Journal of Software Engineering, Information and Communication Technology (SEICT)

Journal homepage: https://ejournal.upi.edu/index.php/SEICT

COBIT 2019-Based IT Governance Maturity Assessment in Airport Services Provider

Ozmar Azhari[1], M. Fauzi Isputrawan[2], Francka Sakti Lee[3], Hendriyana[4], Parman Suparman[5]*

[1-3]Fakultas Teknologi dan Desain, Universitas Bunda Mulia, Indonesia
[4]Program Doktor Ilmu Komputer, Universitas Bina Nusantara, Indonesia
[5]Fakultas Sains dan Teknologi, Universitas Panca Sakti, Indonesia
Correspondence: E-mail: l1582@lecturer.ubm.ac.id

ABSTRACT

Information Technology (IT) plays a key role in supporting company goals and performance at PT XYZ, an airport services provider, was established in 2024 through merger process. Implementing the right strategy in IT governance is crucial to ensure IT processes align with business objectives in the regulated public service sector. The COBIT 2019 Framework was applied, outlining 14 Governance and Management Objectives (GAMO) across EDM, APO, BAI, DSS, and MEA domains. 13 design factors related to company objectives were used. COBIT 2019 Design Toolkit results show average maturity level 3.13 (Defined) with critical gaps in BAI04 (2.82), BAI06 (2.82), and DSS05 (2.96). These recommendations are supported by COBIT 2019, CMMI, and ISO/IEC 38500 frameworks to enhance governance effectiveness, improve operational reliability, and support sustainable IT service excellence.

ARTICLE INFO

Article History:
Submitted/Received
30 December 2025
First Revised 19 February 2026
Accepted 26 February 2026
First Available online
27 February 2026
Publication Date 01 June 2026

Keyword:
Airport Service Technology;
Capability Level 3;
COBIT 2019;
GAMO Domains;
IT Governance Maturity.

1. INTRODUCTION

Information Technology (IT) has become a critical enabler of business objectives and organizational performance across industries, including airport service, where digital systems underpin passenger processing, baggage handling operations, ground handling coordination, facility management, security screening, and regulatory compliance reporting (Tambunan et al., 2025). In such a safety-critical and highly regulated environment, airport service providers increasingly depend on reliable, secure, and well-governed IT services to ensure seamless passenger processing, baggage handling efficiency, operational coordination among airlines/ground handlers/airport authorities/regulators, and real-time compliance reporting (Harison & Lahav, 2024; Majdalawieh & Khan, 2022; Sudarsono, Cornelius, et al., 2023). Consequently, IT can no longer be treated merely as a supporting function; it must be governed and managed as an integral part of corporate governance and risk management to ensure that every IT initiative delivers measurable value, supports safety objectives, and complies with stringent industry regulations (Skačkauskienė & Leonavičiūtė, 2025). However, the implementation of these technologies must be approached with caution, as the critical nature of airport services demands a robust framework to ensure compliance with security standards and ethical considerations surrounding data privacy (Petrin et al., 2025; Sudarsono, Ananda, et al., 2023). As such, organizations must prioritize transparency and accountability in their IT governance strategies to foster trust among stakeholders and effectively navigate the complexities introduced by these digital innovations.

PT XYZ, an airport service provider company recently established through a 2024 merger process, operates in a complex ecosystem where IT systems support key processes such as ground handling coordination, facility maintenance, procurement, security screening, and biometric data management. Despite substantial technology investments, the organization still developing comprehensive IT governance faces critical challenges including fragmented policy documentation, reactive change/incident handling during peak traffic, limited security control traceability across multi-vendor systems, and inconsistent IT-business alignment focused on throughput maximization and service compliance. These conditions create substantial risks related to passenger processing disruptions, non-compliance with security and data protection regulations, operational inefficiencies during peak hours, and potential negative impacts on passenger safety experience and airline stakeholder satisfaction (Berrada et al., 2023; Charolina et al., 2024). This situation also indicates the need for a structured and measurable approach to assess and improve IT governance maturity in the organization (Simatupang & Adrianto, 2024). To address these challenges effectively, PT XYZ must adopt a comprehensive IT governance framework that not only aligns with industry standards but also enhances operational resilience and stakeholder confidence.

COBIT 2019 has emerged as a widely recognized framework for designing and assessing enterprise IT governance and management (Yusuf et al., 2024). The framework structures governance and management objectives into domains such as Evaluate, Direct and Monitor (EDM), Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS), and Monitor, Evaluate and Assess (MEA), and introduces design factors and focus areas to tailor governance systems to specific organizational contexts (Kwak & Desanti, 2023). While previous studies have demonstrated the applicability of COBIT 2019 in

DOI: https://doi.org/10.17509/seict.v7i1.95229
p-ISSN 2774-1656 | e-ISSN 2774-1699

banking, government, and education sectors (Kwak & Desanti, 2023; Yusuf et al., 2024) empirical research focusing on airport service companies, particularly those providing integrated airport operations technology services remains relatively limited. Moreover, there is a lack of studies that explicitly connect COBIT 2019 maturity assessment results with enterprise goals and design factors in a safety-critical environment such as airport services, where operational disruptions concern of the regulatory compliance and multi-stakeholder coordination consequences.

This research addresses these gaps by assessing the IT governance maturity level of PT XYZ using COBIT 2019 across 14 Governance and Management Objectives (GAMO), while considering relevant design factors and enterprise goals of a services company. The study aims to answer the following questions: (1) What is the current maturity level of IT governance and management processes at PT XYZ based on COBIT 2019? (2) What gaps exist between the current maturity and the targeted level required to support business objectives and regulatory demands in the sector? (3) What improvement roadmap can be proposed to enhance IT governance maturity in a structured and realistic manner? By focusing on both capability levels and evidence completeness (policies, procedures, and operational artefacts), the study provides a holistic view of the organization's strengths and weaknesses.

This study contributes to the IT governance literature by extending the application of the COBIT 2019 framework to the airport services provider industry, a safety-critical and highly regulated environment that has received limited empirical attention. Unlike prior studies focused on banking, government, or education sectors, this research highlights the unique governance requirements of airport service operations, particularly in ensuring service continuity, security, and regulatory compliance. Moreover, this study integrates COBIT 2019 design factors, capability maturity assessment, and evidence-based gap analysis to provide a more comprehensive evaluation of IT governance maturity. The findings also demonstrate how COBIT 2019 can be used not only to assess current maturity levels but also to develop a structured governance improvement roadmap. This contributes to the theoretical understanding of COBIT 2019 as a practical and adaptable framework for governance capability development in high-reliability service environments.

2. METHODS

This research employs a systematic, iterative IT Maturity Level assessment methodology aligned with COBIT 2019 best practices, specifically designed for airport services provider industry where unique challenges appear especially during operation in complying the regulatory, 24/7 service reliability, and safety-critical operation to support the operation and services.

The methodology comprises six sequential phases spanning 3 months of implementation, utilizing mixed methods including document analysis, structured interviews across three iterations, which include 84 days total, direct process observations, and quantitative capability scoring to ensure triangulation and validity. The following sections detail the methodology as depicted in Figure 1.

DOI: https://doi.org/10.17509/seict.v7i1.95229
p-ISSN 2774-1656 | e-ISSN 2774-1699

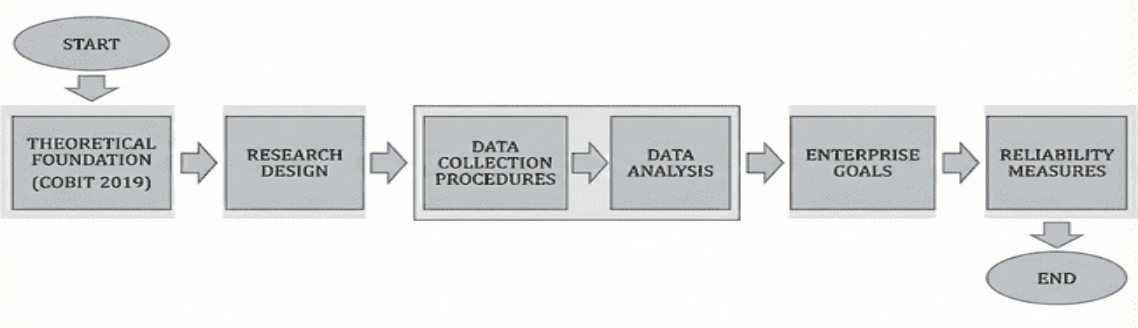

Figure 1. Research Design Method Flow

As shown in Figure 1, the research begins by establishing the theoretical foundation based on the COBIT 2019 framework as the basis for evaluating IT governance maturity. This is followed by the research design stage, where the assessment scope, selected GAMO, and methodology are defined. Data collection is then conducted through interviews, document analysis, and process observations to obtain governance evidence. The collected data are analysed using COBIT 2019 capability level criteria to determine maturity levels and identify governance gaps. The results are subsequently aligned with enterprise goals to ensure support for organizational objectives and service continuity. Finally, reliability is ensured through triangulation and cross-verification to maintain the accuracy and credibility of the assessment.

2.1. COBIT 2019 Framework Overview

One of the top approaches for enterprise IT governance and management is COBIT 2019. The framework has developed into a more comprehensive and integrated system for monitoring IT management and governance procedures. The Governance System and Governance Framework are the two fundamental principles categories that form the basis of COBIT 2019 (Lompoliu & William Tangka, 2024).

Among the tenets of the governance system are: 1. Providing value to stakeholders; 2. Taking a holistic approach; 3. Creating a dynamic governance system; 4. Distinguishing governance from management; 5. Adapting to enterprise needs; and 6. Meeting end-to-end enterprise needs. The principles of the Governance Framework include: 1. Designed for Openness and Adaptability; 2. Based on a Conceptual Model; and 3. Harmonized with Leading Standards.

2.2 Research Design and Scope

This study adopts a single-case study design with mixed methods approach, combining quantitative capability maturity scoring and qualitative gap analysis to evaluate PT XYZ's IT governance progression and elevate the score of maturity level.

The assessment comprehensively evaluates six COBIT governance enablers: processes, organizational structures, information flows, people competencies, policies/procedures, and service-infrastructure-applications, tailored to specific priorities like 99.9% service availability, regulatory compliance, and safety continuity (Asriannoor, 2024; Charolina et al., 2024). This evaluation ensures that each enabler is effectively aligned with the

DOI: https://doi.org/10.17509/seict.v7i1.95229
p-ISSN 2774-1656 | e-ISSN 2774-1699

organization's goals and objectives (Ciptaningtyas et al., 2024). By doing so, it enhances overall governance and helps in achieving optimal performance across various domains.

2.3 Data Collection

Data collection and analysis followed a rigorous, multi-phase methodology spanning utilizing mixed methods to ensure triangulation and validity for PT XYZ's IT governance assessment (Novrian et al., 2025).

Phase 1: Kick-off & Preparation established a joint assessment team with PT XYZ stakeholders and external consultants, finalizing scope across 14 GAMO domains, deploying the COBIT 2019 Design Toolkit, and approving protocols for interviews, observations, and capability scoring.

Phase 2: Iterative Data Collection employed three cycles: Iteration 1 conducted initial IT/non-IT interviews, process observations, and 26 Standard Operational Procedure (SOP) inventory; Iteration 2 deepened insights via expanded interviews and preliminary SOP validation; Iteration 3 finalized evidence with scope adjustment, from 26 to 17 processes.

Phase 3: Gap Analysis & Maturity Scoring applied quantitative COBIT indicators, where can be divided into several categories such as Fully Achieved, Largely Achieved, Partially Achieved, to compute domain capability levels.

The analysis was obtained from integrated thematic coding from interview transcripts, document completeness ratios, and observation findings, validated through stakeholder review for specific reliability.

2.4 Data Analysis

The data analysis comprises three steps: Quantitative analysis focused on systematic capability level calculations across each of the 14 Governance and Management Objectives (GAMO) domains using COBIT 2019's standardized maturity indicators, complemented by comprehensive document completeness ratios derived from 1,370 ideal evidence requirements spanning policies, procedures, templates, and operational artifacts essential for IT governance validation, alongside activity achievement percentages encompassing all 191 process activities categorized into Fully Achieved, Largely Achieved, and Partially Achieved levels to establish precise baseline maturity metrics and identify performance distribution patterns across critical domains such as service availability and security services (Fianty & Brian, 2023).

Qualitative analysis employed rigorous thematic coding and content analysis of extensive interview transcripts compiled from three iterative stakeholder engagement cycles involving IT and non-IT personnel, combined with detailed process observation field notes documenting real-time operational workflows, followed by systematic gap identification through multi-source data triangulation that cross-referenced diverse stakeholder perspectives, documented procedures, and observed practices to uncover underlying root causes of maturity deficiencies, including reactive change management approaches and inconsistent security control implementation particularly vital for 24/7 service continuity (Yusuf et al., 2024).

Validation procedures implemented multiple layers of methodological rigor, including exhaustive cross-verification of all collected documents against the complete spectrum of

DOI: https://doi.org/10.17509/seict.v7i1.95229
p-ISSN 2774-1656 | e-ISSN 2774-1699

1,370 ideal evidence requirements, inter-rater reliability assessments conducted by independent dual assessors for capability level scoring consistency, formal stakeholder confirmation workshops facilitated with designated Process Owners (PICs) for finding validation and contextual accuracy, and comprehensive audit trail documentation maintaining full traceability from raw evidence through analytical outputs, thereby ensuring the credibility, reproducibility, and practical applicability of assessment results for PT XYZ's specific IT governance improvement roadmap (Sudarsono, Ananda, et al., 2023).

2.5 Enterprise Goals

This study operationalized COBIT 2019 through a comprehensive maturity assessment targeting progression from Level 2.0 (Managed—process-focused but reactive) to Level 3.1 (Defined—standardized and documented), evaluating six governance enablers: processes, organizational structures, information flow, people competencies, policies/procedures, and service-infrastructure-applications (COBIT 2019 Framework Governance and Management Objectives, 2019).

The assessment focused specifically on 14 strategically selected Governance and Management Objectives (GAMO) that align with organization's priorities such as operational reliability, regulatory compliance, and safety continuity (Primaditama et al., 2025). These GAMO span five core domains, which contain of:

1. Evaluate, Direct, and Monitor (EDM) with EDM03 Managed Risk Optimisation for executive oversight of IT-related enterprise risks.
2. Align, Plan, and Organize (APO) including APO02 Managed Strategy (IT-business alignment), APO09 Managed Service Agreements (SLA enforcement), APO10 Managed Vendors (third-party risk), and APO12 Managed Risk (proactive threat mitigation).
3. Build, Acquire, and Implement (BAI) covering BAI02 Managed Requirements Definition (traceable needs), BAI03 Managed Solution Identification and Build (fit-for-purpose development), BAI04 Managed Availability and Capacity (service continuity), BAI06 Managed IT Changes (controlled modifications), and BAI11 Managed Projects (delivery assurance);
4. Deliver, Service, and Support (DSS) encompassing DSS01 Managed Operations (daily stability), DSS02 Managed Service Requests and Incidents (rapid recovery), and DSS05 Managed Security Services (access controls);
5. Monitor, Evaluate, and Assess (MEA) with MEA01 Managed Performance and Conformance (KPI tracking and audits).

2.6 Validity & Reliability Measures

Methodological validity and reliability were rigorously ensured through a multi-layered validation framework comprising complementary techniques that collectively minimized bias, enhanced credibility, and guaranteed the robustness of findings for PT XYZ's IT governance assessment (Fraga et al., 2024; Skačkauskienė & Leonavičiūtė, 2025), where consist of:

1. Triangulation integrated three primary data sources: documentary evidence, structured interviews across three iterations with IT and non-IT stakeholders, and direct process observations by enabling cross-verification and reducing single-method bias while capturing the comprehensive spectrum of PT XYZ's IT governance practices.

DOI: https://doi.org/10.17509/seict.v7i1.95229
p-ISSN 2774-1656 | e-ISSN 2774-1699

2. Inter-rater reliability was maintained through dual independent scoring of capability levels by qualified assessors for all 14 GAMO domains, with discrepancies resolved via consensus protocols to achieve consistent maturity ratings and minimize subjective interpretation in quantitative capability assessments.
3. Audit trail rigor documented complete traceability for all collected evidence against ideal requirements, including evidence matrices, scoring worksheets, interview transcripts, observation logs, ensuring full reproducibility for regulatory audits.
4. Stakeholder validation involved formal review workshops with Process Owners (PICs) who confirmed findings accuracy, validated gap analyses, and bridging assessment results with organizational context for enhanced practical applicability.

3. RESULTS AND DISCUSSION

3.1 Overall Maturity Assessment Findings

The COBIT 2019 assessment began with systematic evidence collection across PT XYZ's 14 GAMO domains, identifying 1,370 required governance artifacts, including policies, SOPs, and operational records. Of these, 552 documents were successfully validated, resulting in 49% evidence completeness. Strengths were observed in operational areas such as service request and incident management (82%), while significant gaps were identified in security documentation (7%) and capacity planning.

Process activity evaluation assessed all 191 COBIT-defined activities across the 14 GAMO domains, categorizing them as Fully Achieved (71 activities, 37%), Largely Achieved, and Partially Achieved to identify governance strengths and gaps affecting service reliability. This evidence validation and activity mapping formed the basis for capability maturity scoring using COBIT 2019's six process attributes: process performance, work products, process definition, process deployment, process measurement, and process improvement. This approach enabled precise domain-level maturity assessment reflecting PT XYZ's IT governance profile, as presented in Table 1.

Table 1. Result Analysis

No	Domain Code	Domain Name	Result
1	EDM03	Managed Risk Optimisation	3,02
2	APO02	Managed Strategy	3,27
3	APO09	Managed Service Agreements	3,15
4	APO10	Managed Vendors	3,35
5	APO12	Managed Risk	3,11
6	BAI02	Managed Requirements Definition	2,98
7	BAI03	Managed Solution Identification and Build	3,35
8	BAI04	Managed Availability & Capacity	2,82
9	BAI06	Managed IT Changes	2,82
10	BAI11	Managed Projects	3,47
11	DSS01	Managed Operations	3,34
12	DSS02	Managed Service Requests and Incidents	3,04
13	DSS05	Managed Security Services	2,96
14	MEA01	Managed Performance and Conformance Monitoring	3,08
		Average	3,13

DOI: https://doi.org/10.17509/seict.v7i1.95229
p-ISSN 2774-1656 | e-ISSN 2774-1699

The resulting average capability maturity level of 3.13 - Defined confirms that PT XYZ operates primarily at Level 3 characteristics with standardized processes across most domains, reflecting established practices for delivery assurance (BAI11: 3.47) and KPI tracking (MEA01: 3.08) essential for operations continuity. Post-audit adjustment refined this to 3.10, accounting for evidence quality consistency and formal documentation gaps, establishing a credible, defensible baseline for organization's regulatory reporting and strategic improvement planning.

3.2 Domain-Specific Maturity Performance

High-Performing Domains consistently demonstrated Level 3+ (Defined and above) characteristics indicative of mature, standardized practices well-suited to technology demands. BAI11 Managed Projects (3.47) exhibited robust project governance frameworks featuring clearly defined methodologies tailored for complex system implementations, such as software deployments and ground handling integrations, including standardized delivery tracking mechanisms with milestone gates and progress dashboards, and rigorous quality assurance processes ensuring on-time, within-budget delivery critical for maintaining service continuity during peak operational periods. Similarly, MEA01 Managed Performance and Conformance (3.35) showcased established KPI monitoring dashboards providing real-time visibility into Service Level Agreements (SLAs), automated periodic compliance reviews aligned with regulatory cycles (e.g., monthly safety reporting, quarterly audit readiness), and structured conformance monitoring protocols that proactively identify deviations from operational excellence benchmarks, thereby supporting PT XYZ's reputation for reliable technology solutions in high-stakes environments.

Critical Domains Requiring Priority Remediation fell significantly below Level 3 thresholds, exposing substantial risks to operations continuity and regulatory compliance. BAI04 Managed Availability and Capacity (2.82) revealed critically inadequate capacity planning processes lacking annual forecasting models for peak travel seasons, absence of formalized Business Impact Analysis (BIA) to prioritize mission-critical support systems, and insufficient service continuity planning exposing 24/7 service operations to unplanned outages with potentially cascading effects across ecosystems. BAI06 Managed IT Changes (2.82) demonstrated fundamental deficiencies including the lack of centralized change request logging systems, standardized impact assessment protocols, and mandatory Post-Implementation Reviews (PIR), creating uncontrolled modification environments prone to service disruptions in safety-critical service applications. DSS05 Managed Security Services (2.96) exhibited fragmented access control architectures, complete absence of physical security logging for data centre facilities supporting operations and inadequate audit trail mechanisms compromising traceability requirements essential for organization's regulatory investigations and cybersecurity incident response.

Performance distribution analysis highlighted systematic maturity gaps contributing approximately 60% to overall aggregate variance, with disproportionate deficiencies concentrated in Build-Acquire-Implement (BAI) domains responsible for system development, capacity management, and change control, alongside Deliver-Service-Support (DSS) domains handling operational security and incident response, precisely the functional areas underpinning zero-tolerance security postures protecting safety-related data flows, and rapid recovery capabilities essential for regulatory reporting obligations within PT XYZ's services ecosystem.

DOI: https://doi.org/10.17509/seict.v7i1.95229
p-ISSN 2774-1656 | e-ISSN 2774-1699

3.3 Key Gap Analysis

Evidence Completeness Gaps exhibited stark disparities across governance domains, highlighting systemic documentation deficiencies that undermine Level 3 formalization requirements essential for regulatory compliance and operational audit readiness. Service request and incident management processes achieved 82% coverage through resolution reports and SLA monitoring artifacts, supporting rapid operational recovery and demonstrating mature incident response capabilities critical to maintaining airport ecosystem service continuity. Conversely, physical security controls lagged dramatically at only 7% completeness, lacking essential access logs, badge swipe records, CCTV audit trails, and facility access matrices, underscoring urgent prioritization needs for comprehensive access management formalization within airport ecosystem integrations, where unauthorized access represents existential safety and compliance risks.

Process Maturity Distribution revealed a polarized landscape with 37% of activities achieving Full Achievement status concentrated in established operational procedures such as daily operations monitoring (DSS01) and service delivery (DSS02), where consistent execution patterns supported 24/7 service imperatives through documented runbooks and performance metrics. However, strategic alignment processes including APO02 Managed Strategy remained Partially Achieved, where <2.5 due to fragmented IT-business road mapping and enterprise goal cascading insufficient for long-term organization's technology investment prioritization, while change governance under BAI06 exhibited similar deficiencies characterized by ad-hoc modification approvals and absent impact assessments.

IT and operations personnel juggled real-time passenger processing responsibilities, security compliance reporting deadlines, and peak-period airport throughput demands, necessitating multiple rescheduling cycles across the three data collection iteration. Despite these temporal challenges, the assessment achieved 100% deliverable completion, including validation and refinement of 17 existing SOPs as foundational Level 3 artifacts, specifically enhancing Capacity Planning templates (BAI04), formalizing Change Request Log protocols (BAI06), and developing Security Access Review matrices (DSS05) by demonstrating methodological resilience while establishing immediately actionable governance instruments tailored to PT XYZ's services ecosystem requirements.

3.4 Discussion: Implications for Organization's IT Governance

These findings validate PT XYZ's impressive transition from Level 2 reactive management toward Level 3 defined standardization, a remarkable achievement considering the company was newly formed through a 2024 merger process, where organizations at this early stage typically operate at Level 1-2 (Initial/Ad-hoc), by establishing process consistency essential for organization's high-reliability requirements while exposing domain-specific vulnerabilities threatening service continuity and regulatory compliance. The 3.10 adjusted maturity confirms operational foundation strength but underscores strategic remediation imperatives in capacity planning (BAI04), change control (BAI06), and security services (DSS05) comprising 60% gap contribution, demonstrating highly effective system integration and governance standardization within an impressively short timeframe.

BAI04 deficiencies reflect the absence of capacity forecasting for peak travel periods; BAI06 gaps expose change-related incidents in mission-critical systems; DSS05 weaknesses

DOI: https://doi.org/10.17509/seict.v7i1.95229
p-ISSN 2774-1656 | e-ISSN 2774-1699

compromise data integrity for safety reporting. Collectively, these represent unacceptable risk exposure in safety-critical technology services demanding >99.9% availability and zero-tolerance security postures.

The assessment's 49% evidence completeness underscores documentation formalization as Level 3 prerequisite, while 37% Full Achievement rate validates established operational practices suitable as quick-win foundations. Timeline deviations highlight operational realities necessitating flexible assessment scheduling without compromising methodological rigor.

4. CONCLUSION

This research successfully validated PT XYZ's IT governance maturity at Level 3.10 (Defined) through comprehensive COBIT 2019 assessment across 14 GAMO domains, confirming standardized processes suitable for organization technology demands while identifying critical remediation priorities in BAI04 (2.82), BAI06 (2.82), and DSS05 (2.96) representing 60% of maturity gaps. The 49% evidence completeness where 552 of 1,370 documents completed and 37% Full Achievement rate of activities where 71 of 191 activities accomplished. This indicates the credible baselines for regulatory compliance and operational excellence, despite timeline extension reflecting real-world constraints.

Key contributions include a prioritized remediation roadmap of enhanced maturity by 2026 through immediate quick wins by improving Capacity Planning templates, Change Logs, Access Matrices, medium-term process formalization BIA protocols, security audits, and delivering measurable value alignment with organization’s enterprise goals for 99.9% service reliability, zero-tolerance security, regulatory compliance, while providing empirical evidence of COBIT 2019 applicability in safety-critical contexts complementing CMMI and ISO/IEC 38500 standards.

Future research should explore longitudinal maturity tracking post-implementation, comparative analyses across organization’s sector, which is airport services, and integration with emerging standards like ISO 27001 for cybersecurity maturity specific to organizational data flows, ultimately advancing enterprise IT governance scholarship within high-reliability industries demanding uncompromised safety, compliance, and operational performance.

5. ACKNOWLEDGMENT

The authors express profound gratitude to the management team and IT department of PT. XYZ for their unwavering support, active participation in assessment interviews, and generous access to operational documentation in IT governance maturity evaluation.

6. AUTHORS’ NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. Authors confirmed that the paper was free of plagiarism.

7. REFERENCES

Asriannoor, M. (2024). Maturity Level Analysis of FT ULM Service System Using The Cobit 2019 Framework. *Jurnal Teknologi Informasi Universitas Lambung Mangkurat (JTIULM)*, *9*(2), 89–100.

Berrada, H., El Ghazi El Houssaïni, S., and Boutahar, J. (2023). Implementing Information Technology Risk Management: A Case Study in the African Airline Industry. *Journal of Organizations, Technology and Entrepreneurship*, *1*(1), 58–76.

Charolina, Y., Andry, J. F., Honni, Lee, F. S., and Azhari, O. (2024). Evaluasi Kinerja Aplikasi Accurate Menggunakan Cobit 5 Domain MEA (Kasus Perusahaan Dagang). *JBASE - Journal of Business and Audit Information Systems*, *7*.

Ciptaningtyas, H. T., Ginardi, R. V., Aliski, A. D., Caronongan, D., and Santoso, M. (2024). *Change Management Implementation on E-Government System Using PROSCI ADKAR with Control Standard of COBIT2019 and ITIL v4*. Scopus.

COBIT 2019 Framework Governance and Management Objectives. (2019).

Fianty, M. I., and Brian, M. (2023). Leveraging COBIT 2019 Framework to Implement IT Governance in Business Process Outsourcing Company. *Journal of Information Systems and Informatics*, *5*(2), 568–579.

Fraga, C., Abelém, A., Borges, V., Pinheiro, B., and Cordeiro, W. (2024). A Blockchain-based Approach for Continuous Auditing in IT Change Management. *NOMS 2024-2024 IEEE Network Operations and Management Symposium*, 1–4.

Harison, E., and Lahav, Y. (2024). Finding the "Secret Sauce" for Organizational Sustainability: Towards Successful Completion of IT Implementation Projects. *Sustainability*, *16*(18), 8154.

Kwak, P., and Desanti, R. I. (2023). IT Governance Evaluation Using COBIT 2019 Framework in A Manufacturing Company. *2023 7th International Conference on New Media Studies (CONMEDIA)*, 62–67.

Lompoliu, E., and William Tangka, G. M. (2024). Information Technology Governance Using the COBIT 2019 Framework at PT Bank Pembangunan Daerah Papua. *International Journal of Engineering, Science and Information Technology*, *4*(4).

Majdalawieh, M., and Khan, S. (2022). Building an Integrated Digital Transformation System Framework: A Design Science Research, the Case of FedUni. *Sustainability*, *14*(10), 6121.

Novrian, M. R., Dazki, E., Pradita, U., and Sangereng, C. (2025). *Evaluation of information technology governance maturity using cobit 2019: study of a telecommunication company*. *10*(2).

Petrin, N. S. M., Néto, J. C., and Mariano, H. C. (2025). MAISTRO: Towards an Agile Methodology for AI System Development Projects. *Applied Sciences*, *15*(5), 2628.

Primaditama, A., Miftah Fadhil, M. R., and Sanan, F. F. (2025). Application of Company Goal Design Factor Based on COBIT 2019 to Improve Startup Company Goals. *Journal of Software Engineering, Information and Communication Technology (SEICT)*, *6*(1), 63–72.

Simatupang, A., and Adrianto, H. J. (2024). Audit Tata Kelola Teknologi Informasi dalam Mendukung Penerapan Good Corporate Governance (Studi Kasus PT XYZ). *Jurnal Sistem Informasi Bisnis*, *14*(2), 162–170.

Skačkauskienė, I., and Leonavičiūtė, V. (2025). Change Management in Aviation Organizations: A Multi-Method Theoretical Framework for External Environmental Uncertainty. *Sustainability*, *17*(15), 6994.

Sudarsono, B. G., Ananda, V. R., Kandi, M. R., and Azhari, O. (2023). Audit Aplikasi Keuangan Menggunakan Framework COBIT 5.0 Domain DSS Studi Kasus Perusahaan Peralatan Tambang. *JBASE - Journal of Business and Audit Information Systems*, *6*(1).

Sudarsono, B. G., Cornelius, W., Lesmana, K., Azhari, Samuel, S., Natanael, J., and Andry, J. F.

DOI: https://doi.org/10.17509/seict.v7i1.95229
p-ISSN 2774-1656 | e-ISSN 2774-1699

(2023). IT Policy di Perusahaan Pelayaran. *JBASE - Journal of Business and Audit Information Systems*, *6*(2).

Tambunan, S. R., Sihombing, I. E., and Sibarani, T. (2025). Implementasi Audit Internal WebTrust CA/NS pada Perusahaan Penyedia Tanda Tangan Digital. *JBASE - Journal of Business and Audit Information Systems*, *8*.

Yusuf, A., Saputra, W. A., and Jamilah, J. (2024). Capability Gap Analysis in IT Governance for a Logistics Company Using COBIT 2019. *Journal of Information Systems and Informatics*, *6*(3), 1804–1821.

DOI: https://doi.org/10.17509/seict.v7i1.95229
p-ISSN 2774-1656 | e-ISSN 2774-1699