Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.16083
e-ISSN : 2541-2019
p-ISSN : 2541-044X

CTRI Framework: Integrating COBIT 4.1 Maturity, Risk Priority, and Transition to COBIT 2019

Kasmala[1)*], Hilyah Magdalena[2)]
[1,2)]information systems study program ISB Atma Luhur, Indonesia
[1)]2222500007@mahasiswa.atmaluhur.ac.id, [2)]hilyah@atmaluhur.ac.id

Submitted :April 11, 2026 | **Accepted** : May 6, 2026 | **Published** : July 5, 2026

Abstract: This study proposes the CTRI (COBIT Transition and Risk Integration) framework, a novel methodological integration for IT governance evaluation in SMEs. Unlike prior COBIT 4.1 studies that only report maturity gaps, the CTRI framework addresses three critical gaps: (1) lack of actionable recommendations, (2) absence of risk and feasibility considerations, and (3) no systematic bridge from COBIT 4.1 to COBIT 2019. The CTRI framework consists of three integrated layers. Layer 1 quantifies maturity gaps across six COBIT 4.1 domains (PO2, AI2, AI6, DS5, DS11, ME1). Layer 2 introduces the Risk–Feasibility Priority Matrix (RFPM) which calculates a Priority Action Score (PAS) = Risk Impact × Implementation Feasibility, where risk impact is high (3), medium (2), or low (1), and feasibility is easy (3), moderate (2), or difficult (1). Recommendations with PAS ≥ 6 are top priority. Layer 3 provides explicit transition mapping from each COBIT 4.1 recommendation to COBIT 2019 governance objectives and design factors. Applied to a sales application at PT Ciequ (Indonesian SME), data were collected via observation, interviews with three key informants, and documentation review. Findings reveal an average maturity level of 2.45, with largest gaps in AI2 (1.23) and DS5 (0.89). The RFPM prioritizes AI2 (PAS=9), DS5 (PAS=6), and AI6 (PAS=6) as top actions. A three-phase transition roadmap (Stabilize → Standardize → Monitor) to COBIT 2019 is provided, with APO13 (security) and APO05 (portfolio) as priority objectives. This study contributes a reusable, risk-aware, transition-forward methodology that bridges legacy and modern IT governance frameworks for resource-constrained SMEs.

Keywords: CTRI framework, COBIT 4.1, COBIT 2019, risk-feasibility matrix, SME

INTRODUCTION

Digital transformation has fundamentally reshaped business operations across all sectors. Information technology (IT) is no longer a mere support function but a strategic driver of competitive advantage, operational efficiency, and market reach (Ricky Rohmanto1, Miki Wijana2, Sarah Nurfadhilah3, 2025). For small and medium enterprises (SMEs), which dominate the Indonesian economy, the adoption of sales applications and e-commerce platforms has become essential to expand market reach and facilitate business-to-customer (B2C) transactions (Maghfiroh et al., 2023)(Widiana et al., 2022). However, the increasing dependence on IT also introduces significant risks if not governed properly.

COBIT (Control Objectives for Information and Related Technology) is a comprehensive framework for IT governance and management published by ISACA. COBIT 4.1 covers four main domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate (Charoensiwarak et al., 2025). Many SMEs have adopted information systems but lack systematic IT governance evaluations, resulting in suboptimal management and increased risks (Septiawan et al., 2024).

Despite the widespread use of COBIT 4.1 for maturity assessment, existing studies predominantly focus on measuring current conditions without offering actionable, prioritized recommendations tailored to resource-constrained SME environments (Nurfadhiilah et al., 2024)(Purba, 2024). A systematic review of the literature reveals three critical research gaps. First, no prior study has integrated risk impact and implementation feasibility into the prioritization of improvement recommendations. Second, there is no methodological bridge connecting COBIT 4.1 assessment results to COBIT 2019 design factors, leaving a gap in how legacy framework findings can inform modern IT governance implementation. Third, the specific context of sales applications in Indonesian SMEs remains underexplored in COBIT literature.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.16083
e-ISSN : 2541-2019
p-ISSN : 2541-044X

To address these gaps, this study proposes the CTRI (COBIT Transition and Risk Integration) framework, a novel three-layer methodological integration. Layer 1 quantifies maturity gaps using six COBIT 4.1 domains (PO2, AI2, AI6, DS5, DS11, ME1). Layer 2 introduces the Risk–Feasibility Priority Matrix (RFPM), which calculates a Priority Action Score (PAS) = Risk Impact × Implementation Feasibility, where risk impact is categorized as high (3), medium (2), or low (1), and feasibility as easy (3), moderate (2), or difficult (1) based on SME resource constraints. Recommendations with PAS ≥ 6 are designated as top priority. Layer 3 provides explicit transition mapping from each COBIT 4.1 recommendation to COBIT 2019 governance objectives (e.g., AI2 → APO05, DS5 → APO13/DSS04) and aligns with the seven COBIT 2019 design factors (enterprise strategy, enterprise goals, risk profile, IT-related issues, threat landscape, compliance requirements, and role of IT).

Unlike previous studies that merely report maturity scores, the CTRI framework transforms descriptive assessments into prescriptive, risk-aware, transition-forward decision support. This represents the first documented integration of COBIT 4.1 maturity assessment with COBIT 2019 design factors in the Indonesian SME context. The framework is specifically designed to be reusable and adaptable by other resource-constrained SMEs.

While COBIT 5 and COBIT 2019 offer more comprehensive guidance, COBIT 4.1 remains a valid choice for this study for three reasons, including simplicity and accessibility for SMEs new to formal IT governance evaluation (Andika et al., 2024), availability of established benchmarks allowing meaningful comparison with prior Indonesian SME studies, and proportionality, where the complexity of COBIT 2019 would be counterproductive for PT Ciequ's current maturity level (Antariksa et al., 2025). However, to ensure forward compatibility, this study uniquely maps assessment findings to COBIT 2019 design factors, creating a transition pathway not previously documented in the literature.

PT Ciequ is a company that utilizes a sales application to support online sales transactions, including customer data management and transaction processing. Preliminary observations indicate that IT management practices are not yet standardized, documented, or formally evaluated. Therefore, this research aims to: (1) assess the current maturity level of IT governance for the sales application at PT Ciequ using COBIT 4.1 domains PO2, AI2, AI6, DS5, DS11, and ME1, (2) identify the gap between current and expected (level 3) maturity, (3) formulate prioritized improvement recommendations based on risk impact and implementation feasibility using the RFPM, and (4) map the findings to COBIT 2019 design factors to provide a transition roadmap.

LITERATURE REVIEW

COBIT 4.1 for IT Governance Evaluation in SMEs, Research on IT governance evaluation using the COBIT framework has been widely conducted across various organizational contexts, including SMEs. Previous studies indicate that COBIT 4.1 is effective in assessing the maturity level of IT governance and identifying weaknesses in technology-based business processes (Lusiana U. et al., 2024). However, recent studies highlight that IT governance implementation in Indonesian SMEs still faces significant challenges, such as limited resources, lack of process documentation, and the absence of systematic evaluation of information systems (Antariksa et al., 2025). Other research shows that although organizations have adopted information systems, the management of these systems is often not aligned with IT governance best practices, leading to operational and security risks(Andika et al., 2024).

Limitations of Existing COBIT 4.1 Studies, A systematic examination of prior COBIT 4.1 research reveals four critical limitations. First, most studies are purely descriptive, measuring current maturity levels without providing structured, actionable improvement recommendations (Nurfadhiilah et al., 2024)(Septiawan et al., 2024). Second, no prior study has integrated risk impact assessment into the prioritization of recommendations—risk is typically mentioned only conceptually. Third, implementation feasibility—a crucial factor for resource-constrained SMEs—is never considered in improvement planning. Fourth, there is no methodological bridge connecting COBIT 4.1 assessment results to more recent frameworks such as COBIT 2019. These limitations are particularly critical in SME environments, where resource constraints require improvement strategies that are not only effective but also practical and feasible.

Risk-Based Priority in IT Governance: A Missing Operationalization, Risk-based approaches to IT governance have gained attention in recent years. ISACA (2018) emphasizes that effective IT governance must be risk-aware, particularly for organizations with limited resources. However, within the COBIT 4.1 literature, risk is typically discussed only at the conceptual level. (Purba, 2024) conducted risk management analysis but did not operationalize risk into a prioritization mechanism. Similarly, (Septiawan et al., 2024) mentioned security risks but provided no systematic method to rank recommendations based on risk impact, let alone combine risk with implementation feasibility. This study addresses this gap by introducing the Risk–Feasibility Priority Matrix (RFPM) , which operationalizes risk impact as domain-specific (e.g., data breach risk for DS5, bus factor risk for AI2) and combines it with implementation feasibility to produce a quantifiable Priority Action Score (PAS) = Risk Impact × Feasibility. This operationalization has not been previously documented in COBIT 4.1 studies.

Transition from COBIT 4.1 to COBIT 2019: An Unaddressed Gap, COBIT 2019 introduces seven design factors that influence how an organization should implement IT governance: enterprise strategy, enterprise goals, risk

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

profile, IT-related issues, threat landscape, compliance requirements, and role of IT (ISACA, 2018). While COBIT 2019 is more comprehensive, many SMEs continue using COBIT 4.1 due to its simplicity and lower learning curve (Andika et al., 2024). However, a major gap exists in the literature: no prior study has systematically mapped COBIT 4.1 assessment findings to COBIT 2019 design factors. This creates a disconnect where organizations using COBIT 4.1 cannot easily transition to modern governance frameworks. This study uniquely addresses this gap by providing explicit mapping from each COBIT 4.1 domain to COBIT 2019 governance objectives (e.g., AI2 → APO05, DS5 → APO13/DSS04) and developing a three-phase transition roadmap (Stabilize → Standardize → Monitor).

Research Gap and Positioning of This Study, Based on the literature review, a research gap still exists in integrating maturity level assessment with risk-based priority analysis and in linking legacy framework results with modern IT governance approaches. Prior studies by (Lusiana U. et al., 2024), (Nurfadhiilah et al., 2024), (Septiawan et al., 2024), and (Purba, 2024) all share the same limitations: they are descriptive, lack risk-feasibility integration, and provide no transition pathway to COBIT 2019. In contrast, this study makes three novel contributions. First, it proposes the CTRI (COBIT Transition and Risk Integration) framework, a three-layer methodology that integrates maturity assessment, risk analysis, and feasibility evaluation. Second, it introduces the RFPM with PAS for objective, quantifiable prioritization of recommendations based on risk impact and implementation feasibility. Third, it provides a systematic transition roadmap from COBIT 4.1 to COBIT 2019 based on design factors mapping. This contribution is expected to provide a more comprehensive and applicable approach, particularly for SMEs in Indonesia seeking to improve their IT governance practices.

METHOD

Research Design, The data and information obtained in this study are used as the basis for analyzing user needs (Bangsa & Hasugian, 2022). This research employs a descriptive method with a qualitative approach to analyze the maturity level of IT governance in the sales application at PT Ciequ using the COBIT 4.1 framework and to identify the current state of system management (Cipta M Pasaribu et al., 2023). A single case study design was adopted to allow an in-depth exploration of IT governance in its real-life context.

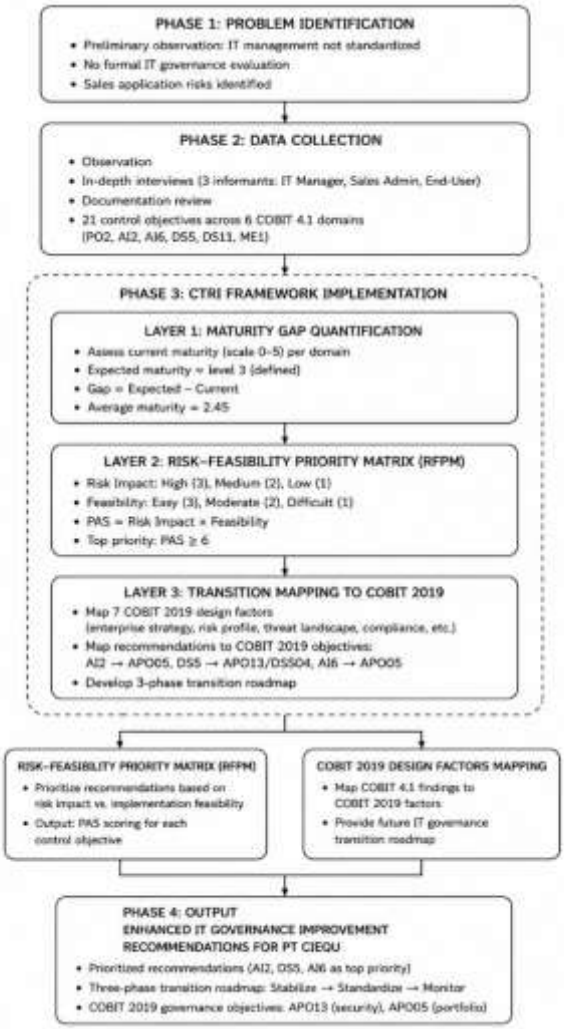
Research Object and Informatics, The object of this study is the sales application utilized by PT Ciequ to support online sales transactions, including customer data and transaction processing (Anggraeni et al., 2023). The research subjects were three key informants selected purposively: the IT manager, the sales admin, and an end-user (Amalsyah et al., 2025).

3.3 Data Collection, Data were collected through observation, in-depth interviews using a questionnaire mapped to 21 control objectives within six COBIT 4.1 domains (PO2, AI2, AI6, DS5, DS11, and ME1), and documentation review.

CTRI Framework Implementation, To address the novelty gap in prior COBIT 4.1 studies (Nurfadhiilah et al., 2024)(Septiawan et al., 2024)(Purba, 2024), this research implemented the CTRI (COBIT Transition and Risk Integration) framework through three layers. In Layer 1 (Maturity Gap Quantification), the collected data were analyzed using the COBIT 4.1 maturity model (Cipta M Pasaribu et al., 2023)(Lusiana U. et al., 2024). Current maturity was assessed on a scale of 0 to 5, with expected maturity set at level 3. The gap was calculated as Expected minus Current, and domains with gaps of 0.5 or greater were prioritized. In Layer 2 (Risk–Feasibility Priority Matrix/RFPM), each prioritized domain was assessed for Risk Impact (high=3, medium=2, low=1) and Implementation Feasibility (easy=3, moderate=2, difficult=1). The Priority Action Score (PAS) was calculated as Risk Impact multiplied by Feasibility, with PAS of 6 or greater designated as top priority (Andika et al., 2024). In Layer 3 (Transition Mapping to COBIT 2019), the seven COBIT 2019 design factors were assessed through interviews (Antariksa et al., 2025), and each recommendation was mapped to COBIT 2019 objectives (e.g., AI2→APO05, DS5→APO13/DSS04, ME1→EDM03/APO11). A three-phase transition roadmap (Stabilize → Standardize → Monitor) was then developed.Data Validity, To ensure trustworthiness, source triangulation and member checking were applied (Cipta M Pasaribu et al., 2023).

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Number 3, July 2026
DOI : https://doi.org/10.33395/sinkron.v10i3.16083
e-ISSN : 2541-2019
p-ISSN : 2541-044X



Research Framework, Figure 1 illustrates the complete research framework, showing the flow from problem identification to CTRI framework implementation and prioritized recommendations.

Fig 1. CTRI Framework Implementation for IT Governance Evaluatin

RESULT

This section presents the findings of the IT governance maturity evaluation for PT Ciequ's sales application using the CTRI (COBIT Transition and Risk Integration) framework across three layers: maturity gap quantification (Layer 1), risk–feasibility priority matrix (Layer 2), and transition mapping to COBIT 2019 (Layer 3). Layer 1: Maturity Gap Quantification, Based on the COBIT 4.1 maturity assessment across six domains (PO2, AI2, AI6, DS5, DS11, and ME1), the average maturity level for IT governance at PT Ciequ was calculated as 2.45. This score indicates level 2 (repeatable but intuitive), meaning that IT processes are ongoing but have not yet been formally standardized or documented.

Table 1 below presents the detailed maturity assessment per domain, including key findings from interviews and observation, current maturity scores, expected maturity (level 3), and the calculated gaps.

Table 1. Detailed Maturity Assessment per Domain

Domain	Key Findings from Interviews&Observation	Current Maturity Score	Expected Maturity	Gap
PO2	Information architecture planning exists but no formal documentation	2,72	3	0,28

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

AI2	Development and maintenance processes lack SOPs; dependent on one person	1,77	3	1,23
AI6	System changes are made informally; no approval process	2,40	3	0,60
DS5	No formal security policy; basic password protection only	2,11	3	0,89
DS11	Data backup is performed irregularly; no retention policy	2,82	3	0,18
ME1	IT performance is not formally monitored; no KPIs defined	2,87	3	0,13
Avarage		**2,45**	**3**	**0,55**

As shown in Table 1, the largest gaps are found in AI2 (1.23), DS5 (0.89), and AI6 (0.60). These three domains were selected for deeper analysis in Layer 2 (RFPM), as they represent the most critical improvement opportunities.

Layer 2: Risk–Feasibility Priority Matrix (RFPM), For each of the three domains with significant gaps (AI2, DS5, and AI6), the Risk Impact and Implementation Feasibility were assessed through expert judgment involving the IT manager and researcher triangulation. Risk Impact measures the potential consequence if the issue remains unaddressed for twelve months, categorized as High (3), Medium (2), or Low (1). Implementation Feasibility measures the ease of implementing the recommendation given PT Ciequ's resource constraints, categorized as Easy (3), Moderate (2), or Difficult (1). The Priority Action Score (PAS) was calculated as Risk Impact multiplied by Feasibility, with PAS ≥ 6 designated as top priority.

For the AI2 domain, the Risk Impact was assessed as High (score 3) because the "bus factor" risk could halt all application maintenance if the sole knowledgeable individual leaves the company. The Implementation Feasibility was assessed as Easy (score 3) because documenting existing procedures requires less than five person-days with no new tools. Thus, PAS = 3 × 3 = 9 (top priority). For the DS5 domain, the Risk Impact was assessed as High (score 3) because the absence of a security policy exposes customer data to potential breaches. The Implementation Feasibility was assessed as Moderate (score 2) because developing a security policy and role-based access control requires five to fifteen person-days. Thus, PAS = 3 × 2 = 6 (top priority). For the AI6 domain, the Risk Impact was assessed as Medium (score 2) because unapproved changes could introduce errors but with lower immediate impact. The Implementation Feasibility was assessed as Easy (score 3) because an Excel-based change log requires less than five person-days. Thus, PAS = 2 × 3 = 6 (top priority).

Table 2 presents the PT Ciequ profile based on COBIT 2019 design factors, which were assessed through interviews with the IT manager and operations director as part of Layer 3.

Table 2. PT Ciequ's Profile Based on COBIT 2019 Design Factors

Design Factor	**Assessment Result for PT Ciequ**	**Implication**
1. Enterprise Strategy	Growth/Aggressive - seeking market expansion through digital sales	Need governance that supports agility and scalability
2. Enterprise Goals	Operational excellence and customer satisfaction (primary); financial stability (secondary)	Focus on DS5 (security to protect customer data) and AI2 (reliable application)
3. Risk Profile	Moderate - aware of cyber risks but no formal risk management	Need basic risk assessment and mitigation procedures
4. IT-Related Issues	Security vulnerabilities, lack of documentation, dependency on key individuals	Prioritize DS5, AI2, and AI6 improvements
5. Threat Landscape	Increasing - SMEs are targeted due to weak security	Urgent need for security policy and access control

*name of corresponding author

6. Compliance Requirements	Minimal - no specific regulatory mandates for data protection currently	Voluntary governance improvements sufficient; no compliance-driven urgency
7. Role of IT	Support - IT enables sales but is not the primary product	Governance should be lightweight and practical, not overly complex

Layer 3: Transition Mapping and Prioritized Recommendations, Based on the integration of Layer 1, Layer 2, and COBIT 2019 transition mapping, six prioritized recommendations are proposed. For the AI2 domain, which achieved the highest PAS score of 9, the recommendation is to document existing maintenance procedures into a simple SOP and cross-train a second staff member to eliminate the bus factor risk, mapped to COBIT 2019 objective APO05. For the DS5 domain with PAS score of 6, the recommendation is to develop a one-page formal security policy, implement role-based access control, and conduct security awareness training, mapped to APO13 and DSS04. For the AI6 domain with PAS score of 6, the recommendation is to implement an Excel-based change management log including approval, testing, and recording, mapped to APO05.

For secondary priority recommendations, the PO2 domain requires creating formal documentation for information architecture including a data dictionary, mapped to APO01. The DS11 domain requires establishing an automated daily backup schedule and data retention policy, mapped to DSS04. The ME1 domain requires defining simple KPIs such as system uptime and response time and conducting monthly IT performance reviews, mapped to EDM03 and APO11. These secondary recommendations have lower priority given their smaller gaps and PAS scores below 6.

Transition Roadmap to COBIT 2019, Based on the CTRI framework findings, a three-phase transition roadmap from COBIT 4.1 to COBIT 2019 is proposed. Phase 1 (Stabilize, months 1-3) focuses on the highest-priority domains (AI2, DS5, AI6) with actions including SOP documentation, security policy development, and change log implementation, mapped to APO13 and DSS04. Phase 2 (Standardize, months 4-6) focuses on PO2 and DS11 with actions including information architecture documentation and automated daily backup, mapped to APO05 and DSS01. Phase 3 (Monitor, months 7-9) focuses on ME1 with actions including KPI definition and monthly performance reviews, mapped to EDM03 and APO11. By following this roadmap, PT Ciequ can systematically improve its IT governance maturity from 2.45 to level 3 while transitioning from COBIT 4.1 to COBIT 2019.

DISCUSSIONS

Interpretation of Findings in the Context of CTRI Framework, The findings reveal that PT Ciequ's IT governance maturity level of 2.45 is consistent with previous studies on SMEs. (Septiawan et al., 2024) reported a similar average maturity level of 2.3 for a transportation agency, while (Nurfadhiilah et al., 2024) found comparable results in general IT governance assessments. However, unlike prior studies that stop at reporting maturity scores, this research applied the CTRI (COBIT Transition and Risk Integration) framework to transform descriptive findings into actionable, prioritized recommendations.

The lowest score was recorded in the AI2 domain (1.77), which is concerning because this domain governs how application software is acquired and maintained. The lack of SOPs and dependence on a single individual creates a "bus factor" risk. This finding aligns with Lusiana U. et al. (2024), who identified similar vulnerabilities in online data systems. Through the CTRI framework's Layer 2 (RFPM), this domain received the highest PAS score of 9, confirming it as the top priority for intervention.

The DS5 domain (Ensure System Security) scored 2.11, the second lowest. The absence of a formal security policy exposes the company to data breaches. This finding is consistent with (Septiawan et al., 2024), but the CTRI framework further reveals that the primary cause at PT Ciequ is organizational (absence of written security roles) rather than technological. With a PAS score of 6, DS5 was designated as top priority alongside AI2 and AI6.

Methodological Contribution: The CTRI Framework, This study makes a novel methodological contribution through the CTRI framework, which addresses three critical gaps in prior COBIT 4.1 literature. First, while previous studies by (Nurfadhiilah et al., 2024), (Septiawan et al., 2024), and (Purba, 2024) only report maturity gaps, the CTRI framework introduces the Risk–Feasibility Priority Matrix (RFPM) with a quantifiable Priority Action Score (PAS = Risk Impact × Feasibility). This operationalization of risk—domain-specific rather than generic—has not been previously documented in COBIT 4.1 studies.

Second, unlike prior research that ignores implementation feasibility, the CTRI framework explicitly considers PT Ciequ's resource constraints by categorizing feasibility as easy, moderate, or difficult based on person-days, budget, and technical skills. This is particularly critical for SMEs where resources are limited.

Third, this study provides the first documented bridge from COBIT 4.1 assessment findings to COBIT 2019 design factors and governance objectives. While (Andika et al., 2024) and (Antariksa et al., 2025) have discussed COBIT 2019 implementation, no prior study has systematically mapped COBIT 4.1 results to COBIT 2019. The

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

three-phase transition roadmap (Stabilize → Standardize → Monitor) offers a forward-compatible pathway for SMEs still using COBIT 4.1.

Transition Roadmap and COBIT 2019 Alignment, The mapping of PT Ciequ's profile to COBIT 2019 design factors (Table 2) reveals several important insights. First, the enterprise strategy (growth/aggressive) suggests that IT governance should enable rather than hinder speed and flexibility. This justifies the prioritization of recommendations that are easy to implement (AI2 documentation, AI6 change log) over more complex initiatives. Second, the moderate risk profile combined with an increasing threat landscape indicates that security improvements (DS5) cannot be delayed. Third, the minimal compliance requirements mean PT Ciequ has the freedom to implement lightweight, practical solutions without needing to satisfy external auditors—a significant advantage for an SME.

The recommended COBIT 2019 core model for PT Ciequ is the "Governance and Management Objectives for Small and Medium Enterprises" (ISACA, 2018), with APO13 (Security) and APO05 (Portfolio) as priority objectives. This aligns with the RFPM findings where AI2 and DS5 received the highest PAS scores.

Limitations of the Study, This study has several limitations. First, the assessment relies on self-reported information from three key informants, which may introduce bias despite triangulation. Second, the study is limited to six COBIT 4.1 domains and does not cover all IT processes. Third, the findings are specific to PT Ciequ and may not be generalizable to other SMEs without contextual adaptation. Fourth, the CTRI framework has been applied only to a sales application context; further validation is needed across different types of information systems. Finally, COBIT 4.1 has been superseded by COBIT 5 and COBIT 2019, although this study explicitly addresses this through transition mapping.

CONCLUSION

This study evaluated the maturity level of IT governance for the sales application at PT Ciequ using the COBIT 4.1 framework across six domains (PO2, AI2, AI6, DS5, DS11, and ME1) and introduced the CTRI (COBIT Transition and Risk Integration) framework as a novel methodological contribution. The findings reveal an average maturity level of 2.45 (level 2: repeatable but intuitive), with the largest gaps identified in AI2 (1.23) and DS5 (0.89).

This study makes three novel contributions to the IT governance literature. First, unlike prior COBIT 4.1 studies that only report maturity scores (Nurfadhiilah et al., 2024; Septiawan et al., 2024; Purba, 2024), this research proposes the CTRI framework, a three-layer methodology that integrates maturity gap quantification, risk–feasibility analysis, and transition mapping. Second, this study introduces the Risk–Feasibility Priority Matrix (RFPM) with a quantifiable Priority Action Score (PAS = Risk Impact × Feasibility) , which transforms generic risk-based priority analysis into a domain-specific, resource-aware decision tool. The RFPM successfully prioritized AI2 (PAS=9), DS5 (PAS=6), and AI6 (PAS=6) as top priority actions for PT Ciequ. Third, this study provides the first documented transition roadmap from COBIT 4.1 to COBIT 2019 for an Indonesian SME, including explicit mapping of COBIT 4.1 recommendations to COBIT 2019 governance objectives (APO13, APO05, DSS04) and a three-phase roadmap (Stabilize → Standardize → Monitor).

The results of this study answer the research questions by showing that the current maturity level of IT governance at PT Ciequ is 2.45, the average gap to level 3 is 0.55, and the prioritized recommendations are AI2 (SOP documentation and cross-training), DS5 (security policy and access control), and AI6 (change management log). The COBIT 2019 design factors mapping indicates that PT Ciequ should adopt the "Governance and Management Objectives for Small and Medium Enterprises" core model, with APO13 (Security) and APO05 (Portfolio) as priority objectives.

For future research, it is recommended to apply the CTRI framework to other SME contexts to validate its generalizability, adopt COBIT 2019 directly for a more comprehensive evaluation using the transition roadmap developed in this study, expand the scope to include all COBIT domains, and conduct longitudinal studies to measure the impact of implemented recommendations on actual maturity improvement.

REFERENCES

Amalsyah, M. R., Kurniawan, D., Rifai, A., Sari, P., Studi, P., Informasi, S., Komputer, I., Sriwijaya, U., Masjid, J., Gazali, A., Lama, B., Palembang, K., & Selatan, S. (2025). Analisis Sentimen Ulasan Pengguna Aplikasi Fintech menggunakan Framework CRISP-DM dalam Penentuan Prioritas Pengembangan Produk. *Sistemasi: Jurnal Sistem Informasi*, *14*(2), 813–825. http://sistemasi.ftik.unisi.ac.id

Andika, D., Mulyana, R., & Ramadhani, L. (2024). IT Governance Design Based on COBIT 2019 SME Focus Area for UMKM BPRBCo Digital Transformation. *Journal of Information System Research (JOSH)*, *6*(1), 205–218. https://doi.org/10.47065/josh.v6i1.5905

Anggraeni, O. P., Karyadi, K., & Abdussalaam, F. (2023). Perancangan Sistem Informasi Penjualan Berbasis Web di PT. MARKTEL. *Jurnal Teknologi Sistem Informasi Dan Aplikasi*, *6*(4), 523–530.

*name of corresponding author

https://doi.org/10.32493/jtsi.v6i4.33156

Antariksa, M. D. S., Angin, M. P., & Widodo, A. P. (2025). COBIT 2019 Framework in IT Governance: A Systematic Literature Review of Implementation Challenges and Benefits Across Various Industry Sectors. *Journal of Renewable Energy, Electrical, and Computer Engineering*, *5*(1), 99–105. https://doi.org/10.29103/jreece.v5i1.19501

Bangsa, G. P., & Hasugian, H. (2022). Perancangan Dan Implementasi Sistem Informasi Penjualan Berbasis Web E-Commerce Pada Toko Febriyanahelmet. *IDEALIS : InDonEsiA JournaL Information System*, *5*(2), 126–134. https://doi.org/10.36080/idealis.v5i2.2950

Charoensiwarak, K., Kuljirakul, K., Khomsom, P., Tasana, M., Saengkaew, K., Promduangsi, P., Watakulsin, P., & Saenkum, N. (2025). AUDIT SISTEM INFORMASI PADA APLIKASI SISTEM KLINIK MENGGUNAKAN FRAMEWORK COBIT 4.1 DOMAIN MONITOR AND EVALUATE Studi Kasus: WW Dental Clinic. *Jurnal Sistem Informasi (TEKNOFILE)*, *10*(2), 66–79.

Cipta M Pasaribu, Mega Mustika, Dewi Rosmayanti, Abdul Rahman Kadafi, & Eko Setia Budi. (2023). Sistem Informasi Monitoring Absensi Menggunakan Framework COBIT 4.1. *Bulletin of Computer Science Research*, *3*(4), 289–296. https://doi.org/10.47065/bulletincsr.v3i4.268

Lusiana U., Imtihan K., & Zaen M.T.A. (2024). Audit Aplikasi Online Data Sistem (Ods) Menggunakan Cobit 4.1. *Jurnal Informatika Teknologi Dan Sains (JINTEKS)*, *6*(2), 211–216.

Maghfiroh, Ma'sumatul, F., Natalina, Anugrah, S., Efendi, & Rofik. (2023). Transformasi Ekonomi Digital: Connection Integration E-Commerce Dan S-Commerce Dalam Upaya Perkembangan Ekonomi Berkelanjutan. *Proceedings of Islamic Economics, Business, and Philanthropy*, *2*(1), 01–10. https://jurnalfebi.iainkediri.ac.id/index.php/proceedings

Nurfadhiilah, A., Faharuddin, F., & Jumaryadi, Y. (2024). Analisa Audit Sistem Informasi Tata Kelola TI menggunakanFramework COBIT 4.1 dengan mengukur Tingkat MaturityLevel. *SISTEMASI: Jurnal Sistem Informasi*, *13*(2), 412–419. http://sistemasi.ftik.unisi.ac.id

Purba, F. A. (2024). ANALISIS MANAJEMEN RESIKO TEKNOLOGI INFORMASI DAN PEMETAAN MATURITY LEVEL MENGGUNAKAN FRAMEWORK COBIT 4.1 (Studi Kasus: PT. CAHAYA BINTANG). *Jurnal Teknologi Dan Manajemen Sistem Industri*, *3*(1), 11–20. https://doi.org/10.56071/jtmsi.v3i1.497

Ricky Rohmanto1, Miki Wijana2, Sarah Nurfadhilah3, M. E. H. (2025). Pengukuran Tingkat Maturity Tata Kelola Sistem Informasi Rumah Sakit dengan Menggunakan Framework Cobit 4.1 (Studi Kasus: Rumah Sakit "A"). *INTERNAL (Information System Journal) Indormatika*, *8*(3), 135–144.

Septiawan, E., Andini, S., & Rahmawati, S. (2024). Analysis of Information Technology Governance in the Transportation Agency using the Cobit 4.1 Framework. *Journal of Computer Scine and Information Technology*, *10*, 108–113. https://doi.org/10.35134/jcsitech.v10i4.112

Widiana, S. A., Sintaro, S., Arundaa, R., Alfonsius, E., & Lapihu, D. (2022). Aplikasi Penjualan Baju Berbasis Web (E-Commerce) dengan Formulasi Penyusunan Kode. *Journal of Information Technology, Software Engineering and Computer Science (ITSECS)*, *1*(1), 35–43. https://doi.org/10.58602/itsecs.v1i1.11

*name of corresponding author