI04, BAI06, BAI07, BAI09, and BAI10. Detailed recommendations, together with the relevant international standards and implementation strategies, are summarized in Table 7.

Table 6.
Capability Level

Process	Capability Target	Score (Category)		Final Level
		Level 2	Level 3	
BAI01 – Managed Program	Level 3	55% (L)	39% (P)	Level 2
BAI02 – Managed Requirements Definition	Level 3	71% (L)	75% (L)	Level 3
BAI03 – Managed Solutions Identification and Build	Level 3	64% (L)	51% (L)	Level 3

Process	Capability Target	Score (Category)		Final Level
		Level 2	Level 3	
BAI04 – Managed Availability and Capacity	Level 3	25% (P)	50% (P)	Level 1
BAI05 – Managed Organizational Change	Level 3	68% (L)	61% (L)	Level 3
BAI06 – Managed IT Changes	Level 3	70% (L)	37% (P)	Level 2
BAI07 – Managed IT Change Acceptance and Transitioning	Level 3	81% (L)	47% (P)	Level 2
BAI08 – Managed Knowledge	Level 3	82% (L)	90% (F)	Level 3
BAI09 – Managed Assets	Level 3	75% (L)	38% (P)	Level 2
BAI10 – Managed Configuration	Level 3	12% (N)	30% (P)	Level 1
BAI11 – Managed Projects	Level 3	82% (L)	65% (L)	Level 3

Table 7.
Recommendations

Process	Final Level	Key Evidence	Gaps	Priority Actions (Recommendation)	Best Practice
BAI01 – Managed Program	Level 2	- ITD Organization Structure - IT Master Plan 2025 - Application development SOP	- Operations are fragmented at the project level, lacking cross-unit integration. - Missing formal Program Manager, integrated Charter, Business Case, and Benefits Register.	- Create a Program Methodology SOP - Appoint a Program Manager and develop formal Program Charters for the 15 strategic priorities. - Build a centralized Benefits Register and Executive Dashboard.	PMBOK– Program Management [23]
BAI04 – Managed Availability and Capacity	Level 1	- Incident Management SOP - Incident Monitoring Report June 2025 - Service Catalog 2025	- Lacks a formal Capacity & Performance Plan. - Infrastructure resource monitoring is partial and ad-hoc. - Capacity incidents are escalated via WhatsApp instead of a formal log system, causing delays >24 hours.	- Draft a Capacity & Performance Plan aligned with ITIL 4 / ISO 20000. - Formalize the Service Catalog with business-criticality metrics for IT services. - Require system monitoring registration (Libre/Grafana) in the server provisioning SOP.	- ITIL V4 – Capacity & Performance Management [14] - ISO/IEC 20000-1:2018 – IT Service Management [24] - NIST SP 800-137: Information System Continuous Monitoring [25]
BAI06 – Managed IT Changes	Level 2	- Change Management SOP - User Manual - Technical Proposal	- Lacks a Configuration Management Database (CMDB), forcing manual impact analysis of infrastructure changes on business processes. - Missing post-incident log control and verification for Emergency Access Requests. - BCP document updates are excluded from the major release workflow.	- Integrate mandatory Configuration Item (CI) attribute fields into the Change Request (CR) form. - Mandate a Post-Event Log Review within 1 day (T+1) after emergency access is revoked. - Add change freeze periods and change success rate metrics into vendor SLAs.	- ISO/IEC 20000-1:2018 – IT Service Management [24] - NIST SP 800-53 – Security and Privacy Controls for Information Systems and Organizations [26] - ITIL V4 – Supplier Management [14]
BAI07 – Managed IT Change Acceptance and Transitioning	Level 2	- Application development SOP - Backup and Restore Management SOP	- Lacks written Deployment Plans (runbooks) and rollback strategies. - Missing regular reports for	- Mandate minute-by-minute technical Deployment Plans and data recovery runbooks. - Use test management tools	- ITIL V4 –Release Management [14]

Process	Final Level	Key Evidence	Gaps	Priority Actions (Recommendation)	Best Practice
		- System Integration Test (SIT) & User Acceptance Test (UAT)	formal security testing, stress tests, and automated script testing. - Absence of Post-Implementation Review (PIR) documentation.	(TestRail) to archive historical test assets. - Make the PIR a mandatory requirement to close out project administration.	- ISO/IEC/IEEE 29119-3:2021 – <i>Test Documentation</i> [27] - ISO/IEC 20000-1:2018 – <i>IT Service Management</i> [24] - ISO/IEC 55001:2024 – <i>Asset Management</i> [28] - ISO/IEC 19770-1:2017 – <i>IT Asset Management</i> [29] - ISO 10007:2017 – <i>Guideline for Configuration Management</i> [30] - ITIL V4 – <i>Service Configuration Management</i> [14]
BAI09 – Managed Assets	Level 2	- Data & Application Disposal SOP - Access Right Management SOP - IT Asset List	- Asset inventory practices are inconsistent across units. - IT inventory data is not synchronized with physical assets and university financial records. - Missing Effective License Position reports and asset portfolio value reviews.	- Conduct regular asset reconciliations - Digitalize and centralize asset handover certificates (BAST). - Draft an Effective License Position Report.	
BAI10 – Managed Configuration	Level 1	- Change Management SOP - IT Master Plan 2025 - Weekly Report	- Lacks a Configuration Management Plan (CMP) and CMDB database. - Dependencies between infrastructure components, databases, and applications are unmapped. - Missing regular verification mechanisms to reconcile production logs with formal CR tickets.	- Design a CMP formally agreed upon by Infrastructure and Development teams. - Establish standard CI class hierarchies and mandatory naming conventions. - Execute routine weekly configuration audits.	

Specific recommendations were formulated by aligning the identified organizational gaps with international best practices to support the transition from a managed or initial state to a defined state. For BAI01, the recommendation focuses on standardizing program management methodologies and roles in accordance with PMBOK standards [23]. Improvements for BAI04, BAI06, and BAI07 draw on ITIL V4 [14], NIST SP 800-137 [25], NIST SP 800-53 [26], ISO/IEC/IEEE 29119-3:2021 [27], and ISO/IEC 20000-1:2018 [24] to strengthen service availability management and change transition practices. For BAI09 and BAI10, the strategy involves implementing centralized repositories and formal verification procedures guided by ITIL V4, ISO/IEC 55001:2024 [28], ISO/IEC 19770-1 [29], and ISO 10007:2017 [30]. These measures are intended to elevate each process capability to the target level 3 (Defined), ensuring that IT processes

are standardized and consistently documented across the institution.

D. Discussion

The evaluation results show that IT governance at the ITD EFGU remains inconsistent, as most assessed processes do not meet the institutional target of capability level 3 (Defined). The organization has established standard procedures that cover application development requirements definition and project management activities. The organization has reached the initial stages of development for both service capacity management and configuration management because it lacks established written rules. The pattern shows that EFGU identifies as technologically competent but needs to improve its operational systems management because of weak procedures and poor documentation standards.

The disparity between IT processes that successfully attain maturity level 3 and those lagging at level 1 in higher education institutions possibly stems from the visibility of their outcomes and their immediate impact on KPIs. Processes such as managed requirements definition (BAI02) and managed solution identification and build (BAI03) reach level 3 because they yield highly visible results and dictate project viability. Conversely, managed availability and capacity (BAI04) and managed configuration (BAI10) operate as background infrastructure services whose performance organizations take for granted during seamless operations. As the theory of invisible work states, stakeholders typically notice infrastructure processes only when a systemic failure occurs [31]. Consequently, institutions fall into a firefighting trap, in which proactive processes consistently lose out in competitions for resource allocation to initiatives that generate immediate outputs. Organizations overlook and fail to reward individuals who design capacity and prevent system downtime because crises never happen. Recognition arrives only when they resolve an active disruption [32].

This asymmetric landscape reflects an unbalanced organizational ambidexterity, in which an institution channels its collective energy into exploratory activities to secure prestige in digital innovation while neglecting exploitative tasks such as configuration management [33]. This imbalance aligns with the concepts of Bimodal IT and Dual-Speed Governance, in which organizations deliberately or unconsciously bifurcate the speeds of their IT evolution [34], [35]. Driven by external stakeholder pressures, such as digital transformation mandates from rectorates or ministries, institutions accelerate their innovation efforts to achieve high levels of maturity. Meanwhile, core operational layers stall at primitive stages because management misperceives basic governance as a bureaucratic hindrance [10]. From an institutional theory perspective, localized, informal practices mean that these lagging-field activities remain stuck in the habitualization phase [36]. Transitioning to Level 3 requires an objectification phase driven by formal codification and SOPs [36]. The absence of formal documentation creates a discrepancy between performative capabilities (actual field practices) and ostensive capabilities (the regulatory-bound

institutional understanding) [37]. This discrepancy validates the critique that maturity models frequently suffer from administrative formalism bias [38]. Assessment frameworks penalize organizations that execute practical processes effectively simply because they lack an administrative paper trail, thereby transforming documentation into an artificial bottleneck for IT maturity evaluations.

Large-scale governance frameworks such as COBIT 2019 and CMMI impose unrealistic expectations on higher education IT units operating under resource constraints. Administrative overhead is the primary catalyst for governance failure, diverting productive hours that staff would otherwise allocate to operational problem-solving [39]. The investigated institution clearly exhibits this capacity imbalance, with the ITD operating with only 35 personnel, compared to the 190 stated in the IT Master Plan. Under such constraints, enforcing rigid documentation standards triggers goal displacement [40], [41]. Formal instruments like COBIT Level 3 SOPs mutate into primary goals, forcing the IT unit to marginalize its fundamental mandate: delivering excellent operational services to students and faculty. This compliance trap ultimately degrades actual organizational performance [42]. The audit pressures of COBIT 2019 generate what Power in 1999 defined as rituals of verification, inducing an artificial busyness revolving around the manufacture of paper trails to appease external auditors [42]. This bureaucratic drain exhausts the cognitive and operational capacity of the IT staff, paralyzing their daily responsiveness and agility. Therefore, a lack of formal documentation at level 3 may not signify a failure of governance, but a logical resistance and a survival mechanism adopted by an organization navigating severe structural limitations.

E. Limitations

Several limitations in this study should be acknowledged. First, due to resource constraints and institutional positioning, primary data collection was limited to interviews with five key individuals who are directly responsible for the targeted IT processes. Other personnel within EFGU were excluded because they function strictly as operational executors and lack a strategic, high-level view of enterprise IT governance. Second, this study did not utilize the COBIT 2019 Goal Cascade or Design

Factors to filter priorities or adjust capability targets. This approach was bypassed because ITD required a comprehensive, all-inclusive assessment across the entire BAI domain. Finally, to maintain a well-defined research scope, this study did not formulate a highly detailed or organizationally validated implementation roadmap. Instead, the final output focuses strictly on delivering specific action items for individual process activities that fell short.

V. CONCLUSION

The assessment revealed an asymmetric capability landscape where five project and organizational change processes achieved capability level 3 (Defined). In contrast, six core operational processes stalled at levels 1 and 2 due to a lack of formal documentation, standardized SOPs, and configuration baselines. These findings imply that higher education IT departments must look beyond process execution to institutionalize documentation actively. However, because this institution operates with only 35 of its 190 planned personnel, enforcing rigid frameworks risks compliance traps and operational paralysis. Management should instead prioritize lightweight, scalable governance documentation aligned with actual staffing capacity.

This study conceptualizes how severe resource constraints shape the adoption of frameworks in public institutions. While existing literature often blames organizational resistance or poor design for low maturity scores, this study demonstrates that lagging maturity reflects a rational, survival-driven prioritization of immediate operational demands over administrative formalism. By linking COBIT metrics with institutional theory and the "invisible work" concept, we show that bottlenecks are institutional and resource-dependent rather than merely technical.

Limitations include a small primary dataset limited to five strategic personnel, which excluded insights from operational executors, as well as the omission of the COBIT 2019 Goal Cascade. To address these gaps, future research should gather perspectives directly from ground-level practitioners

and executors. Additionally, researchers should conduct longitudinal case studies using periodic evaluations over an extended timeframe to track how resource-constrained institutions gradually evolve to meet COBIT demands.

REFERENCES

- [1] A. Wibowo, *Revolusi Industri 4.0 dan Society 5.0*. Semarang: Yayasan Prima Agus Teknik, 2023.
- [2] M. Nashrullah, S. Rahman, A. Majid, N. Hariyati, and B. Budiyo, "Transformasi digital dalam pendidikan Indonesia: Analisis kebijakan dan implikasinya terhadap kualitas pembelajaran," *Mudir: Jurnal Manajemen Pendidikan*, vol. 7, no. 1, pp. 52–59, Jan. 2025, doi: 10.55352/mudir.v7i1.1290.
- [3] A. S. Bimantoro and R. Jayadi, "IT governance measurement using COBIT 5 for evaluating IT project management aspect: Case study of insurance company," *Journal of System and Management Sciences*, vol. 12, no. 6, pp. 315–333, Dec. 2022, doi: 10.33168/JSMS.2022.0620.
- [4] T. Wulyatiningsih and J. Y. Mambu, "IT governance maturity and business alignment: A COBIT 2019 evaluation at RSUD ODSK," *International Journal of Engineering, Science and Information Technology*, vol. 5, no. 2, pp. 248–255, Mar. 2025, doi: 10.52088/ijesty.v5i2.822.
- [5] W. Febriyani, F. R. Hendrawan, and T. F. Kusumasari, "Advancing towards IT maturity governance excellence: COBIT 2019 in higher education (Indonesia)," in *2023 Eighth International Conference on Informatics and Computing (ICIC)*, IEEE, Dec. 2023, pp. 1–6. doi: 10.1109/ICIC60109.2023.10382082.
- [6] A. Ishlahuddin, P. W. Handayani, K. Hammi, and F. Azzahro, "Analysing IT governance maturity level using COBIT 2019 framework: A case study of small size higher education institute (XYZ-edu)," in *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)*, IEEE, Sep. 2020, pp. 236–241. doi: 10.1109/IC2IE50715.2020.9274599.
- [7] R. A. Nugraha and R. Syaiah, "Smart campus governance design for XYZ polytechnic based on COBIT 2019," *International Journal on Informatics Visualization*, vol. 6, no. 3, pp. 718–725, Sep. 2022, doi: 10.30630/ijov.6.3.1257.
- [8] I. N. A. P. Siboro, J. Siallagan, A. Purba, L. Ambarita, S. Nggebu, and Lasino, "Evaluation of information security governance in educational institutions using the COBIT 5 framework," in *2024 6th International Conference on Cybernetics and Intelligent System (ICORIS)*, IEEE, Nov. 2024, pp. 1–6. doi: 10.1109/ICORIS63540.2024.10903958.
- [9] Y. D. Prabowo, E. Fernando, and J. Gate, "Evaluation of IT governance with BAI domain at senior high school using Cobit 5," in *2023 International Conference on Information Management and Technology (ICIMTech)*, IEEE, Aug. 2023, pp. 01–06. doi: 10.1109/ICIMTech59029.2023.10277731.
- [10] ISACA, *COBIT 2019: Introduction and Methodology*. ISACA, 2018.
- [11] P. Kwak and R. I. Desanti, "IT governance evaluation using COBIT 2019 framework in a manufacturing company," in *2023 7th International Conference on New Media Studies (CONMEDIA)*, IEEE, Dec. 2023, pp. 62–67. doi: 10.1109/CONMEDIA60526.2023.10428517.
- [12] B. S. Yulistiawan, R. Widyastuti, R. O. Mulianingtyas, G. P. R. Ariono, and H. T. Sihotang, "Developing the adaptive digital IT governance framework for next-generation IT governance," *MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 25, no. 1, pp. 97–112, Nov. 2025, doi: 10.30812/matrik.v25i1.5628.
- [13] M. Ayat and S. Shafiee, "Developing a comprehensive IT governance framework for Iranian hospitals: a fuzzy Delphi approach," *International Journal of Health Governance*, vol. 30, no. 4, pp. 410–421, Nov. 2025, doi: 10.1108/IJHG-03-2025-0027.
- [14] A. Budiman and Y. F. A. Lubis, "Perbandingan framework COBIT 2019 dan ITIL 4 dalam tata kelola teknologi informasi," *Jurnal Ilmu Komputer*

- dan *Teknik Informatika*, vol. 1, no. 2, pp. 52–57, Jul. 2025, doi: 10.64803/juikti.v1i2.50.
- [15] ISACA, *COBIT 2019: Governance and Management Objectives*. ISACA, 2018.
- [16] R. Y. Pratama and S. Umaroh, “An IT asset governance model design using COBIT 2019 and ITIL V4 framework at BKU itenas,” *E3S Web of Conferences*, vol. 484, Art. no. 02006, Feb. 2024, doi: 10.1051/e3sconf/202448402006.
- [17] M. S. Afiani, M. Lubis, A. F. Santoso, and M. F. Safitra, “Aligning IT asset management at XYZ university with infocom standard and COBIT 2019 BAI09 domain: Assessment and design,” in *Proceedings of the 2023 9th International Conference on Industrial and Business Engineering*, New York, NY, USA: ACM, Sep. 2023, pp. 537–544. doi: 10.1145/3629378.3629444.
- [18] M. S. Fauzi, M. Lubis, L. Abdurrahman, F. S. Lubis, and H. Fakhurroja, “Optimizing IT human capital: Evaluating and crafting an innovative management system with COBIT 2019,” in *Proceedings of the 2023 9th International Conference on Industrial and Business Engineering*, New York, NY, USA: ACM, Sep. 2023, pp. 545–550. doi: 10.1145/3629378.3629445.
- [19] K. Vasileiou, J. Barnett, S. Thorpe, and T. Young, “Characterising and justifying sample size sufficiency in interview-based studies: Systematic analysis of qualitative health research over a 15-year period,” *BMC Med. Res. Methodol.*, vol. 18, no. 1, pp. 1–18, Dec. 2018, doi: 10.1186/s12874-018-0594-7.
- [20] J. W. Creswell and J. D. Creswell, *Research Design*, 5th ed. SAGE, 2017.
- [21] A. Moser and I. Korstjens, “Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis,” *European Journal of General Practice*, vol. 24, no. 1, pp. 9–18, Jan. 2018, doi: 10.1080/13814788.2017.1375091.
- [22] Project Management Institute, *The Standard for Program Management*, 5th ed. Project Management Institute, 2024.
- [23] G. M. Khan *et al.*, “Complex outsourcing relationships management model,” *Journal of Software: Evolution and Process*, vol. 37, no. 1, Jan. 2025, doi: 10.1002/smr.2724.
- [24] S. K. Sahu, “Incident response and security monitoring,” in *Building Secure PHP Applications*, Berkeley, CA: Apress, 2024, pp. 347–388. doi: 10.1007/979-8-8688-0932-3_7.
- [25] R. Quinlan, A. Brinister, T. Macdonald, and A. White, “Securing ATE using the DoD’s risk management framework,” in *2022 IEEE AUTOTESTCON*, IEEE, Aug. 2022, pp. 1–6. doi: 10.1109/AUTOTESTCON47462.2022.9984778.
- [26] M. Ilman and C. A. Anwar, “Analysis and quality assurance testing on Alpha97 landing page based on ISO/IEC/IEEE 29119 international standard,” *Journal of Information Systems and Business Technology*, vol. 1, no. 4, pp. 101–106, Dec. 2025, [Online]. Available: <https://journal.jci.co.id/jisbt/article/view/259>
- [27] Y. Gerek and M. N. Aydin, “Management frameworks and management system standards in the context of integration and unification: A review and classification of core building blocks for consilience,” *Systems*, vol. 13, no. 4, pp. 234–267, Mar. 2025, doi: 10.3390/systems13040234.
- [28] A. Falkiewicz, “Education of IT students in the field of IT management practices and software asset management in framework of IT studies at academic level,” *Journal of Education, Health and Sport*, vol. 8, no. 11, pp. 718–736, Nov. 2018, [Online]. Available: <https://apcz.umk.pl/JEHS/article/view/6773>
- [29] L. English, A. Yunusa-Kaltungo, M. Kidd, and A. Labib, “Development of a complementary framework for implementing asset register solutions,” *Engineering Reports*, vol. 4, no. 6, Art. no. e12493, Jun. 2022, doi: 10.1023/A:1008651105359.
- [30] S. L. Star and A. Strauss, “Layers of silence, arenas of voice: The ecology of visible and invisible work,” *Computer Supported Cooperative Work (CSCW)*, vol. 8, no. 1–2, pp. 9–30, Mar. 1999, doi: 10.1002/eng2.12493.
- [31] N. P. Repenning and J. D. Sterman, “Nobody ever gets credit for fixing problems that never happened: creating and sustaining process improvement,” *IEEE Engineering Management Review*, vol. 30, no. 4, pp. 64–64, 2002, doi: 10.1109/EMR.2002.1167285.
- [32] C. A. O’Reilly and M. Tushman, “Organizational ambidexterity: Past, present and future,” *SSRN Electronic Journal*, vol. 27, no. 4, pp. 324–338, 2013, doi: 10.2139/ssrn.2285704.
- [33] M. Acharya and R. Thakurta, “Digital transformation in organisations - a review and research agenda,” *Int. J. Bus. Inf. Syst.*, vol. 51, no. 2, pp. 212–251, 2026, doi: 10.1504/IJBIS.2026.151691.
- [34] M. Hamidi, S. Ghazinoori, M. Naghizadeh, and N. Bagheri-Moghaddam, “Digital transformation as a technological innovation system: diversity of policy instruments in the lifecycle of upstream oil and gas technologies,” *Technol. Anal. Strateg. Manag.*, pp. 1–16, Jul. 2025, doi: 10.1080/09537325.2025.2509241.
- [35] P. S. Tolbert and L. G. Zucker, “The institutionalization of institutional theory,” in *Studying Organization: Theory & Method*, London, UK: SAGE Publications, 1999, pp. 169–184. doi: 10.4135/9781446218556.n6.
- [36] M. S. Feldman and B. T. Pentland, “Reconceptualizing organizational routines as a source of flexibility and change,” *Adm. Sci. Q.*, vol. 48, no. 1, pp. 94–118, Mar. 2003, doi: 10.2307/3556620.
- [37] J. Poeppelbuss, B. Niehaves, A. Simons, and J. Becker, “Maturity models in information systems research: Literature search and analysis,” *Communications of the Association for Information Systems*, vol. 29, no. 1, pp. 491–502, 2011, doi: 10.17705/1CAIS.02927.
- [38] M. Staples, M. Niazi, R. Jeffery, A. Abrahams, P. Byatt, and R. Murphy, “An exploratory study of why organizations do not adopt CMMI,” *Journal of Systems and Software*, vol. 80, no. 6, pp. 883–895, Jun. 2007, doi: 10.1016/j.jss.2006.09.008.
- [39] K. J. Meier and M. A. Calderon, “Goal displacement and the protection of human subjects: The view from public administration,” *Political Science and Politics*, vol. 49, no. 2, pp. 294–298, Apr. 2016, doi: 10.1017/S1049096516000238.
- [40] R. K. Merton, “Bureaucratic structure and personality,” *Social Forces*, vol. 18, no. 4, pp. 560–568, May 1940, doi: 10.2307/2570634.
- [41] M. Power, *The Audit Society*. Oxford University Press, 1999. doi: 10.1093/acprof:oso/9780198296034.001.0001.